Probabilistic Process Algebra

Probabilistic Process Algebra

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr. R.A. van Santen,
voor een commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op dinsdag 26 november 2002 om 16.00 uur

door

Suzana Andova

geboren te Veles, Macedonië

Dit proefschrift is goedgekeurd door de promotoren:

prof.dr. J.C.M. Baeten
en
prof.dr. C.A. Middelburg

CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN

Andova, Suzana

Probabilistic process algebra / by Suzana Andova. - Eindhoven :
Technische Universiteit Eindhoven, 2002.
Proefschrift. - ISBN 90-386-0592-7
NUR 993
Subject headings : process algebra
CR Subject Classification (1998) : F.3.2, F.1.2, D.2.4, D.1.3

IPA Dissertation Series 2002-15.

This thesis has been supported by the Netherlands Computer Science Research Foundadtion (SION) with financial support from the Netherlands Organization for Scientific Research (NWO) whitin the scope of the project NWO/SION 612-10-000. It has been carried out under the auspicies of the Institute for Programming Research and Algorithmics (IPA).

Dedicated to Danilo and Sofia-Ana

Acknowledgements

My interest in Process Algebra started about seven years ago. While I was still at the Faculty of Natural Sciences and Mathematics in Macedonia, on several occasions I met and had discussions with Jos Baeten. And it became very clear to me that I would like to do a doctoral studies in this field. So, I decided to move to the Netherlands. I have never regretted that. The next four years, that I spent at the University of Eindhoven as a Ph.D. student in the Formal Methods Group, was a period of hard work, of learning and exploring the beauty of formal methods and concurrency theory, and of course, a period of a great fun and an exploration of the Dutch culture. Many people have contributed to my life or to my research in different ways. Here I mention some of them.

First of all, I would like to thank my promotor Jos Baeten. My first contact ever with Process Algebra was his famous "blue book". But during these four years I had a great opportunity to work with him and learn from him much more than I could ever read in any book. No matter how busy he was, he would always find time to listen and discuss my problems and provide new ideas whenever I got stuck. It happened all the time that I would walk into his office with a long list of axioms and in only a day or two I would get his comments and suggestions back. Also I would like to thank him for having such a great understanding and for the support he gave me during some difficult times.

Next I would like to thank Smile Markovski and Gjorgji Čupona, two very important persons in my life. I had the pleasure to be their student, and later, after my graduation, to work with them on different projects. Their passion for research and enthusiasm during very difficult times in Macedonia, made a very deep impression on me and left lasting marks on my personality. I also thank them for organizing many interesting seminars where I "made my first steps" in the world of science and research.

This thesis would have not been the same without the help of my second promotor Kees Middelburg. I thank him for the careful reading of all my writings and for teaching me how to write papers. I thank Joost-Pieter Katoen and Jan Bergstra who reviewed the manuscript before it was submitted. Their suggestions and comments helped to improve considerably this dissertation, specially in the presentation aspects. In particular Joost-Pieter made several remarks that helped me to correct mistakes that, though they did not seem very important, they could have annoyed and misled the reader.

An important source of feedback on my ideas I found in the members of PROMISE (PRObabilistic Methods In Software Engineering) during our meetings. PROMISE was a cooperation set up among people in the Netherlands working on probabilistic systems that provided an excellent forum for informal presentations and discussions. Hence, Mariëlle Stoelinga , Pedro D'Argenio, Holger Hermanns, Joost-Pieter Katoen, Erik de Vink, Jerry den Hartog, Perry de Groot, Frits Vaandrager and Ed Brinksma thank you for many interesting and enjoyable meetings and fruitful discussions. I also enjoyed the regular meetings of the PROMACS-project (Probabilistic Methods for the Analysis of Continuous Systems) where I learned about probabilistic GSOS, categorical coalgebra and game theory. Many thanks go to Jan Rutten, Jos Baeten, Jaco de Bakker, Falk Bartels and Alexandru Baltag. I am also grateful to Rob van Glabbeek, Roberto Segala, Wan Fokkink, Pedro D'Argenio, Jan

Friso Groote, Onno Boxma and Chris Verhoef for some productive discussions and for their useful suggestions on several problems I was stuck with.

Not only important for productive work but also desirable to keep enjoying it, is to be part of a research group in which people get along both socially and scientifically. The Formal Methods Group provided an excellent atmosphere for work and also for joy. Special thanks go to my office mates: Tim, Georgi and Martijn and also to the members of the RISK group: Marceltje, Ana, Dragan and Victor. I thank all of you for many enjoyable coffee breakes, lunches, dinners and late-night risk games. Without your help and support my life in Eindhoven would have been very tough and miserable. Unique thanks go to Tim and Georgi. I could not imagine better office mates. With their stupid jokes, they always succeeded to cheer me up even in the most difficult moments. Our discussions and the sketches of probabilistic bisimilar graphs on the white board in the office with the sign "Do not erase", encouraged me and put me back on track many times. Furthermore, they helped me with final arrangements for this thesis, Tim translated the summary into Dutch and Georgi arranged things with the printer. I thank my other colleagues of the Formal Methods Group, Jos, Kees, Erik, Michel, Rob, Andre, Roel, Sjouke, Ruurd, Jerry, Gia, Elize, Anne-Meta, Francien and Tijn for enjoyable gatherings organized in different occasions within the group.

During these years I had the greatest pleasure to have Nino and Olga as my friends. We have spent so much time together that I do not remember how my life was before I met them. Also a big thanks to my other friends Helene, Rosane, Fred, Eric, Carlos, Bart, Tatjana who make my life interesting in Eindhoven.

I am also grateful to the members of the Institute of Informatics, at the Faculty of Natural Sciences and Mathematics in Skopje for giving me a leave and for taking over my teaching obligations within that period. I would like to thank Ed Brinksma, Joost-Pieter Katoen and Holger Hermanns for offering me a job at the University of Twente and also to my colleagues from the Formal Methods and Tools Group for helping me in settling in Enschede.

My mother, Vera, deserves endless thanks for her unconditional love and support, in spite for me being away from her.

My final grateful thanks go to my husband Danilo for his unconditional love and never ceasing support and understanding. His telephone calls, visits and e-mail messages kept me strong during these difficult years for the both of us.

Contents

List of Tables

Chapter 1

Introduction

1.1 Formal methods

Formal methods are not introduced and developed for coffee and coca-cola vending machines. The complexity of these systems is still low enough to fit within the limits of the complete understanding of a single designer or a small group of designers. As the complexity of system designs begins to exceed the human limits the necessity of additional instruments and techniques starts to increase. Thus the idea of formal methods appears.

Formal methods are analytical approaches based on a rigorous mathematical models intended to exclude or at least to reduce errors in software and hardware design. Due to their mathematical basis, formal specifications given in a formal language are precise, clear and unambiguous. Besides a language meant to let the designer write a model of a system and construct a specification, a formal method should include a proof system (mathematical rules) that allows the user to reason about statements in the formal language. By analysis and manipulation of the given formal expressions he or she can reason about the dynamic behaviour of the system and even more can establish certain relationships between different expressions (systems). Of course the final goal of such an analysis is to prove (to verify) that the proposed implementation conforms to the specification (or that the system satisfies certain properties). This process is called *formal verification*. If a system has been formally verified, one knows that the system is correct (error free) in all possible instances of its behaviour (under all possible weather conditions [89]).

However, we should not forget that formal methods work with (abstract) models of systems. Thus the analysis methods are applied to these models but not to the real systems themselves. This implies that formal verification assures only that the model satisfies certain properties. Therefore, if the model is too abstract and it does not adequately describe the real system, or if the written specification differs from the intended one, then the proof is worthless.

Initial attempts to reason formally about programs were undertaken by Floyd [52], Hoare [76] and Dijkstra [51]. The methods they developed (based on first order logic) were focused on proving correctness of imperative programs. In the late seventies and early eighties a different approach was taken - developing methods for reasoning about concurrent processes. Thus, Pnueli [97] proposed a temporal logic to reason about concurrent programs. Petri [94] developed a theory of concurrency - now well known as the theory of Petri nets - where real concurrency of events is considered. Milner [89] and Hoare [77] proposed algebraic methods to reason about concurrent processes. These methods are called *process algebra*. In the last two decades several variants of process algebra have come into existence, the most important of which are CCS (Calculus of Communicating Systems [89, 92]), CSP (Communication Sequential Processes [77, 78]) and ACP (Algebra of Communicating Processes

[34, 36, 27]). As the title of the thesis says we will look at this class of formal methods.

The main idea of process algebra is to have a simple language by which the behaviour of concurrent systems can be described and which has "as few operators or combinators as possible, each of which embodies some distinct and intuitive idea, and which together give completely general expressive power" [91]. And also "a useful calculus[1] should be possible to describe existing systems, to specify and program new systems, and to argue mathematically about them, all without leaving the notational framework of the calculus" [89]. In fact, the possibility to have specification and implementation expressed in the same language and even more, staying in the same formalism when establishing the relation between these two is one of the biggest strengths of process algebra.

Every process algebra is supplied with an operational semantics (usually based on transition systems). While the algebraic equations give an insight into the relationship between processes described by some algebraic expressions, the operational semantics concerns the process behaviour. It describes which activities and operational steps a process can perform by which the operational behaviour of the process is completely captured. Thus, on the semantic level one can reason about processes that show identical behaviour defined by some equivalence relation - usually strong or branching or weak bisimulation.

Among the process theories *ACP* is considered most algebraic since it puts more emphasis on the axiomatic theory itself rather than on its (operational) semantics. In this thesis, we propose several process algebras that extend *ACP*. A brief introduction to *ACP* is given in Chapter 2.

1.2 Probability

When using traditional methods to model a concurrent system, designers restrict themselves to the functional behaviour of that system. This means that the designer, for instance, can detect an error in the system or may claim that the system is deadlock free, or can say that eventually the process leaves the critical section or that the process terminates or that the message will be delivered. But in real-life systems not only functionality but also quantitative aspects of the system behaviour are important. Thus, one would rather know the probability that the system reaches an error state or the number of retransmissions that should be done in order to have the message delivered correctly. Even more due to the physical implementation of the system and its interaction with the environment one cannot expect a perfect system without a possibility to fail. Naturally, the designer wants to be certain that the probability for this to happen is sufficiently small. To mention an example reported in [5] where the security protocol has been claimed unsafe because the method used for its verification lacks techniques for accurate modelling of the protocol. Using probabilistic formal methods the authors show that the protocol can reach an "unsafe" state but the probability for the system to end up in this state can be controlled and made desirably small.

In this thesis, we turn our attention to probabilistic phenomena and propose methods for specifying and verifying systems that show probabilistic behaviour - probabilistic systems. There are several instances where probabilistic aspects have to be considered. First, in the case of an unreliable system where the whole system or some of its components are subject to failure. Usually, failures of system (components) are probabilistic in nature or can be approximated by some probabilistic process. Clearly in these cases probabilities should be used for the sake of obtaining a more accurate model of the system. Second, probabilities can be used in distributed algorithms that use the concept of randomization (randomized algorithms). In this case the random choice is introduced to increase performance and even in some cases to produce a solution for problems that are unsolvable in the

[1] We use the words process algebra, process calculus and process theory as synonyms.

fully deterministic setting. The third application of probabilities that we will discuss in more detail in Chapter 6 is that they can be used to model fairness. Besides, another aspect where probabilities play an important role is performance analysis. Lately, many efforts have been done to get together research communities working in the areas of probabilistic (stochastic) modelling and performance analysis. This issue goes beyond the scope of this thesis and for further reading we refer to [47] and [46].

1.2.1 Introducing probabilities in formal methods

As known from probability theory, probability means to assign a real number from the interval $[0, 1]$ to a possible event, outcome or object; if the same experiment is repeated a number of times then the probability gives the frequency that the particular event/outcome will appear or that the object will be chosen. Think about flipping a coin or throwing a die or pulling a white ball out of a bag. When modelling the probabilistic behaviour of a (concurrent) system we are not far from this situation. Simply because governed by a probabilistic law the system or the environment "chooses" between several alternative behaviours (system components). In the first case where the probabilistic choice is resolved independently of the environment we talk about *internal* probabilistic choice. A probabilistic choice is considered *external* if the environment determines which alternatives among all possible ones are enabled. In this thesis, we assume internal probabilistic choices.

Mainly two approaches have been taken to extend the traditional formal methods with probabilities. One approach is to replace alternative composition by probabilistic choice. As a result a fully probabilistic model of a system is obtained. On the other hand, some models allow probabilistic choice as well as alternative composition.

One may argue that in the presence of probabilities alternative composition can be thrown away; basically that the fully probabilistic model is sufficient. In [98] we can find interesting arguments on this issue. However, in the presence of a probabilistic choice operator, we still have a need of an alternative composition because (see also [11]):

- alternative composition used in the interleaving approach of parallel composition does not model uncertainty but independent activities of the parallel processes or a lack of information for their dependencies. Even though the source of it may be a random process the system can be so complex that practically it is impossible to determine or even approximate the probability distribution of that process. In [17] an attempt to replace alternative composition by probabilistic choice in interleaving of parallel processes was done but this turned out to be very impractical in system specification;

- alternative composition is very practical in modelling value passing: sending a particular value by a process will communicate with a process allowing the receipt of any possible value. Replacing it by probabilistic choice may easily lead to a deadlock situation. This use of alternative composition will always be resolved in the parallel composition, except in the case of an open system, where interactions with the environment are modelled;

- non-determinism may not make much sense for people doing performance analysis, but in formal methods, the main issue is functionality of systems, (correctness, deadlock-freeness) whether probabilistic aspects are taken into account in the specification of the system or not. Even though introducing probabilities in the specification may lead to easier proofs of desired properties, this does not mean that the system should be underspecified by "approximating" alternative composition by a probabilistic distribution.

1.3 Time

Certainly, another aspect that has to be taken into account when modelling hardware or software systems is *time*. Thus it is not sufficient to know that some event will occur eventually but in some cases it is desirable to occur and in some other situations it has to occur within some time bounds. For instance, we expect that our computer promptly responds to our request; if it does not no harm is done (except that we are annoyed). But if the flight control system does not react within a specific period of time, catastrophic consequences may occur.

In this thesis, we propose an algebraic framework that can be used to model both the probabilistic and time behaviour of a system. By means of a method that can reason about probabilistic and time aspects at the same time we are able to deal with (specify and verify) more realistic properties of systems like "with probability 0.9 your computer will respond within 30 seconds". In this thesis, we consider discrete-time systems. This means that if the system occupies state s at moment k, then the next occupied state at moment $k+1$ is randomly chosen governed by some discrete probability distribution. This distribution does not depend on the previous states that the system has been in but only depends on the last occupied state, namely s. This property is well known as *memory-less property* or *Markov property* [85]. Our semantical model is strongly related to discrete-time Markov chains [85, 79] in the deterministic case and to Markov decision processes [79] in the presence of non-determinism.

Alternatively, there are models where time and probabilities are integrated by considering delays of a continuous probabilistic nature. In this case, a transition that the system makes from state s to state s' is assigned a continuous distribution function expressing the probability that this transition will be taken (among the other possible ones) within some period of time (that the system spends in state s). Various theories have been proposed with respect to the distributions allowed in the model like TIPP [62], Interactive Markov Chains [74], PEPA [75], EMPA [39, 40] that restrict the attention to exponential distributions, and stochastic automata, SPADES [50], a general semi-Markovian process algebra [45], NMSPA [87] that consider a more complex case and consider general distributions.

1.4 Main results

This thesis is divided into four parts. In the first part, we propose an extension of ACP with probabilities called *pACP*$^+$. This means that the probabilities are introduced in the process algebra by introducing a new probabilistic choice operator. At the same the alternative composition operator of ACP is kept. In order to achieve the interleaving nature of the asynchronous parallel composition we add an auxiliary operator by means of which we obtain a finite axiomatization of the parallel composition operator. We also define an operational semantics for our theory including the notion of strong probabilistic bisimulation. We show that the axiomatization is sound and complete with respect to the bisimulation model.

In the second part, we concentrate on a time extension of the previously defined probabilistic process algebra called $pACP^+_{drt}$. In $pACP^+_{drt}$ timing is considered to be discrete. In our language, we can model undelayable process as well as processes that can be delayed an arbitrary period of time.

While the first two parts are mainly focused on developing a specification method, the third part focuses on verification. In this part, we introduce the notion of abstraction to the untimed fully probabilistic process algebra. In the case of the ACP-like approach this is not included in the basic theory, but rather is introduced as an additional feature. A set of verification rules is defined as well as the notion of probabilistic branching bisimulation that constitutes a model for the axiomatization. We

remark that this bisimulation relates processes that are not related by any of the existing equivalence relations for probabilistic processes and that intuitively should be related. An algorithm that decides this relation is defined as well.

The last part presents several case studies that show how the earlier defined formalisms can be used to model concurrent systems. It also shows how the verification method can be integrated with the specification method and how it is used to prove the correctness of the described systems.

1.5 Outline of the thesis

The thesis consists of seven chapters organized in the following way:

Chapter 2 This chapter is an introductory part into process algebra. In short, we present several process algebras, among which ACP, relevant for this thesis. This chapter also presents some proof techniques used later in the thesis.

Chapter 3 A basic process algebra containing basic operators is introduced. The probabilistic choice operator is defined and the way it is combined with the alternative composition operator is described.

Chapter 4 The process algebra from Chapter 3 is extended with the notion of an asynchronous parallel composition. We give a number of theoretical results about the new algebra like the elimination property and soundness and completeness results for the axiomatization with respect to the defined model.

Chapter 5 Timing features are added to the process algebras from Chapter 3 and Chapter 4. We discuss the necessity of introducing a new operator when probabilities, time and the interleaving approach to asynchronous concurrency are combined. Operational semantics and a time variant of probabilistic bisimulation are defined.

Chapter 6 This chapter treats the issue of abstraction in the fully probabilistic model. A probabilistic process algebra with abstraction is defined as well as its semantical model based on probabilistic branching bisimulation.

Chapter 7 We apply the theories from Chapter 4, 5 and 6 to the specification and verification of an untimed and a timed variant of the PAR (Positive Acknowledgment with Retransmission) protocol. By means of the CABP (Concurrent Alternating Bit Protocol) we describe possible directions to extend the process algebra and the bisimulation from Chapter 6 with non-determinism.

Chapter 8 We give an overview of the results from the thesis and discuss future research.

1.6 Related work

Work on probabilistic extensions of process algebras started in the early nineties. The pioneer work has been presented in [86, 54, 56, 81, 80, 70]. These approaches use labelled transition systems as an underlying operational model in which probabilities are associated to transitions. Certainly one of the major results is presented in [86] where the notion of traditional (strong) bisimulation equivalence is extended to the notion of probabilistic bisimulation for probabilistic processes. For fully probabilistic

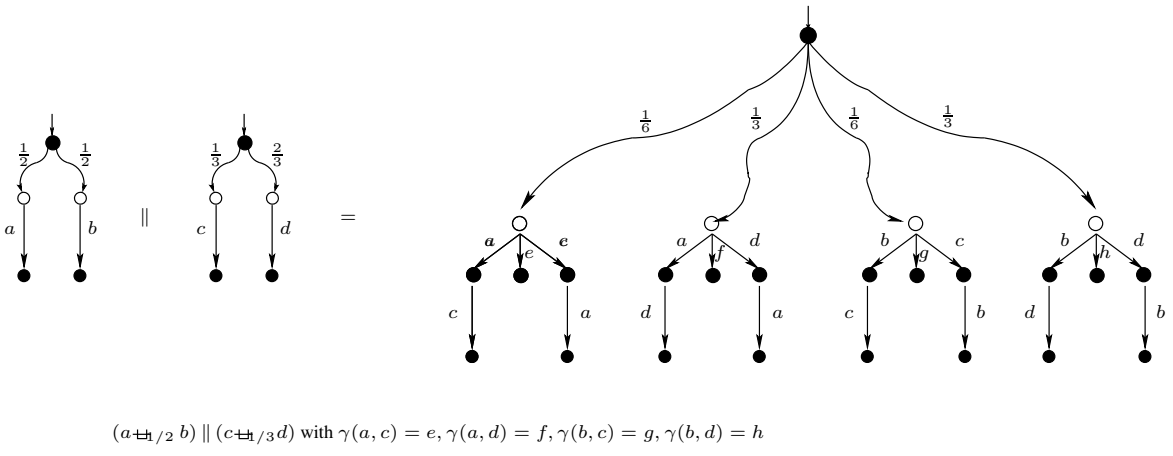
systems this notion corresponds to lumping equivalence [82]. In [56], the authors classified probabilistic models into three classes: reactive, generative and stratified. In the reactive model, different probability distributions are assigned to different actions. The probabilities assigned to the outgoing transitions of one state labelled with the same action name sum up to 1. The philosophy behind this scheme is that the environment chooses an action among all possible ones, and afterwards the system internally chooses the next state according to the probability distribution. In the generative model every state is assigned one probability distribution defined over all outgoing transitions regardless which action label transitions have. The stratified model extends the generative model in a way that it captures the branching structure of purely probabilistic choice made by a process. Using PCCS [54, 80], an extension of SCCS [91], the authors define an operational semantics and a bisimulation equivalence for each model.

In contrast to these models, in [70, 71] we find a new probabilistic model, called the *alternating model*. In this model, probabilistic transitions are separated from action transitions. As a result this model distinguishes between probabilistic and non-deterministic states. Outgoing transitions of a probabilistic state are labelled by probabilities that sum up to 1, like in the generative model. Outgoing transitions of a non-deterministic state are labelled by atomic actions. We employ this model to define the semantics of our process algebras. In the proposed probabilistic extension of Milner's CCS in [71] also called PCCS, a new probabilistic choice operator is introduced in addition to (and not as a replacement of) non-deterministic choice operator. Thus, there are two types of expressions: non-deterministic and probabilistic ones. In Figure 1.1[2] we give an example of the parallel composition of two PCCS processes. One of the processes can perform a with probability $1/2$ and b with probability $1/2$. The other process can perform c with probability $1/3$ and d with probability $2/3$. The parallel composition of these processes with probability $1/6$ behaves as a (non-deterministic) process (the snaky arrow in the figure labelled by $1/6$ that starts in the initial state and reaches a state represented by $\circ$) that actually represents the interleaving of a and c. Thus, this state represents a process that chooses non-deterministically between action a, action c and action e. e is the communication action of a and c. If a is chosen, the execution of a is followed by an execution of c. If the non-deterministic choice is resolved in favour of c then the execution of c is followed by an execution of a. In the third case in which e is chosen after the execution of e the process terminates. In a similar way we interpret the other branches shown in the figure. Thus, in order for the processes to start to interleave both have to resolve the internal probabilistic choices and only afterwards the interleaving between the two obtained non-deterministic processes can take place. Our approach differs exactly on this issue since according to our definition two parallel processes can start to interleave as soon as one of them has resolved its internal probabilistic choice. This will be presented in more detail in Chapter 4.

In [49], a probabilistic model based on so-called bundle transition systems is defined on which a probabilistic variant of asynchronous parallel composition very similar to our definition is proposed. Besides, several criteria that an asynchronous parallel composition for probabilistic processes has to satisfy are defined.

A first attempt to extend ACP with probabilities has been reported in [17]. The alternative composition operator is replaced by a probabilistic choice operator. Due to the absence of alternative composition, the defined parallel composition operator is decorated with two probabilistic parameters σ and θ. θ gives the probability that the parallel processes synchronize on a communication action. The probability that the processes do not synchronize but proceed autonomously is thus $1 - \theta$. In this case, the left-hand process of the parallel composition is selected to make the first action with probability σ and the right-hand process does so with probability $1 - \sigma$. Basically, the probabilistic choice

[2]Here we borrow the notation we use in Chapter 4.



$(a \leftthreetimes_{1/2} b) \parallel (c \leftthreetimes_{1/3} d)$ with $\gamma(a,c) = e, \gamma(a,d) = f, \gamma(b,c) = g, \gamma(b,d) = h$

Figure 1.1: Parallel composition as defined in Hansson's alternating model.

in this setting is considered to be external. This causes certain problems in defining the encapsulation operator since renormalization of probabilities has to be taken into account (see also the discussion in [49]).

In [102], a complete axiomatization for a probabilistic CCS-like language with possibly unguarded finite-state recursive definition is studied. Based on this result, in [3] the authors propose a complete axiomatization obtained by extending the general axioms of iteration algebra [41], which characterize the equational properties of the fixed point operator on continuous or monotonic function, with several axiom schemas that express laws specific to probabilistic bisimulation.

In [100], a model of probabilistic automata is introduced and studied. In the case of probabilistic automata a transition from a state leads to a probability distribution over states rather than to a single state, as it is the case in ordinary automata. Thus, the choice between different transitions is a nondeterministic choice, while the choice of a state within a transition is a probabilistic choice. In [32] a comparison of the alternating model and the model of probabilistic automata is given. Different axiomatizations corresponding to different bisimulation relations are analyzed. The authors show that for both models the axiomatizations for strong probabilistic bisimulation coincide. On the other side, they show that the alternating semantics and the semantics of probabilistic automata based on weak bisimulation of [101, 100] are incomparable.

Developing verification techniques for probabilistic models has been a central issue of many researchers as well. Inspired by their counterparts in the nonprobabilistic case, several probabilistic bisimulation and simulation relations have been proposed. As mentioned above in [86] the first definition of (strong) bisimulation for probabilistic systems is defined. Basically, this definition later has been adapted into a probabilistic bisimulation for different probabilistic models: [56] for the reactive, generative and stratified models, [71] for the alternating model and [101, 100] for probabilistic automata. On the other hand, it is still a great challenge to define a relation that abstracts away internal actions.

In his dissertation [80], Jou defines a notion of probabilistic branching bisimulation for finite processes. Basically, the probabilistic branching bisimulation that we define in Chapter 6 coincides with the one of Jou for finite processes. In [29] weak and branching bisimulation relations for fully probabilistic processes are defined. The authors show that in the probabilistic setting these two definitions coincide. They also give an algorithm to compute the weak bisimulation equivalence relation in time $\mathcal{O}(n^3)$ where n is the number of states in the considered probabilistic transition system.

For models of probabilistic systems with non-determinism different bisimulation relations are defined in [101, 100, 95, 30, 103]. In [101, 100] the strong and weak bisimulation relations defined in [92] and [88] are generalized to the probabilistic framework. Since in probabilistic automata a transition leads to a probability distribution over states, an equivalence relation defined between two automata has to be extended to probability distributions over states. In this case, non-determinism is resolved by means of randomized schedulers. In [95] another variant of weak bisimulation is defined for labelled concurrent Markov chains. To compute this bisimulation only a finite set of schedulers, so-called deterministic schedulers, have to be investigated. Based on this result an algorithmic method that decides the weak bisimulation relation is defined. In [30, 103] so-called delay bisimulation is introduced which uses the concept of norm functions [63].

Chapter 2

Preliminaries from Process Algebra

In this chapter, we give a brief introduction into the basic aspects of ACP-style process algebra. We limit ourselves to those aspects relevant for this thesis. The purpose of this overview is to give the foundations upon which we build our of probabilistic and timed extensions. The definitions are presented without many details and technicalities. For more details concerning this material we direct the reader to [34, 27, 26, 53, 38].

2.1 Process Algebra

Process algebra is an algebraic theory used to specify and verify, in general to study processes. As the name says itself, process algebra finds its mathematical foundation in algebra. And so, compared with other formal methods developed for the same purposes, in process algebra, the processes and their behaviour are written in the form of process expressions and the relations between them are written in the form of algebraic equations. In that way, manipulations with processes becomes manipulations with equations in the algebraic sense.

The kernel of every process algebra consists of a set of operators (including constants as nullary operators) and a set of axioms. Axioms are of the form $t = t'$ where t and t' are terms in the considered process algebra containing operators and/or free variables. Sometimes axioms are extended to so-called conditional axioms: an axiom that can only be applied provided a certain condition holds. They have the form $\bigwedge_{i \in I} t_i = t'_i \Rightarrow t = t'$ for a finite set I and terms t_i, t'_i, t and t'.

Behind every operator and axiom there is an intuitive motivation: an insight that explains in which way we want to compose small processes to bigger ones (by means of operators) and which processes should be considered equal (by means of axioms). In other words, equations and operators do not have any meaning unless we place them in a certain real "world" and match the terms of the process algebra with the entities of the real world. This step is traditionally called "giving an interpretation of the formal theory" in the algebraic community and "giving a semantics of the syntax" in the computer science community. Consider, for example, the algebraic equation $x \hat{} 2 = 1$ where x is a variable. If we do not say what we mean by " $\hat{}$ ", "2", "1" and "=" and what is the range of x, this equation is meaningless. On the other hand, it can have different solutions (the values x takes for which the equation becomes true) depending on our idea behind the above symbols. Thus, if the symbols are given the standard meaning in the set of natural numbers we obtain that 1 is the solutions of the equation. In the set of real numbers there are two solutions, namely for $x = 1$ and $x = -1$. If x ranges over the set of natural numbers and $=$ means $\equiv_{mod5}$ then the equation has another meaning. In the second year of elementary school according to their own interpretation of the symbols the equation

may have as a solution the number of pupils in the class. In the same way, the equation $X = a \cdot G$ as such does not mean anything. But it may mean: read a message (the meaning of a) and answer it (the meaning of G), press $Alt - F4$ (for a) and switch off your computer (for G) or press any key (for a) and go on with your work (for G).

The *operational semantics* of terms of process algebra is usually given by transition relation(s) in the form $p \rightarrow p'$ (usually labelled). Namely, each term represents a process and the behaviour of one process is described by a set of activities that it can perform: for every possible activity there is one assigned transition. We read $p \stackrel{l}{\rightarrow} p'$ as: p can do some activity that is described by l and afterwards it behaves like p'. Transition relations are defined by a set of rules, called *deduction rules* that together with the operators form a *term-deduction system* (for the formal definitions see Section 2.3). These rules basically describe the way the behaviour of small processes reflects on the behaviour of a bigger process obtained by composing the smaller ones. The issue of operational semantics will be constantly treated through the thesis. More details about operational semantics in general and particular semantics of the process algebras presented in the thesis will be discussed in almost all subsequent chapters.

A popular way to present process algebras is by *modularization*. Namely, starting from a small set of operators and axioms, one can add new features by adding new operators and axioms. It is a very convenient concept if a more complex theory needs to be constructed. The track to the desired theory may lead through a growing sequence of embedded theories starting from a very simple one. Also, having small modules for one feature (or a few) makes it possible to combine them in different ways, in different theories suitable for particular problems. Following this concept, we structure the introduction as follows. We start with a basic process algebra. Then step by step we introduce more complex theories with their signatures and related set of axioms, each of them as an extension of some simpler theory previously defined. After that, we say a few words about the operational semantics and the bisimulation models of these theories.

The last section of this chapter presents some proof techniques and strategies which will be used throughout the thesis many times. This section also introduces the notations and the abbreviations used in the thesis. The concept of term-rewriting systems and some techniques developed in this field, and shown useful in solving problems in the area of process theory, will be presented as well. Finally, we discuss two approaches to show that a given set of deduction rules defines a transition relation. As mentioned above, deduction systems give meaning of algebraic expressions and algebraic equations. So, we are predisposed to a deduction system that defines meaningful transition relations.

2.1.1 Basic process algebras

Every process algebra has basic constructors: constants and operators. Constants stand for the atomic actions that the considered processes (intended to be modelled by the relevant process algebra) can execute. Therefore, every process algebra is parametrized by a fixed, finite set A - a set of designated atomic actions. A will be also used to denote the set of constants that correspond to the atomic actions. Some process algebras have some additional constants that stand for special processes (for example the deadlock process).

The most simple process algebra that we start this introduction with is called Basic Process Algebra, *BPA*[1]. This process algebra forms the core on which all other process algebras are built. Nevertheless, we have to point out that in Chapter 3 we will start with a process algebra that is not an

[1]More precisely Basic Process Algebra is a class of process algebras that have the properties presented here. In the sequel by BPA and in general by PRA we mean an element of the relevant class of algebras.

extension of *BPA*.

BPA has two (binary) operators: the sequential composition operator $\cdot$ and the alternative composition operator also called non-deterministic choice operator $+$. The sequential composition is used to express when two processes are executed one after the other (sequentially); given processes p and q the process that first executes p and after p terminates successfully continues with q is denoted by $p \cdot q$. If a process can proceed with two (or more) different processes, say alternative p or alternative q, the choice between these two alternatives is presented by $p + q$. The choice between p and q is made exactly when the first action of p or q is executed. The process which has not been chosen is discarded; it cannot be recovered later. To conclude, the signature of *BPA* consists of $\Sigma_{BPA} = (A, \cdot, +)$. These operators are called basic operators since all other operators introduced later in this chapter can be eliminated in favour of these. The axioms of process algebra *BPA* are shown in Table 2.1.

$x + y$	=	$y + x$	$A1$
$(x + y) + z$	=	$x + (y + z)$	$A2$
$x + x$	=	x	$A3$
$(x + y) \cdot z$	=	$x \cdot z + y \cdot z$	$A4$
$(x \cdot y) \cdot z$	=	$x \cdot (y \cdot z)$	$A5$

Table 2.1: Axioms of *BPA*.

$a + a$	=	a	$AA3$

Table 2.2: Alternative axiom for the idempotency law.

Axiom $A1$ and $A2$ express commutativity and associativity, respectively, of the alternative composition: ordering and grouping of the alternatives is irrelevant for the outcome of the choice. Axiom $A4$ expresses the right distributivity of sequential composition over alternative composition; no matter which alternative is chosen, x or y, after its successful termination the process continues to execute z. Once again we point out that the choice between x and y is resolved at the moment when the first action of x or y is executed. This interpretation is the reason the left distributivity law of sequential composition over alternative composition is not present; if $x \cdot (y + z)$ and $x \cdot y + x \cdot z$ are considered equal then the intuition behind the alternative composition will be that all choices are resolved at the very first moment when the process is initialized (see e.g. [18]). Adding this axiom to the set of axioms of *BPA* leads to a so-called trace semantics [55, 61]. Axiom $A5$ does not need any justification. Axiom $A3$ expresses the idempotency of the alternative composition: choice between the same alternatives gives always the same outcome. Notice that in presence of the other axioms of *BPA*, the axiom $A3$ in Table 2.1 is equivalent, for closed and guarded terms in *BPA* (the notion of guardedness will be discussed in Section 2.1.3), to the axiom $AA3$ in Table 2.2. Thus, $A3$ in *BPA* (and any extension of *BPA*) can be replaced by $AA3$ without affecting the equalities in *BPA* valid for closed and guarded terms. The reason to do so, is the fact that $AA3$ remains valid in all probabilistic process algebras we will describe, whereas $A3$ does not (see Example 3.2.3). Since we stick here to the set of axioms of *BPA* as it is in [27], we use $A3$ in the definition of *BPA* and all other non-probabilistic process algebras.

Deadlock

Every term of *BPA* represents a process that can perform at least one action. But sometimes it is desirable and even necessary to model a process that does nothing. Such a process is called a *deadlock process*. As it cannot be expressed by means of the *BPA* constructors, we add a new constant δ - deadlock or inaction - meaning exactly what has been said above: it represents a process that nor executes an action neither terminates successfully. It is defined by the axioms given in Table 2.3. The new algebra will be denoted by BPA_δ.

$x + \delta$	=	x	$A6$
$\delta \cdot x$	=	δ	$A7$

Table 2.3: Axioms for inaction.

Axiom $A7$ expresses that once deadlock is reached no further activities are possible. Note that $a \cdot \delta$ is not equal to a because the latter one executes action a and terminates successfully. In the literature two type of termination can be found: deadlock as described above and successful termination (also called empty process). The latter one sometimes is also introduced by means of a new constant ε ([84, 14, 27, 20, 25]). Thus, $\varepsilon \cdot a = a$ because the only activity that process ε can do is to terminate successfully and afterward action a is executed. In other process algebras, for instance CCS, CSP no distinction between successful and unsuccessful termination is made.

Axiom $A6$ expresses that the deadlock process can never be chosen as an alternative if there is another possibility; when a process contains a deadlock alternative the alternative composition tries to avoid it whenever possible. In [72] the authors build a semantical model in which this axiom is not valid.

Definition 2.1.1. The set of basic terms in BPA_δ is defined inductively as follows:

1. For every $a \in A_\delta$, a is a basic term;
2. If $a \in A_\delta$ and t is a basic term, then $a \cdot t$ is a basic term;
3. If t, s are basic terms, then $t + s$ is a basic term.

If in the first and the second items, instead of $a \in A_\delta$ we take $a \in A$ and the third item is unchanged, we obtain the inductive definition of the set of basic terms of *BPA*.

From now on, if we state something for *BPA* and BPA_δ, instead of giving two separate statements, one for *BPA* and another one for BPA_δ, we use in short $BPA_{(\delta)}$ as a variable that means either *BPA* or BPA_δ.

Example 2.1.2. We finish this section by an example to show a type of process that can be described by BPA_δ. Consider a communication channel that reads a datum from a process and sends it out to an other process. During the transmission the datum can be damaged. We will define the term that represents the behaviour of the channel, the other two processes are not important at this moment. For the specific problem the following set of atomic actions suffices to describe the process: $A = \{read\_from, send\_to, damage\}$. In accordance to this, our process algebra has four constants, namely $A = \{r_f, s_t, d, \delta\}$ where r_f stands for atomic action $read\_from$, s_t stands for atomic action

$send\_to$ and d stands for atomic action $damage$. The channel behaviour can be described by the following term $r_f \cdot (s_t + d)$. Clearly, by this we model a highly unrealistic communication channel: it can be used to transmit only one message. Yet we neither have constructors to model a communication channel that can be used for infinitely many transmissions, nor we can model the way our channel reacts in a "real" communication with the processes on "the ends" of the channel. δ is not used in this specification but it will be essential in some later examples where we improve the specification of the communication channel.

2.1.2 Algebra of communicating processes

The conclusion which finishes the example above implies that BPA_δ should be strengthened. First we solve the second problem stated in the conclusion by adding new operators to the signature of BPA_δ. The key operator for modelling concurrent systems, as one of the main aims of process algebra, is the parallel composition or merge operator $\parallel$. $p \parallel q$ describes a process that executes p and q in parallel, generating all possible interleavings and all possible communications of the two components. Thus, p and q may synchronise (communicate) on certain actions but they can also perform actions autonomously. Communication is defined by means of a function $\gamma : A_\delta \times A_\delta \to A_\delta$ that indicates which atomic actions communicate. This function is assumed to be commutative and associative, and satisfies the equation $\gamma(\delta, a) = \delta$ for all $a \in A$. The latter constraint expresses that δ does not communicate with any action. There are two other merge like operators added: the left merge operator $\between$ and the communication merge operator $|$. $p \between q$ represents a process similar to $p \parallel q$ with the restriction that the first action must be performed by p. The term $p \mid q$ represents a process similar to $p \parallel q$ whose first action is a communication between p and q; it forces the processes to synchronize. These operators, $\between$ and $|$ are actually auxiliary operators introduced to obtain a finite axiomatization for the parallel composition operator. The last operator added to the extended signature is the encapsulation operator ∂_H parametrized by a set of atomic actions H ($H \subseteq A$). The ∂_H operator is in fact a renaming operator which renames all actions from H into δ. It is used to encapsulate atomic actions that are intended to synchronize such that their asynchronous execution is not permitted.

The axioms of the new operators are given in Table 2.4 where a and b range over A_δ. These axioms together with the axioms in Table 2.1+2.3 constitute the axiom system of the process algebra *ACP*, called Algebra of Communicating Processes.

We briefly explain some of the axioms. Axiom $CM1$ expresses exactly the idea behind the parallel composition operator described above: the behaviour of two processes running in parallel consists of the independent execution of actions by the components (the first and the second summand) and of actions that are the result of synchronization between the two parallel components (the third summand). Axioms $CM2$ and $CM3$ state that the first action performed by $x \between y$ comes from the first argument x. If the first argument cannot proceed, it is a deadlock process, and then the entire process is blocked (as $\delta \between x = \delta$ follows from $CM2$). Axioms $CM5$, $CM6$ and $CM7$ capture a similar idea behind the communication merge operator: the first action performed by $x \mid y$ has to be a communication action of x and y. Axiom CF gives the basic step of the communication operator by relating the communication merge operator applied on atomic actions and the communication function γ defined also on pairs of atomic actions. $CM4$, $CM8$ and $CM9$ express that the left merge is right distributive and that the communication merge left and right distributes over the alternative composition. Note that axioms $CM1$, $CM8$ and $CM9$ will be modified later in the probabilistic setting. Axioms $D3$ express that encapsulation of an alternative composition is an alternative composition of encapsulation applied on the two alternatives. In other words, the encapsulation operator distributes over the alternative composition. Axiom $D4$ expresses that the encapsulation operator distributes over the se-

$a \mid b$	=	$\gamma(a, b)$		CF
$x \parallel y$	=	$x \between y + y \between x + x \mid y$		$CM1$
$a \between x$	=	$a \cdot x$		$CM2$
$a \cdot x \between y$	=	$a \cdot (x \parallel y)$		$CM3$
$(x + y) \between z$	=	$x \between z + y \between z$		$CM4$
$a \mid b \cdot x$	=	$(a \mid b) \cdot x$		$CM5$
$a \cdot x \mid b$	=	$(a \mid b) \cdot x$		$CM6$
$a \cdot x \mid b \cdot y$	=	$(a \mid b) \cdot (x \parallel y)$		$CM7$
$(x + y) \mid z$	=	$x \mid z + y \mid z$		$CM8$
$z \mid (x + y)$	=	$z \mid x + z \mid y$		$CM9$
$\partial_H(a)$	=	a	if $a \notin H$	$D1$
$\partial_H(a)$	=	δ	if $a \in H$	$D2$
$\partial_H(x + y)$	=	$\partial_H(x) + \partial_H(y)$		$D3$
$\partial_H(x \cdot y)$	=	$\partial_H(x) \cdot \partial_H(y)$		$D4$

Table 2.4: Additional axioms for *ACP*.

quential composition operator. Thus, in a case of closed or guarded terms after a finite number of times these axioms are applied encapsulation takes as an argument a constant. At this level either $D1$ or $D2$ can be applied.

In the previous section, we mentioned that the constants in A and the constant δ if included, together with operators $\cdot$ and $+$ are considered as basic operators. It is due to the fact that every closed term that contains other operators, added to the signature of $BPA_{(\delta)}$ (in order to obtain an extension of this algebra), can be rewritten by means of the axioms into a closed term that contains only the basic operators. The following theorem formulates that *ACP* possesses this property, namely, the operators that extend the signature of BPA_δ to the signature of *ACP*, just being introduced, can be eliminated from every closed term of *ACP*. The formal definition of the elimination property is given on page 27. Here the symbol $\vdash$ denotes that the equation on the right side of the symbol can be derived by means of the axioms of the algebra which is on the left side of the symbol.

Theorem 2.1.3 (*Elimination theorem of ACP*). Let p be a closed *ACP* term. Then there is a closed BPA_δ term q such that $ACP \vdash p = q$. □

Example 2.1.4. Back to the example with the faulty channel, using *ACP* we can go a step further and model the two communications that happen when a datum is read on one end of the channel and when the datum is sent out on the other end of the channel. Thus, if there are very simple processes, say S and R, the first which brings a datum to the channel and the second that accepts the delivered message from the channel, they are described by terms s_f and r_t where s_f is a new constant that stands for an atomic action meaning "send a datum through the channel" and r_t is a new constant that stands for an atomic action meaning "receive a message from the channel". Then $S \parallel Ch \parallel R$ represents a process that sends a message from S to R which is possibly not delivered correctly. The communication function is defined as: $\gamma(s_f, r_f) = c_f$, $\gamma(s_t, r_t) = c_t$ and for any other pair it gets

value δ. Note that the set of constants A is now extended with s_f, r_t, c_f and c_t. By means of the axioms taking $H = \{s_f, r_f, s_t, r_t\}$ we derive the following equation:

$\partial_H(S \parallel Ch \parallel R) = c_f \cdot (c_t + d \cdot \delta)$.

If the message gets damaged during the delivery process, R does not accept it. In other words, no communication is then established between processes Ch and R. This is expressed by the sub-term $d \cdot \delta$; after a corruption of the message the process deadlocks. Note that the original term has been reduced to a term containing only basic operators.

2.1.3 Recursion and projection

In Example 2.1.2 and 2.1.4 the processes specified by terms of *BPA*$_\delta$ and *ACP* are finite; after finitely many steps they terminate. Of course in reality a communication protocol should be designed such that it can broadcast a sequence of messages, possibly an unbounded sequence. After one message is transferred, it has to be able to continue with the next message, and so on. In other words, we need to make our process algebra powerful enough to model processes that show infinite behaviour.

An algebraic concept of infinite processes is based on the notion of recursion, recursive equations and process variables. When a recursive equation is interpreted in a certain model of the relevant process algebra, the process variables which are part of it take processes as values. Those processes that when substitute for the process variables make the interpretation of the recursive equation valid in the model are called a solution of the recursive equation. Of course, certain recursive equations do not have finite processes as their solution. Thus we come to the key of our problem: infinite processes are introduced as solutions of a (set of) recursive equation(s) in a suitable model of the considered process theory.

Very often if we deal with recursion and infinite processes the notion of projection is introduced because it facilitates the coping with infinite processes. The idea behind the projection is to observe the behaviour of one process (finite or infinite) till a certain moment (in the sense of number of action occurrences). In fact, the finite processes are not an interesting subject to be treated by projection; sooner or later they exhaust all possible actions and terminate. On the other hand, the infinite processes cannot be observed as a whole, but only their finite parts constituted of atomic actions or deadlock. This is exactly what projection offers: it gives the finite sub-processes of an infinite process.

The notion of projection in process algebra is introduced by a new operator $\Pi_n(p), n \geq 1$, called the projection operator[2]. The term $\Pi_n(p)$, represents a process which performs the same actions as p but at most n steps can be executed. The projection operator, Π_n is defined as an unary operator by the axioms in Table 2.5 where a ranges over A (or A_δ if *BPA*$_\delta$ is considered). Since it is meant to generate the finite approximations of infinite processes, this operator (or the set of operators) is included mainly if solutions of recursive specifications are considered in the model. By *BPA* $+ PR$ (*BPA*$_\delta + PR$) we denote a theory obtained from *BPA* (*BPA*$_\delta$) by adding the projection operators Π_n, $n \geq 1$, and the relevant axioms. We believe that the axioms do not need additional explanation. Neither does the theorem below. More properties and a thorough discussion of projection will be carried out in Section 3.3.2.

Theorem 2.1.5 (*Elimination of the projection operator*). If s is a closed *BPA*$_{(\delta)} + PR$ term then there exists a basic *BPA*$_{(\delta)}$ term t such that *BPA*$_{(\delta)} + PR \vdash s = t$. □

Using recursion we can improve the specification of our communication channel.

[2]A usual notation for the projection operator is π_n, but since we use π as a variable ranging over probabilities, we introduce a new notation for this operator.

$\Pi_n(a)$	=	a	$PR1$
$\Pi_1(a \cdot x)$	=	a	$PR2$
$\Pi_{n+1}(a \cdot x)$	=	$a \cdot \Pi_n(x)$	$PR3$
$\Pi_n(x + y)$	=	$\Pi_n(x) + \Pi_n(y)$	$PR4$

Table 2.5: Axioms for projection operator ($n \geq 1$).

Example 2.1.6. The specification in Example 2.1.4 defined a communication protocol that transmits only one message. Now we change the specification in the following way:
$S = s_f \cdot S$
$R = r_t \cdot R$ and
$Ch = r_f \cdot (s_t + d) \cdot Ch$,
where S, R and Ch are process variables. The recursive equation $S = s_f \cdot S$ defines a process that does action "send a frame" denoted by the constant s_f and afterwards behaves the same as the process before the execution this action; clearly it is a process that keeps on sending frames. Likewise, we interpret the recursive equations for R and Ch. Note that this specification abstracts from the contents of the message. Also at this point it is beyond our interest to discuss the properties of the processes defined by these equations.

In addition we observe from the example above the structure of the given equations. Namely, the left-hand side of every equation contains only a variable, and the right-hand side is a term that contains a variable (in this case it is only one variable but in general it may contain more than one variable). We can also detect that every occurrence of a variable on the right-hand sides of the equations is prefixed by an atomic action or by a closed term (in the case of Ch). If a recursive equation has such a structure we say that it is *guarded*. On the other hand, there is the concept of unguarded recursion. Take the equation $X = X$, for example. In every model whose domain has more than one element, this equation has more than one solution. Since we tend to the idea that every recursive specification defines a unique process, unguarded recursion is not desired in our concept of recursion. In [27], the authors show that in the term model and the graph model (to be discussed later in this chapter) of *BPA* and *ACP* every guarded recursive specification has a unique solution. We come to this issue once again in Chapter 3 where we investigate it for probabilistic process algebras.

The formal characterization of the notion of guardedness is given in Section 3.3. Although there, it is considered in a probabilistic setting, the reader can easily derive the relevant definitions for the non-probabilistic setting from the given ones.

2.1.4 Discrete time extension(s)

Timed process algebras [24] are certain process algebras which incorporate information about time. A usual way to do so is to add new operators that allow the explicit specification of timing aspects. In Chapter 5, we follow the discrete-time approach where time is discrete: time is divided into an infinite number of time slices. Events can occur within such a time slice; also, a process can idle for a certain number of time slices. This approach is taken in [19, 20, 108, 6] and also [22].

Another way to introduce time is to parametrize atomic actions with non-negative real numbers that represent the moment of execution. Algebras that model the passing of time as a continuous value are called real-time process algebras. This type of process algebras are for example presented

in [16, 22, 23].

Discrete-time methods are as expected less expressive than real-time ones, but, on the other hand, they are less complex and still expressive enough for practical purposes. As is shown in [42] and [108], discrete time process algebra can be successfully applied in the analysis of real-life problems.

We briefly sketch a possible way to extend BPA_δ and *ACP* to discrete time process algebras with relative timing. The model we present is based on the model defined in [108] and references given there. In Chapter 5 it will be the basic model on top of which we build a probabilistic time theory.

Timed process algebras that are presented here are $BPA^-_{drt} - ID$ and $ACP^-_{drt} - ID$; the latter one as an extension of the former one by the merge operator. $BPA^-_{drt} - ID$ extends BPA_δ with two new operators: the time-unit delay operator σ_{rel} and the "now" operator ν_{rel}. The operator σ_{rel} is introduced to make the passage of time explicit: term $\sigma_{rel}(p)$ represents a process which is postponed for one time unit and then it behaves like p. The term $\nu_{rel}(p)$ represents the sub-process of p which starts its activities in the current time slice; all activities of p that idle are not included in $\nu_{rel}(p)$.

For a given set of atomic actions A, $BPA^-_{drt} - ID$ has signature $\Sigma_{BPA^-_{drt}-ID} = \big(\{\underline{\underline{a}} : a \in A_\delta\}, +, \cdot, \sigma_{rel}, \nu_{rel}\big)$. The constant $\underline{\underline{a}}$, called undelayable action, denotes a process which executes a in the same time slice it is initialized and then it terminates. Note that it cannot be passed on to the next time slice: it gets lost at the moment the next time slice starts.

The axioms of $BPA^-_{drt} - ID$ are given in Table 2.1+2.6+2.7. The most interesting fresh axioms

$\sigma_{rel}(x) + \sigma_{rel}(y)$	=	$\sigma_{rel}(x + y)$	$DRT1$
$\sigma_{rel}(x) \cdot y$	=	$\sigma_{rel}(x \cdot y)$	$DRT2$
$\nu_{rel}(\underline{\underline{a}})$	=	$\underline{\underline{a}}$	$DCS1$
$\nu_{rel}(x + y)$	=	$\nu_{rel}(x) + \nu_{rel}(y)$	$DCS2$
$\nu_{rel}(x \cdot y)$	=	$\nu_{rel}(x) \cdot y$	$DCS3$
$\nu_{rel}(\sigma_{rel}(x))$	=	$\underline{\underline{\delta}}$	$DCS4$

Table 2.6: Axioms for the time operators.

$x + \underline{\underline{\delta}}$	=	x	$DRT3$
$\underline{\underline{\delta}} \cdot x$	=	$\underline{\underline{\delta}}$	$DRT4$

Table 2.7: Axioms for the undelayable deadlock.

will be discussed in short. Axiom $DRT1$ expresses that time passage does not determine a choice. In other words, no sub-process that can idle till the next time slice gets lost when the next time slice is initialized. Axiom $DRT2$ captures the relative-timing character of the theory. It means that the moments at which certain actions occur are relative with respect to the previous action executed by the same process. Thus, if the prefix x idles till the next time slice then the complete remaining part of the process also idles till the next time slice, irrespective of the scope of the time-unit delay operator. Axiom $DCS1$ expresses that an undelayable action always starts in the current time slice. Axiom $DCS2$ expresses that the part of $x + y$ that starts in the current time slice consists of the alternative composition of the parts of x and y that starts in the current time slice. Axiom $DCS3$ expresses that the part of $x \cdot y$ that starts in the current time slice consists of the part of x that starts in the current time slice, followed by y. Axiom $DCS4$ expresses that $\sigma_{rel}(x)$ cannot start in the current time slice.

$ACP^-_{drt} - ID$ is a discrete time process algebra with the notion of parallel composition that can be seen as a combination of $BPA^-_{drt} - ID$ and *ACP*. Its signature contains the constants and the operators of $BPA^-_{drt} - ID$ and the operators of *ACP*. The set of axioms for the merge and encapsulation operators in discrete time setting and the auxiliary operators are shown in Table 2.8 and together with the axioms in Table 2.1+2.6+2.7 (the axioms of $BPA^-_{drt} - ID$) constitute the axiom system of $ACP^-_{drt} - ID$.

$\underline{\underline{a}} \mid \underline{\underline{b}}$	=	$\underline{\underline{\gamma(a,b)}}$		$DRTCF$
$x \parallel y$	=	$x \between y + y \between x + x \mid y$		$CM1$
$\underline{\underline{a}} \mid \underline{\underline{b}} \cdot x$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot x$		$DRTCM2$
$\underline{\underline{a}} \cdot x \mid \underline{\underline{b}}$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot x$		$DRTCM3$
$\underline{\underline{a}} \cdot x \mid \underline{\underline{b}} \cdot y$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot (x \parallel y)$		$DRTCM4$
$\sigma_{rel}(x) \mid \nu_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTCM5$
$\nu_{rel}(x) \mid \sigma_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTCM6$
$\sigma_{rel}(x) \mid \sigma_{rel}(y)$	=	$\sigma_{rel}(x \mid y)$		$DRTCM7$
$(x + y) \mid z$	=	$x \mid z + y \mid z$		$CM8$
$z \mid (x + y)$	=	$z \mid x + z \mid y$		$CM9$
$\underline{\underline{a}} \between x$	=	$\underline{\underline{a}} \cdot x$		$DRTM2$
$\underline{\underline{a}} \cdot x \between y$	=	$\underline{\underline{a}} \cdot (x \parallel y)$		$DRTM3$
$(x + y) \between z$	=	$x \between z + y \between z$		$DRTM4$
$\sigma_{rel}(x) \between \nu_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTM5$
$\sigma_{rel}(x) \between (\nu_{rel}(y) + \sigma_{rel}(z))$	=	$\sigma_{rel}(x \between z)$		$DRTM6$
$\partial_H(\underline{\underline{a}})$	=	$\underline{\underline{a}}$	if $a \notin H$	$DRTD1$
$\partial_H(\underline{\underline{a}})$	=	$\underline{\underline{\delta}}$	if $a \in H$	$DRTD2$
$\partial_H(x + y)$	=	$\partial_H(x) + \partial_H(y)$		$D3$
$\partial_H(x \cdot y)$	=	$\partial_H(x) \cdot \partial_H(y)$		$D4$
$\partial_H(\sigma_{rel}(x))$	=	$\sigma_{rel}(\partial_H(x))$		$DRTD5$

Table 2.8: Additional axioms for $ACP^{-}_{drt} - ID$.

Many axioms in Table 2.8 represent timed counterparts of axioms of *ACP* where the untimed action a is replaced by the undelayable action $\underline{\underline{a}}$. Axioms $DRTM5$ and $DRTM6$ describe the time-step behaviour of the left merge operator. If the left argument of the left merge must idle but the right argument cannot then the entire process ends up in an undelayable deadlock, as the right argument cannot be passed on to the next time slice, which actually the left argument tries to do. However, if the right argument contains a summand that can idle together with the left argument then the time step can be done but the summands of the right component that cannot idle are discarded. Axioms $DRTCM5-7$ express that two processes can communicate only if they perform the actions on which they synchronize in the same time slice.

In [108] new constants denoting delayable atomic actions are added to $BPA^{-}_{drt} - ID$ and $ACP^{-}_{drt} - ID$. But the full axiomatization of delayable processes in general requires a new operator. However, in the discrete-time probabilistic process algebra with delayable actions presented in this thesis (Chapter 5) we take a different approach which does not need a new operator. In other words, the probabilistic process algebra with discrete time and delayable actions does not constitute an extension of the discrete-time process algebra with delayable actions in [108]. For that reason we

do not show more details of the latter. In the notation used above the superscript $-$ stands for the absence of delayable actions[3].

Example 2.1.7. The specification given in Example 2.1.6 abstracts from any timing aspects of the processes involved. In fact, process R as specified waits for a message sent by S for an unspecified period of time. The specification only describes that if S sends a message R eventually receives it, unless it gets damaged. If we think about a situation in which process R is not tremendously patient but it waits for a message a limited period of time, say d time slices, then process R is specified as follows:
$R = \big(\underline{\underline{r_t}} + \sigma^1_{rel}(\underline{\underline{r_t}}) + \sigma^2_{rel}(\underline{\underline{r_t}}) + \ldots \sigma^d_{rel}(\underline{\underline{r_t}})\big) \cdot R + \sigma^{d+1}_{rel}(\underline{\underline{patience\_out}})$,
where $\sigma^i_{rel}(p)$ denotes that σ_{rel} is applied i times. Thus, if S sends a message during (or after) the $d+1$ time slice even though Ch may deliver it correctly to R and without any delay, since R is not ready to receive that message the whole process deadlocks.

2.2 Model(s) - operational semantics

Given a set of axioms of a certain process algebra PRA, it is possible to construct a model: a mathematical structure in which all operators of PRA have an interpretation and all axioms of PRA are obeyed. Such a model usually is called a semantics of PRA. It is worth to highlight that one of the aims of process algebra as a formal method is to develop a theory (method) that can be used in different models. Anyway, in the literature there is a tendency to use a model based on a term-deduction system (also called an operational semantics), called term model, or a model based on a graph representation, called a graph model. Even though the interpretation of terms of PRA differs in both models (the domain of the term model consists of terms which can perform transitions according to some given deduction rules, and in the graph model it consists of graphs and each graph is assigned a relation (relations) over its set of states which defines transitions), they are very strongly related because they are both based on a notion of bisimulation. It is not a surprising result in [27] that the term model and the graph model of ***BPA*** $+ PR$ are isomorphic. In most of the cases occurring in the thesis, we will work with the term model, except in Chapter 6 where we switch to the graph model. We leave the introduction of the graph model for later and now we focus on the term models for the theories presented in Section 2.1 - 2.7, from now on called the bisimulation model.

2.2.1 Stepwise construction of models

In order to give the main idea about constructing of the bisimulation model of a certain process algebra PRA we present the main ingredients and the stepwise procedure of building up such a model. Without going into many details, the bisimulation model of ***BPA*** will be defined and then it will be extended to a model of any other algebra mentioned before.

1. The domain of the model is defined and its elements are called processes[4]. It may contain only finite processes in which case we write $\mathbb{PT}(PRA)$ and we talk about a bisimulation model of finite processes of PRA. The domain of $\mathbb{PT}(PRA)$ coincides with the set of closed terms

[3]Extension $-ID$ stands for the absence of a special constant denoting immediate deadlock. In this thesis we do not deal with this constant.

[4]Usually, in the term model they are called process terms or process expressions and in the graph model they are called process graphs.

over the signature of PRA without recursion. But in addition it may contain infinite processes, which are introduced as solutions of guarded recursive specifications over PRA. In that case, the set of processes is expanded by new constants, one for each solution of a guarded recursive specification. Thus, $< X|E >$ is a new constant denoting the solution of the guarded recursive specification E with X as the root variable. In this case, we write explicitly $\mathbb{PT}^{\infty}(PRA)$. We write $\mathbb{PT}^{(\infty)}(PRA)$ if a given statement holds for both $\mathbb{PT}(PRA)$ and $\mathbb{PT}^{\infty}(PRA)$. It is also quite obvious that $\mathbb{PT}(PRA) \subseteq \mathbb{PT}^{\infty}(PRA)$.

2. Transition relations, that actually describe process activities, are defined by means of deductive rules given (usually) in Plotkin style (citePlo81. These rules define the way the transitions that a process p can possibly perform, are characterized by the transitions of the sub-processes of p. For the process algebras from Section 2.1 - 2.7 three types of transitions are used: $\xrightarrow{a}$ - an action transition, $\xrightarrow{a} \surd$ - an action termination (for $a \in A$) and in the semantics of timed systems the the time transition $\xrightarrow{\sigma}$ is added[5]. The intended meaning of a transition $p \xrightarrow{a} q$ is that process p can perform an action a and then it behaves like process q. Transition $p \xrightarrow{a} \surd$ denotes that process p can terminate by performing an action a. When building the bisimulation models of the probabilistic process algebras a new type of transition will be introduced.

3. By having a method to describe process behaviour it becomes possible to relate and compare two processes whose behaviour is described in the same semantics. Especially it is very important to decide whether two processes behave in the same manner, or in other words, decide whether they are equivalent. If two processes show equivalent behaviour then one of them could be replaced by the other one as part of a bigger system (up to some additional consideration). In such a way instead of a large system a significantly smaller system that shows the same behaviour can be investigated.

Many different equivalence relations have been defined, each of them treating different aspects of the behaviour of systems. A broad overview of different semantics and their comparisons can be found in [57, 61]. A bisimulation [89, 93, 31], on which we focus in this thesis, relates those processes that can match each other on every transition; after they both execute the same action the processes reached have to be related as well.

As mentioned before, one of the reasons to equate processes is our intention to replace a process by an equivalent one in a given context. But in order to do so the equivalence relation has to satisfy certain properties: it has to be preserved by all operators of PRA, in other words, it has to be a *congruence*. This property is stated in a so-called congruence theorem which in this thesis will be formulated and proved for every presented process algebra and its semantics.

4. The bisimulation model of finite processes $\mathcal{M}_{PRA}$ has as a domain the quotient set $\mathbb{PT}(PRA)/\underline{\leftrightarrow}$. The bisimulation model of infinite processes $\mathcal{M}^{\infty}_{PRA}$ has as a domain the quotient set $\mathbb{PT}^{\infty}(PRA)/\underline{\leftrightarrow}$.

5. We say that PRA is complete for the model $\mathcal{M}_{PRA}$ if for every two processes that are bisimilar in the model, the terms that represent them in PRA can be proved equal using the axioms in PRA. In many cases the completeness property does not hold in general for all processes, but only for finite processes that correspond to the closed terms in PRA. Therefore, the completeness property can be formulated as: if p and q are closed PRA terms, then $p \underline{\leftrightarrow} q \Rightarrow PRA \vdash p = q$.

[5]While $\xrightarrow{a}$ and $\xrightarrow{\sigma}$ represent binary relations on the set of processes, $\xrightarrow{a} \surd$ is a predicate on that set.

Below we give the formal definition of a (strong) bisimulation relation: the equivalence relation from which the quotient sets mentioned in **4.** are obtained. For the untimed process algebras, *BPA*$(+PR)$, *BPA*$_\delta(+PR)$, *ACP* only the clauses 1. and 2. are considered in the definition. The definition of a bisimulation relation for discrete time process algebras has additionally the last clause included.

Definition 2.2.1. Let R be a symmetric relation on the set $\mathbb{PT}^{(\infty)}(PRA)$ such that:

1. If $(s,t) \in R$ and $s \xrightarrow{a} p$ for some $a \in A$, then there exists q such that $t \xrightarrow{a} q$ and $(p,q) \in R$;
2. If $(s,t) \in R$ and $s \xrightarrow{a} \surd$, then $t \xrightarrow{a} \surd$;
3. If $(s,t) \in R$ and $s \xrightarrow{\sigma} p$, then there exists q such that $t \xrightarrow{\sigma} q$ and $(p,q) \in R$. [6]

We say that R is a (strong) bisimulation. Processes s and t are bisimilar, $s \leftrightarrows t$, if there exists a bisimulation R such that $(s,t) \in R$.

2.2.2 Model of *BPA*

The deduction rules for the bisimulation model of *BPA* are given in Table 2.9 where a is a variable that ranges over A. We read the rules in the following way, for instance, the fourth rule reads: if process x can perform a and afterwards behaves as x', then process $x+y$, for any y, can perform a as well and afterwards it becomes x'. Thus, the activities of the smaller process x influence the activities of the bigger process $x+y$. One can notice that this rule has two conclusions: $x+y \xrightarrow{a} x'$ and $y+x \xrightarrow{a} x'$. This means that if the hypothesis of the rule, in this case $x \xrightarrow{a} x'$ is true then both conclusions are true as well. Actually, this is an abbreviation for two rules, namely, $\dfrac{x \xrightarrow{a} x'}{x+y \xrightarrow{a} x'}$ and $\dfrac{x \xrightarrow{a} x'}{y+x \xrightarrow{a} x'}$.

This is the basic term-deduction system from which any other model is obtained by extension. In [27] it is proved that the bisimulation model of finite processes is a model of *BPA* that is complete for closed terms.

$$a \xrightarrow{a} \surd$$

$$\frac{x \xrightarrow{a} x'}{x \cdot y \xrightarrow{a} x' \cdot y} \qquad \frac{x \xrightarrow{a} \surd}{x \cdot y \xrightarrow{a} y}$$

$$\frac{x \xrightarrow{a} x'}{x+y \xrightarrow{a} x', y+x \xrightarrow{a} x'} \qquad \frac{x \xrightarrow{a} \surd}{x+y \xrightarrow{a} \surd, y+x \xrightarrow{a} \surd}$$

Table 2.9: Deduction rules for action transitions for *BPA*.

[6] This clause is included only for discrete time process algebras.

2.2.3 Model of *BPA* + PR

The term-deduction system of *BPA* + PR is defined by the rules of *BPA* and the deduction rules for the projection operator in Table 2.10. As we have mentioned, it is common to have projection in a model if infinite processes are also part of it. Hence, we talk about the bisimulation model of *BPA* + PR which contains infinite processes and therefore the rules given in Table 2.11 are added to the term-deduction system.

The rules for the projection operator are rather intuitive. In the deduction rules for recursion (in Table 2.11) by $< t_X|E >$ we denote the right-hand side of the equation $X = t_X$ in E with constants $< Y|E >$ substituted for variables Y. Recall that, if E is a guarded specification, $< Y|E >$ exists for every Y variable in E. These deduction rules express that the behaviour of process $< X|E >$ is determined by the behaviour of the process represented by the right-hand side of the equation of X in E. In [27] it is shown that in the bisimulation model with infinite processes of *BPA* + PR every guarded specification has a unique solution (a property later defined by means of recursive principles).

$$\frac{x \xrightarrow{a} x'}{\Pi_{n+1}(x) \xrightarrow{a} \Pi_n(x')} \qquad \frac{x \xrightarrow{a} \surd}{\Pi_n(x) \xrightarrow{a} \surd} \qquad \frac{x \xrightarrow{a} x'}{\Pi_1(x) \xrightarrow{a} \surd}$$

Table 2.10: Action transitions for projection

$$\frac{\langle t_X|E\rangle \xrightarrow{a} x}{\langle X|E\rangle \xrightarrow{a} x} \qquad \frac{\langle t_X|E\rangle \xrightarrow{a} \surd}{\langle X|E\rangle \xrightarrow{a} \surd}$$

Table 2.11: Action transitions for recursion.

Example 2.2.2. Consider once again the equation $Ch = r_f \cdot (s_t + d) \cdot Ch$ of Example 2.1.6. We rewrite it as a recursive specification E with two equations:
$Ch = r_f \cdot Ch_m$
$Ch_m = (s_t + d) \cdot Ch$.
Then by $< Ch|E >$ and $< Ch_m|E >$ we denote the processes that constitute the solution of E. They behave in the following way: $< Ch|E > \xrightarrow{r_f} < Ch_m|E >$ and this is the only transition that $< Ch|E >$ can perform; $< Ch_m|E > \xrightarrow{s_t} < Ch|E >$ and $< Ch_m|E > \xrightarrow{d} < Ch|E >$. We agree that this representation is not always easy to follow. For that reason in Figure 2.1 we show a graphical representation of the behaviour of the process $< Ch|E >$ (the process defined by E when Ch is the root variable). State 1 corresponds to the process $< Ch|E >$ and state 2 corresponds to the process $< Ch_m|E >$.

2.2.4 Model of *ACP*

The operational semantics of *ACP* is defined by the deduction rules of *BPA* (Table 2.9) together with the rules of the additional operators of *ACP* given in Table 2.12, where a, b, c range over A and $H \subseteq A$.

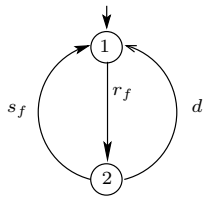


Figure 2.1: Transition system representation of the process $< Ch|E >$.

The deduction rules in Table 2.12 express the interleaving characterization of the parallel composition. If one component of the parallel composition can perform an action a then the same holds for the entire process. If the components can synchronize on an atomic action c then the parallel composition can perform a c transition. Note that the left merge and the communication merge are not used to define the deduction rules for the merge operator. They were only needed in the axiomatization.

In the bisimulation model of *ACP* with recursion, every guarded specification has a unique solution. The model of finite processes is complete for the theory *ACP* (see e.g. [27]).

$$\frac{x \xrightarrow{a} x'}{x \parallel y \xrightarrow{a} x' \parallel y,\ y \parallel x \xrightarrow{a} y \parallel x'} \qquad \frac{x \xrightarrow{a} \surd}{x \parallel y \xrightarrow{a} y,\ y \parallel x \xrightarrow{a} y} \qquad \frac{x \xrightarrow{a} x', y \xrightarrow{b} y', \gamma(a,b) = c}{x \parallel y \xrightarrow{c} x' \parallel y'}$$

$$\frac{x \xrightarrow{a} x', y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \parallel y \xrightarrow{c} x', y \parallel x \xrightarrow{c} x'} \qquad \frac{x \xrightarrow{a} \surd, y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \parallel y \xrightarrow{c} \surd}$$

$$\frac{x \xrightarrow{a} x'}{x \lfloor\!\lfloor y \xrightarrow{a} x' \parallel y} \qquad \frac{x \xrightarrow{a} \surd}{x \lfloor\!\lfloor y \xrightarrow{a} y}$$

$$\frac{x \xrightarrow{a} x', y \xrightarrow{b} y', \gamma(a,b) = c}{x \mid y \xrightarrow{c} x' \parallel y'} \qquad \frac{x \xrightarrow{a} x', y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \mid y \xrightarrow{c} x', y \mid x \xrightarrow{c} x'} \qquad \frac{x \xrightarrow{a} \surd, y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \mid y \xrightarrow{c} \surd}$$

$$\frac{x \xrightarrow{a} x', a \notin H}{\partial_H(x) \xrightarrow{a} \partial_H(x')} \qquad \frac{x \xrightarrow{a} \surd, a \notin H}{\partial_H(x) \xrightarrow{a} \surd}$$

Table 2.12: Action transitions of *ACP*.

2.2.5 Model of Discrete-Time Process Algebra

The deduction rules that define the bisimulation model of $BPA^{-}_{drt} - ID$ comprise the rules of *BPA* for the operators $+$ and $\cdot$ given in Table 2.9 and the rules for action and time transitions of the additional operators in Table 2.13. Note that the time transitions are included in this term-deduction system. Certainly, the most interesting deduction rules are the ones for time transitions of alternative composition in Table 2.13. Here $y \overset{0}{\not\rightarrow}$ denotes that process y cannot idle. (More about negative premises will be said in the following section.) The rule containing this premise expresses that if summand y of the alternative composition cannot do a time transition but the other summand x can, then the alternative

composition can do a time transition to the process reached from x by performing the transition. If both summands can do a time transition then they do so synchronously.

Result concerning infinite processes and recursive principles in this theory can be found in [23].

The term-deduction system of $ACP^-_{drt} - ID$ contains the deduction rules of $BPA^-_{drt} - ID$ (Table 2.9+2.13), the rules for action transitions of *ACP* in Table 2.12 and the rules for time transitions of the merge operators and the encapsulation operator given in Table 2.14. The additional rules define time transitions for the merge operators and the encapsulation operator. For the merge operators we can observe that composition (parallel, left merge or communication) of two processes can do a time transition only if both components can do it as well.

$$\underline{\underline{a}} \xrightarrow{a} \surd$$

$$\frac{x \xrightarrow{a} x'}{\nu_{rel}(x) \xrightarrow{a} x'} \qquad \frac{x \xrightarrow{a} \surd}{\nu_{rel}(x) \xrightarrow{a} \surd}$$

$$\sigma_{rel}(x) \xrightarrow{\sigma} x \qquad \frac{x \xrightarrow{\sigma} x', y \not\xrightarrow{\sigma}}{x + y \xrightarrow{\sigma} x', y + x \xrightarrow{\sigma} x'}$$

$$\frac{x \xrightarrow{\sigma} x', y \xrightarrow{\sigma} y'}{x + y \xrightarrow{\sigma} x' + y'} \qquad \frac{x \xrightarrow{\sigma} x'}{x \cdot y \xrightarrow{\sigma} x' \cdot y}$$

Table 2.13: Additional rules of *BPA* with discrete-time.

$$\frac{x \xrightarrow{\sigma} x', y \xrightarrow{\sigma} y'}{x \parallel y \xrightarrow{\sigma} x' \parallel y'} \qquad \frac{x \xrightarrow{\sigma} x', y \xrightarrow{\sigma} y'}{x \lfloor\!\lfloor y \xrightarrow{\sigma} x' \lfloor\!\lfloor y'} \qquad \frac{x \xrightarrow{\sigma} x', y \xrightarrow{\sigma} y'}{x \mid y \xrightarrow{\sigma} x' \mid y'} \qquad \frac{x \xrightarrow{\sigma} x'}{\partial_H(x) \xrightarrow{\sigma} \partial_H(x')}$$

Table 2.14: Additional time transition rules of $ACP^-_{drt} - ID$.

2.3 Proof techniques and notation

In this section, we introduce certain notational conventions that will be used through out the thesis. Also we present three methods that will be used later for different purposes: a method based on term-rewriting systems that will be used in proofs of the elimination property; two methods based on analysis of term-deduction systems called a method of stratification and a method of reduction, that will be used in the proofs of a conservative extension property used to prove a completeness property.

Used notation

p versus p Sometimes we will prefer to make a clear distinction between terms in the process algebra PRA and the processes in its model $\mathcal{M}_{PRA}$ (Section 3.3.3 for instance). Thus, for the terms

in PRA we will use bold symbols, $\mathbf{p}, \mathbf{q}, \ldots$ and for the processes in the model we will use italic symbols $p, q, \ldots$. Many times without mentioning it we presume that x is an interpretation of $\mathbf{x}$. But, if it is clear from the context which objects we deal with, we use uniformly italic symbols for both.

Summation convention We will use the notation $\sum_{i \in I} t_i$ to denote the summation over some finite index set $I = \{1, 2, \ldots, n\}$: $\sum_{i \in I} t_i = t_1 + t_2 + \ldots + t_n$. The summation over the empty set equals δ: $\sum_{i \in \emptyset} t_i = \delta$.

Operators over sets Let Σ be a signature. By $\mathbb{O}(\Sigma)$ we denote the set of terms over Σ. $\mathbb{C}(\Sigma)$ denotes the set of closed terms over Σ.

If $K_1, K_2, \ldots, K_n, n \geq 1$ are subsets of terms over Σ and f is an n-ary operator in Σ, then we define: $f(K_1, K_2, \ldots, K_n) = \{f(k_1, k_2, \ldots, k_n) \ : \ k_i \in K_i, 1 \leq i \leq n\}$.

Number of symbols If s is a closed term over Σ, by $op(s)$ we denote the number of operators in s defined as:

1. if s is a constant, then $op(s) = 1$;
2. if f_n is an n-ary operator in Σ (for $n \geq 1$) and $s \equiv f_n(s_1, s_2, \ldots, s_n)$ for closed terms $s_1, s_2, \ldots, s_n$, then $op(s) = op(s_1) + op(s_2) + \ldots + op(s_n) + 1$.

By $n_g(s)$ we denote the number of occurrences of the operator g in closed term s defined as: if g is an m-ary operator in Σ, then

1. if s is a constant, $m = 0$ and $s \equiv g$ then $n_g(s) = 1$; otherwise $n_g(s) = 0$;
2. if f_n is an n-ary operator in Σ (for $n \geq 1$), $g \not\equiv f_n$ and $s \equiv f_n(s_1, s_2, \ldots, s_n)$ for closed terms $s_1, s_2, \ldots, s_n$, then $n_g(s) = n_g(s_1) + n_g(s_2) + \ldots + n_g(s_n)$;
3. if $s \equiv g(s_1, s_2, \ldots, s_m)$ for closed terms $s_1, s_2, \ldots, s_m$, then $n_g(s) = n_g(s_1) + n_g(s_2) + \ldots + n_g(s_m) + 1$.

Action transitions In many given proofs we do not write down the parts which treat the action transitions of the considered processes. These parts very much resemble the investigation of action transitions done in the standard process algebras *BPA* and *ACP*. For example, on page 67 in the proof of the Soundness theorem, we should prove that two processes $(u + v) + w$ and $u + (v + w)$ simulate each other on action transitions. But this proof can be found in [27].

Closure of relations If α is a relation defined on set S, then by $Eq(\alpha)$ we denote the equivalence closure of α on S.

If $\xrightarrow{l}$ is a transition relation, by $\stackrel{l}{\Longrightarrow}$ we denote the transitive and reflexive closure of $\xrightarrow{l}$.

Elimination property and a method to prove it The set of axioms of a given process algebra PRA can be transformed into a term rewriting system (TRS) by giving direction to selected axioms in the system. Then every reduction in the TRS corresponds to a derivation in PRA. The elimination to basic terms property in process algebra PRA, formally defined below, expresses that from every

closed term by use of the axioms of PRA a basic term can be derived. If we succeed to transform our axiom system to a TRS in such a way that every reduction step in the TRS corresponds to an application of the associated axiom and every derivation in which at least once an axiom from the set of selected axioms is applied corresponds to a reduction in the TRS, then the problem of proving the elimination property of PRA is transformed into the problem of proving strong termination of the TRS. Furthermore, if the set of normal forms of the TRS is contained in the set of basic terms of the PRA then the proof of the elimination to basic terms property of PRA is completed. In the sequel, we sketch a method called lexicographical path ordering which gives sufficient conditions to reduce the problem of strong normalization to a simple analysis of the rewriting rules in TRS. For details about term rewriting systems and the method of lexicographical path ordering see [26, 83]. We assume that the reader has basic knowledge about TRSs.

Definition 2.3.1. (Elimination property) Let PRA be a process algebra with a defined set of basic terms as a subset of the set of closed terms over PRA. Then PRA has *the elimination to basic terms property* if for every closed term s of PRA there exists basic term t of PRA such that $PRA \vdash s = t$.

Definition 2.3.2. A term s_0 is called *strongly normalizing* if does not exist an infinite series of reductions beginning in s_0. A TRS is called strongly normalizing if every term of it is strongly normalizing.

In fact, strong normalization means that every term can be reduced to a normal form (i.e., a term that cannot be reduced any further). Thus, if the TRS, obtained from our process algebra PRA as described above, is strongly normalizing, the only problem to be treated is to show that the normal form is a basic term. In this way the strong normalization property induces that every term in PRA can be reduced to a basic term. Therefore, when constructing a TRS from axioms of PRA we assume that every axiom of PRA is directed in such a way that it leads to a basic term. For instance, we would have the rewriting rule: $(x + y) \cdot z \rightarrow x \cdot z + y \cdot z$ because the right-hand side needs less reductions to a basic term than the left-hand side. Take for example terms $(a + b) \cdot c$ and $a \cdot c + b \cdot c$.

The key step of the lexicographical path ordering method consists of generating a reduction relation on top of the TRS in a way defined below. Theorem 2.3.4 provides a solution to prove the strong normalization property.

Definition 2.3.3. Let $TR = (\Sigma, R)$ be a TRS. $\mathbb{O}^*(\Sigma)$ denotes a superset of the set of terms over TR, $\mathbb{O}(\Sigma)$ where some symbols in Σ may be marked with *.

Let $s, t \in \mathbb{O}(\Sigma)$. We write $s >_{lpo} t$ if $s \rightarrow^+ t$ where $\rightarrow^+$ is the transitive closure of the reduction relation defined by the rules in Table 2.15 where H and G are symbols in Σ. We assume that $>$ is a given ordering on Σ.

Theorem 2.3.4 (*Strong normalization*). Let $TR = (\Sigma, R)$ be a TRS with finitely many rewriting rules and let $>$ be a well-founded ordering on Σ. If $s >_{lpo} t$ for each rewriting rule $s \rightarrow t \in R$, then the term rewriting system (Σ, R) is strongly normalizing. □

Conservative extension and methods to prove it based on term-deduction systems When developing theories in a modular way it is interesting and important to know whether the same equation in the basic (smaller) theory PRA_0 are preserved in the extended (bigger) theory PRA_1. More precisely, suppose that the signature of PRA_1 is an extension of the signature of PRA_0 and that every axiom of PRA_0 is an axiom of PRA_1. Therefore, the set of terms of PRA_0 is a subset of the set

RPO1.	$H(t_1,\ldots,t_k) \rightarrow H^*(t_1,\ldots,t_k)$, for $k \geq 0$
RPO2.	$H^*(t_1,\ldots,t_k) \rightarrow G(H^*(t_1,\ldots,t_k),\ldots,H^*(t_1,\ldots,t_k))$, for $H > G, k \geq 0$
RPO3.	$H^*(t_1,\ldots,t_k) \rightarrow t_i$, for $k \geq 1, 1 \leq i \leq k$
RPO4.	$H^*(t_1,\ldots,G(s_1,\ldots,s_l),\ldots,t_k) \rightarrow H(t_1,\ldots,G^*(s_1,\ldots,s_l),\ldots,t_k)$, for $k \geq 1, l \geq 0$
RPO5.	$s \rightarrow t \Rightarrow H(\ldots,s,\ldots) \rightarrow H(\ldots,t,\ldots)$
LPO.	$t \equiv H^*(t_1,\ldots,t_{i-1},G(s_1,\ldots,s_l),t_{i+1},\ldots,t_k)$
	$\Rightarrow t \rightarrow H(t,\ldots,t,G^*(s_1,\ldots,s_l),t,\ldots,t)$, for $k \geq 1, 1 \leq i \leq k, l \geq 0$

Table 2.15: Lexicographical path ordering.

of terms of PRA_1. Also, every equation $t = t'$ between some PRA_0 terms t and t', which can be derived in PRA_0 can be derived in PRA_1 as well. If no other equations between terms of PRA_0 can be derived in PRA_1 we say that PRA_1 is a conservative extension of PRA_0. We believe that any further justification of the importance of this property is not needed. The formal definition is given below. It also contains the definition of the elimination property to a basic (smaller) theory.

Definition 2.3.5. Let PRA_1 with a signature Σ_1 be an extension of process algebra PRA_0 with a signature Σ_0. PRA_1 is an *equationally conservative extension* of PRA_0 if for all $s, t \in \mathbb{C}(\Sigma_0)$

$$PRA_1 \vdash s = t \Leftrightarrow PRA_0 \vdash s = t.$$

If for all $s \in \mathbb{C}(\Sigma_1)$ there is a $t \in \mathbb{C}(\Sigma_0)$ such that $PRA_1 \vdash s = t$ we say that PRA_1 possesses the elimination property for PRA_0.

A method to prove the equationally conservative extension property, that will be used in this thesis, has been formulated in [107] (see e.g. [26, 48]). One of the conditions that guarantees this property is an operationally conservative extension property. While the equational conservativity expresses a link between two theories, the operational conservativity expresses a relation between their operational semantics. It expresses that the transitions between process terms of the basic (smaller) semantics are not effected by the extension. In the sequel, we state a theorem that captures the main conditions that guarantee the operationally conservative extension property, preceded by a few basic notions for term-deduction systems.

Formally, a term-deduction system (TDS) is a structure (Σ, D) with Σ a signature and D a set of deduction rules. The set D is parametrized by two sets, the set of predicate symbols, T_p, and the set of relation symbols T_r. For (open) terms s, t, u over the signature Σ, $P \in T_p$ and $R \in T_r$, the expressions Ps, $\neg Ps$, tRu and $t\neg R$ are called *literals* (or *formulas*); Ps and tRu are called positive and $\neg Ps$ and $t\neg R$ are called negative literals. In the TDSs presented earlier in this chapter we used $\xrightarrow{a}$ and $\xrightarrow{\sigma}$ as relation symbols and $\xrightarrow{a}\surd$ as a predicate symbol. A deduction rule $d \in D$ has the form: $\dfrac{prem}{c}$ with $prem$ a set of literals called premises (hypotheses), which can be positive or negative. The set of positive premises is denoted by $pprem(d)$ and the set of negative premises by $nprem(d)$. c is a positive literal, called the conclusion of d, denoted $conc(d)$. If a deduction rule does not contain negative premises we say that it is a *positive* deduction rule; otherwise it is *negative*. If a TDS does not contain deduction rules with negative premises we say that it is a *positive* TDS; otherwise it is *negative*.

If d is a positive rule for which $prem = \{P_j s_j \ : \ j \in J\} \cup \{t_i R_i y_i \ : \ i \in I\}$, for I and J are arbitrary index sets, and the conclusion c has one of the forms: $f(x_1,\ldots,x_n)Rt$ or xRt or

$Pf(x_1, \ldots, x_n)$ or Px, where $t_i, s_j, t \in \mathbb{O}(\Sigma)$, $P_j, P \in T_p$, $R_i, R \in T_r$ for all $i \in I$ and $j \in J$ and where $f \in \Sigma$ is an n-ary function symbol and $x_1, x_2, \ldots, x_n$, x, y_i for $i \in I$, are distinct variables, we say that d is in *path format*. We write $Y = \{y_i : i \in I\}$ and $X = \{x_1, x_2, \ldots, x_n\}$ if c has the form: $f(x_1, \ldots, x_n)Rt$ or $Pf(x_1, \ldots, x_n)$, and $X = \{x\}$ if c has the form xRt or Px. By $var(d)$ we denote the set of all variables occurring in d. If $var(d) = X \cup Y$ we say that d is *pure*. A (positive) TDS is in (pure) path format if all its deduction rules are in (pure) path format. Furthermore, the variables that occur in the premises of d are related in the following way: $x \to y$ iff there is a $tRs \in prem(d)$ such that $x \in var(t)$ and $y \in ar(s)$. If for a given rule d there are no infinite backward chains of variables related by the relation $\to$ we say that d is *well-founded*. A TDS s well-founded if all its rules are well-founded.

An extension of TDS $T^0 = (\Sigma_0, D_0)$ with a TDS $T^1 = (\Sigma_1, D_1)$ is defined through an extension of its signature and the set of deduction rules. The signature Σ_1 can extend Σ_0 only if it preserves the arity of the operators of Σ_0; if f is an operator in both signatures, then it has the same arity in both of them. The extended signature is denoted by $\Sigma_0 \oplus \Sigma_1$. Then, the extension of T^0 with T^1, denoted by $T^0 \oplus T^1$, is defined as $(\Sigma_0 \oplus \Sigma_1, D_0 \cup D_1)$. Let $T(\Sigma, D) = T^0 \oplus T^1$ be an extension of $T^0 = (\Sigma_0, D_0)$ with $T^1 = (\Sigma_1, D_1)$ and let $D = D(T_p, T_r)$.

Definition 2.3.6. The term-deduction system T is an *operationally conservative extension* of T^0 if for all $s, u \in \mathbb{C}(\Sigma_0)$, for all relation symbols $R \in T_r$ and predicate symbols $P \in T_p$, and for all $t \in \mathbb{C}(\Sigma)$ we have

sRt in T if and only if sRt in T^0, and

Pu in T if and only if Pu in T^0.

We observe that the definition of operationally conservative extension only includes preserving transitions of one process from T^0 when it is considered as a process in the extended system T. However, we said that every operational semantics involves an equivalence relation, in our case bisimulation, that equals processes on the semantical level. Naturally, when T^0 is extended to T, the equivalence relation, say $\approx_{T^0}$, defined on T^0 is lifted to an equivalence relation on T, say $\approx_T$. The operationally conservative extension of T_0 up to $\approx_{T^0}$ means that $\approx_T$ restricted on terms on T_0 equals $\approx_{T^0}$; terms of T_0 cannot be related by $\approx_T$ if they are not related by $\approx_{T^0}$. Formally,

Definition 2.3.7. If for all $s, t \in \mathbb{C}(\Sigma_0)$, $s \approx_T t$ iff $s \approx_{T^0} t$ we say that T is an *operationally conservative extension f T^0 up to* $\approx$ equivalence, where $\approx$ is an equivalence elation on $\mathbb{C}(\Sigma)$ defined in terms of relation and predicate symbols only. The subscripts T and T^0 express in which system the relation is defined.

Now we have all the prerequisites to give a theorem providing us with sufficient conditions so that a TDS is an operationally conservative extension of another TDS. The following theorem is valid *only* for positive TDSs and it will be used in Section 4.3.1.

Theorem 2.3.8 (*Operationally conservative extension*). Let $T^0 = (\Sigma_0, D_0)$ be a pure well-founded TDS in path format. Let $T^1 = (\Sigma_1, D_1)$ be a TDS in path format. If there is a conclusion sRt or Ps of a rule $d_1 \in D_1$, with $s = x$ or $s = f(x_1, \ldots, x_n)$ for an $f \in \Sigma_0$, we additionally require that d_1 is pure, well-founded, $t \in \mathbb{O}(\Sigma_0)$ for premises tRy of d_1, and that there is a premise containing only Σ_0 terms and a new relation or predicate symbol. Then if $T = T^0 \oplus T^1$ is defined, then T is an operationally conservative extension of T^0. □

Theorem 2.3.9 (*Operationally conservative extension up to equivalence*). Let $T^0 = (\Sigma_0, D_0)$ and $T^1 = (\Sigma_1, D_1)$ be two TDSs and let $T(\Sigma, D) = T^0 \oplus T^1$ be defined. If T is an operationally conservative extension of T^0 then it is also an operationally conservative extension up to $\approx$ equivalence, where $\approx$ is an equivalence relation defined exclusively in terms of predicate and relation symbols. □

However, in Section 5.4 the operational semantics considered will be defined by means of negative TDSs. The results shown earlier are not applicable in this case. The technique for proving the conservative extension property for that type of TDSs has been formalized in [65, 43] (see e.g. [60, 1, 2]. Basically, it is a combination of two methods: *the method of general conservative extension* (based on stratification) (see e.g. [107, 26, 48]) and *the method of reduced term-deduction systems* [65, 43].

While positive TDSs cannot lead to any confusion (as shown above elegant and simple results can be used to prove important properties of them) this is not the case if negative information appears in the premises. Take for instance the rule $\frac{c \overset{a}{\not\rightarrow}}{c \overset{a}{\rightarrow} c'}$ where c and c' are constants from some signature. One may argue that a TDS containing this rule is meaningless and inconsistent (see e.g. [60]) since it cannot be decided whether the relation defined by the TDS contains transition $c \overset{a}{\rightarrow} c'$ or not. Therefore, the very first question needed to be resolved in case of negative TDSs is if the TDS under consideration is meaningful and which transition relation it defines.

Stratification method The stratification method that has been shown very useful for proving conservativity of negative TDSs is intuitive and easy to check. It is based on the notion of stratification (defined below), a mapping by which the transitions are ordered in different layers, called strata, depending on the complexity of the premises of the rule for which the desired transition is its conclusion. Stratification guarantees that no transition depends negatively on itself and that the validity of a negative transition can be determined only if the validity of all transitions occurring in the earlier strata is known. Note that each positive TDS is trivially stratified by putting all literals in stratum to 0.

Definition 2.3.10. Let $PP(T)$ be the set of all closed positive formulas over T. A mapping $S : PP(T) \rightarrow \alpha$ for an ordinal α is called a *stratification* for T if for all deduction rules $d \in D$ and closed substitutions σ the following conditions hold. For all $\phi \in pprem(d)$, $S(\sigma(\phi)) \leq S(\sigma(conc(d)))$; for all $s\neg R \in nprem(d)$, for all $t \in \mathbb{C}(\Sigma) :\ S(\sigma(sRt)) < S(\sigma(conc(d)))$; for all $\neg Ps \in nprem(d)$, $S(\sigma(Ps)) < S(\sigma(conc(d)))$. A TDS is called *stratifiable* if there exists a stratification for it.

Even though the stratification technique is intuitive and often applicable, it is restrictive and cannot be applied to our TDS in Section 5.5.1. There we will exploit the more powerful technique of reduced TDSs. It is stronger than the method of stratification but for practical purposes it is useful to combine these two methods. In this brief introduction to this method we follow the line of [65, 43]. In [60] the reader can find an extensive review of several methods to associate a transition relation to a TDS. Amongst others, the author treats this approach and compares it with the other proposed methods.

Reduction method In order to keep the original presentation of the method (original definition and results as occurring in [43, 65]) we consider TDSs with only relation symbols. It is easy to see that any predicate symbol can be transformed into a relation symbol by adding a new constant to the signature. Then the rules of the TDS have to be transformed too with respect to the following equivalence:

$$Pt \Leftrightarrow tR_Pa_P,$$

where R_P is a fresh relation symbol and a_P is a fresh constant associated to the predicate symbol P. In such a way considering only TDSs with relation symbols does not make any restriction.

The idea of the reduction method is the following. For a given TDS T, the set of transitions is partitioned into three groups: those that are certainly true, those that are certainly not true and those of which the truth is unknown (it is also called 3-value method). Using this information the TDS T is *reduced* to another TDS that specifies the same transition relation. In the new TDS, the truth and falsity of more transitions may become certain. Repeated reduction may lead to complete information and give the transition relation associated to the original TDS. A transition relation associated to a TDS is defined in terms of an operator $Strip$ on TDSs. For transition relation $\rightarrow$, $Strip(T, \rightarrow)$ is a TDS obtained from T by removing all rules with negative premises that do not hold in $\rightarrow$ and by removing from the remaining rules the negative premises that do hold in $\rightarrow$. This yields a positive TDS whose associated transition relation is defined. Then T is stable for $\rightarrow$ if it is equal to the associated transition relation to $Strip(T, \rightarrow)$. (Different concepts of stability are also given in [60].) Precise definitions are given in the sequel.

Definition 2.3.11. Let A be a set of labels.

- A transition relation $\rightarrow \subseteq \mathbb{C}(\Sigma) \times A \times \mathbb{C}(\Sigma)$ is a *supported model* of T f:

$$\phi \in \rightarrow \iff \exists d \in D \text{ and substitution } \sigma \text{ such that: } \begin{cases} \longrightarrow \models prem(\sigma(d)) \\ conc(\sigma(d)) = \phi. \end{cases}$$

  $\rightarrow$ is a *model* of T if "$\Leftarrow$" holds; T is *supported* by $\rightarrow$ if "$\Rightarrow$" holds.

- The transition relation $\rightarrow_T$ associated with a positive TDS T is *the least model* of T.

- $Strip(T, \rightarrow) = (\Sigma, Strip(D, \rightarrow))$, where

$$Strip(D, \rightarrow) = \Big\{ d' \ : \ \exists d \in D : \rightarrow \models \ nprem(d) \ \& \ d' = \frac{pprem(d)}{conc(d)} \Big\}.$$

- A transition relation $\rightarrow$ is *stable* for TDS T if $\rightarrow$ is the associated relation to $Strip(T, \rightarrow)$.

- If there is a unique transition relation $\rightarrow$ stable for T, then $\rightarrow$ is the transition relation *associated with* T.

Reduction of a TDS is obtained by means of two positive TDSs: $True(T)$ and $Pos(T)$. $True(T)$ determines the transitions that are certainly true: they can be proved with positive rules only. $Pos(T)$ determines the transitions that are possibly true, that is, they are true or unknown. These are transitions that can be proved ignoring the negative premises. Thus $Pos(T)$ is obtained from T by removing all negative premises. A reduction step is defined by Definition 2.3.12 and the iterative method of reduction is given in Definition 2.3.14.

From now on, the set of rules D for TDS $T = (\Sigma, D)$ will be identified by the set of closed instances of rules in D.

Definition 2.3.12. Let $\rightarrow_{true}$ and $\rightarrow_{pos}$ be transition relations on $\mathbb{C}(\Sigma)$.

$$Reduce(T, \rightarrow_{true}, \rightarrow_{pos}) = (\Sigma, Reduce(D, \rightarrow_{true}, \rightarrow_{pos})),$$

where

$$Reduce(D, \rightarrow_{true}, \rightarrow_{pos}) = \Big\{ d' \ : \ \exists d \in D : \rightarrow_{true} \models \ nprem(d), \rightarrow_{pos} \models \ pprem(d) \ \&$$

$$d' = \frac{\{\psi \in pprem(d) \ : \rightarrow_{true} \not\models \ \psi\} \cup \{\psi \in nprem(d) \ : \rightarrow_{pos} \not\models \ \psi\}}{conc(d)} \Big\}$$

.

Definition 2.3.13. $True(T) = (\Sigma, True(D))$ where $True(D) = \{d \in D \ : \ nprem(d) = \emptyset\}$. $Pos(T) = (\Sigma, Pos(D))$ where $Pos(D) = \Big\{d' \in D \ : \ \exists d \in D : d' = \dfrac{pprem(d)}{conc(d)}\Big\}$.

Definition 2.3.14. For every ordinal α, the α-*reduction* of T, notation $Red^{\alpha}(T)$ is recursively efined as follows:

- $Red^{0}(T) = (\Sigma, D_{closed})$ where D_{closed} is the set of all closed instances of rules in D;
- $Red^{\alpha}(T) = Reduce(T, \bigcup\limits_{\beta<\alpha} \rightarrow_{True(Red^{\beta}(T))}, \bigcap\limits_{\beta<\alpha} \rightarrow_{Pos(Red^{\beta}(T))})$.

Combining stratification and reduction Finally, the way the two methods can be combined is given below. Combined reduction with stratification may lead to a desired result "faster" than the reduction method applied only. As soon as a stratified TDS is achieved by reduction, the iteration may stop. The main result used to prove the conservative extension property of the TDS in Section 5.5.1 is stated in Theorem 2.3.17.

Theorem 2.3.15 (*Stratification and reduction*). Let $T = (\Sigma, D)$ be a TDS with stratification $S : PP(T) \rightarrow \alpha$. Then Red^{α} is a positive TDS. □

Lemma 2.3.16. Let $T = (\Sigma, D)$ be a TDS and suppose that for some ordinals α and β, $S : PF(T) \rightarrow \alpha$ is a stratification of $Red^{\alpha}(T)$. Then $Red^{\alpha+\beta}(T)$ is a positive TDS and $\longrightarrow_{Red^{\alpha+\beta}(T)}$ is associated with T. □

Theorem 2.3.17 (*Conservative extension with reduction*). Let $T^0 = (\Sigma_0, D_0)$ be a pure TDS and let $T^1 = (\Sigma_1, D_1)$ be a TDS such that each rule $d \in D_1$ contains at least one function name $f \notin \Sigma_0$ in the source[7] of its conclusion. Furthermore, assume that $T^0 \oplus T^1$ exists and is positive after reduction. Then $T^0 \oplus T^1$ is a (operational) conservative extension of T^0. □

We have to point out that the notion of "positive after reduction" is proved equivalent to the notion of "complete TDS" in [60]. However, we decided to resent the material as given in [65] to give the reader the original version of Theorem 2.3.17, the main result needed in Section 5.4.

The following theorems show the relation between the operationally conservative extension property and the equationally conservative extension property.

Definition 2.3.18. Let $L_0 = (\Sigma_0, E_0)$ and $L_1 = (\Sigma_1, E_1)$ be two equational specifications and let $\Sigma_0 \oplus \Sigma_1$ be defined. The *sum* $L_0 \oplus_1$ of L_0 and L_1 is the equational specification $(\Sigma_0 \oplus Sigma_1, E_0 \oplus E_1)$.

Definition 2.3.19. Let $L_0 = (\Sigma_0, E_0)$ and $L_0 = (\Sigma_0, E_0)$ be two equational specifications and let $\Sigma_0 \oplus \Sigma_1$ be defined. L is an *equationally conservative extension* of L_0 if for all $s, t \in C(\Sigma_0)$

$$L \vdash s = t \Leftrightarrow L_0 \vdash s = t.$$

[7] The left argument of a transition.

Theorem 2.3.20 (*Equationally conservative extension*). Let $L_0 = (\Sigma_0, E_0)$ and $L_1 = (\Sigma_1, E_1)$ be two equational specifications and let $L = (\Sigma, E) = L_0 \oplus L_1$ be defined. Let $T_0 = (\Sigma_0, D_0)$ and $T_1 = (\Sigma_1, D_1)$ be term-deduction systems and let $T = T_0 \oplus T_1$. Let φ be an equivalence relation that is definable in terms of predicate and relation symbols only. Let L_0 be a complete axiomatization with respect to the φ equivalence model induces by T_0 and let L be a sound axiomatization with respect to the φ equivalence model induced by T. If T is an operationally conservative extension of T_0 up to φ equivalence, then L is an equationally conservative extension of L_0. □

Theorem 2.3.21 (*Complete axiomatization*). If in addition to the condition of Theorem 2.3.20 the equational specification L has the elimination property for L_0, then E is a complete axiomatization with respect to the φ equivalence model induced by the term-deduction system T. □

Chapter 3

Basic Probabilistic Process Algebra

3.1 Introduction

Random behaviour of processes in the framework of process algebra is captured by the *probabilistic choice operator*. This operator allows the explicit specification of probabilistic aspects in a way that it expresses (quantitatively) a probability distribution over a set of possible events/behaviours.

The probabilistic choice operator employed in the present thesis is closely related to the partial choice operator in [18] where the authors, besides the standard non-deterministic choice, introduce two more alternative composition operators: static or partial alternative composition $\uplus$ and collecting alternative composition $\sqcup$. The difference between these three operators is the moment when the choice is made. The non-deterministic choice is made at the same moment when the first action is executed. The collecting choice is made at the very beginning before any action in the entire process has been performed. And the partial choice is between these two: it is made before the first action occurs, but the exact moment is not known. That is, there is an internal behaviour of the process which determines the outcome of the choice $p \uplus q$ which takes place before p or q performs any action. Thus, the outcome of this choice cannot be influenced by the environment, but it can be only observed. We reason in the same way about the probabilistic choice with the only difference that there is more quantitative information available for the possible outcomes. Namely, the random behaviour of the process is the result of some uncertain internal behaviour which cannot be affected and does not interact or depend on the environment. For that reason it is called *internal probabilistic choice*, as opposed to the external probabilistic choice which assumes that the environment determines which of the possible processes are enabled. Also, "the (internal) probabilistic choice allows the designer to abstract away from the details of how choices are made, but still provides information on the outcome of the choice [71]".

We would like to point out that the internal probabilistic choice operator has roots in the standard non-probabilistic algebras as well. In particular, there have been attempts to encode random behaviour in non-probabilistic *ACP* using non-determinism and internal actions. For instance, in *ACP* a lossy channel C is usually specified as $C = (i \cdot tr + i \cdot lose) \cdot C$, where tr and $lose$ are atomic actions meaning "the transmission is successful" and "the channel fails", respectively (see e.g., [27]). The use of the internal action i is quite intuitive. We repeat that no quantitative information can be specified in this way. Now, the presence of the probabilistic choice operator gives a possibility to specify the quantitative information of the failure of a system and besides to hide the internal action i making it an integrated part of the operator.

In this chapter, we develop so-called Basic Probabilistic Process Algebra. Several basic process algebras with probabilistic choice will be introduced and we restrict ourselves to the treatment of

the basic operators only. The issues involving parallel composition are complex enough to justify dedicating a whole chapter to them: Chapter 4.

The chapter is organized as follows. First, a fully probabilistic process algebra is introduced in which the non-deterministic choice operator is omitted and the probabilistic choice operator is added. In the next section we present a probabilistic process algebra with the notion of non-determinism in two variants, with and without projection operators. In Section 3.3 we describe the bisimulation model of the process algebras introduced earlier. We define a probabilistic bisimulation relation and construct a model based on this relation with and without infinite processes. For the first model with infinite processes we prove that the RSP principle (pg. 41) holds, and for the second model (containing only finite processes) we prove a completeness property.

3.2 Basic Process Algebras

We introduce several probabilistic basic process algebras working again in a modular way. We begin with a process algebra with no notion of non-determinism, and conclude by an algebra that can cope with both probabilities and non-determinism and which is equipped with the notion of deadlock.

3.2.1 Fully Probabilistic Basic Process Algebra

In this section, we present a fully probabilistic process algebra. It is the smallest algebra considered in the thesis. The non-deterministic choice is not present, instead, we have a probabilistic choice operator. Due to the absence of the non-deterministic choice all choices between processes are supposed to be probabilistic; they are supposed to be resolved according to some probability distributions. It is obvious that this approach is based on discrete-time Markov chains.

Even though non-determinism should be present in the formalism for many reasons, it is quite useful to investigate fully probabilistic methods. A widely accepted approach to analyze systems with both non-determinism and probabilistic behaviour attempts to resolve all occurrences of non-determinism by means of (probabilistic or deterministic) schedulers. Applying a scheduler to a system, the resulting process is fully probabilistic. Also, seen as an extension of Markov chains the fully probabilistic approach can be used to specify, for instance, the probabilistic behaviour of sequential randomized algorithms.

Formally, the signature of *Fully Probabilistic Basic Process Algebra fpBPA* consists of a (finite) set of constants, $A = \{a, b, c, \ldots\}$ and the binary operators: $\cdot$ operator for sequential composition and $\leftthreetimes_\pi$ operator for probabilistic choice, for each $\pi \in \langle 0, 1 \rangle$. The set of axioms consists of the laws given in Table 3.1.

$(x \cdot y) \cdot z$	$=$	$x \cdot (y \cdot z)$	$A5$
$x \leftthreetimes_\pi y$	$=$	$y \leftthreetimes_{1-\pi} x$	$PrAC1$
$x \leftthreetimes_\pi (y \leftthreetimes_\rho z)$	$=$	$(x \leftthreetimes_{\frac{\pi}{\pi+\rho-\pi\rho}} y) \leftthreetimes_{\pi+\rho-\pi\rho} z$	$PrAC2$
$x \leftthreetimes_\pi x$	$=$	x	$PrAC3$
$(x \leftthreetimes_\pi y) \cdot z$	$=$	$x \cdot z \leftthreetimes_\pi y \cdot z$	$PrAC4$

Table 3.1: Axioms for probabilistic choice operator.

Intuitively, the term $x \leftplus_\pi y$ represents a process that behaves like x with probability π and behaves like y with probability $1 - \pi$. We do not permit a zero probability. Now, flipping a coin may be represented by the term: $s \equiv flip \cdot (head \leftplus_\pi tail)$. So, the probability distribution $\{head \mapsto \pi, tail \mapsto 1 - \pi\}$ is an integrated part of the probabilistic choice operator. The interpretation of the actions: $flip$, $head$ and $tail$ is clear. If it is a fair coin, then $\pi = 1/2$. It is the same if we write $t \equiv flip \cdot (tail \leftplus_{1-\pi} head)$ which is declared by the axiom $PrAC1$. Axiom $PrAC2$ expresses that the grouping of the components is irrelevant as long as the probability distribution over the set of all possibilities does not change[1]. This axiom also has a variant, as follows:

$$(x \leftplus_\pi y) \leftplus_\rho z = x \leftplus_{\pi\rho} (y \leftplus_{\frac{(1-\pi)\rho}{1-\pi\rho}} z) \quad PrAC2'.$$

Axiom $PrAC3$ says that if there are two possibilities which cannot be distinguished, then the probability distribution does not play any role. For example, if the coin above has $head$ on both sides, then independently on the probability π the outcome of the flip will always be $head$, in other words "head" shows with probability 1.

If we consider a slightly different term than s, namely, $s' \equiv flip \cdot (head \leftplus_{1/2} tail) \cdot stop$ where $stop$ denotes an action of finishing the flipping, then the axiom $PrAC4$ expresses that s' does not differ from the term $r' \equiv flip \cdot (head \cdot stop \leftplus_{1/2} tail \cdot stop)$ because whatever the outcome of the flip is, the process reaches the end denoted by the $stop$ action. Note that the probability distribution over $\{head, tail\}$ induces the probability distribution on $\{head \cdot stop, tail \cdot stop\}$ in a unique way.

However, the terms s and $r \equiv flip \cdot head \leftplus_{1/2} flip \cdot tail$ are not considered equal because in the former case the choice between $head$ and $tail$ may be resolved after the $flip$ action is executed, which is not possible in the second case. The term r corresponds to a trial with two unfair coins, one which always gives $head$ and the other one always gives $tail$. The probability to choose one of them in the beginning of the experiment is exactly $1/2$ for each of them. Once a coin is chosen, the outcome of the flip is determined. For the reasons mentioned before the left distributive law: $x \cdot (y \leftplus_\pi z) = x \cdot y \leftplus_\pi x \cdot z$ is not present in our axiomatization; thus we cannot derive $s = r$.

We introduce abbreviations in order to deal with probabilistic sums of several arguments:

$$x_1 \leftplus_{\pi_1} x_2 \leftplus_{\pi_2} x_3 \equiv x_1 \leftplus_{\pi_1} (x_2 \leftplus_{\frac{\pi_2}{1-\pi_1}} x_3) \qquad (\pi_1 + \pi_2 < 1)$$
$$x_1 \leftplus_{\pi_1} x_2 \leftplus_{\pi_2} x_3 \leftplus_{\pi_3} x_4 \equiv x_1 \leftplus_{\pi_1} (x_2 \leftplus_{\frac{\pi_2}{1-\pi_1}} x_3 \leftplus_{\frac{\pi_3}{1-\pi_1}} x_4) \qquad (\pi_1 + \pi_2 + \pi_3 < 1), \text{ etc.}$$

This notation explicitly gives the probability with which a process behaves as one of its components. For example, the terms $x_1 \leftplus_{\pi_1} x_2 \leftplus_{\pi_2} x_3 \leftplus_{\pi_3} x_4$ represents a process which behaves as the process represented by x_i, $i = 1, 2, 3$ with probability π_i and as the one represented by x_4 with probability $1 - \pi_1 - \pi_2 - \pi_3$.

Example 3.2.1. The process of throwing a fair die can be specified in the following way. If the number of spots shown on the die is specified by an atomic action $number$, which may be "one", "two", "three", "four", "five" and "six", then the desired process is specified by the *fpBPA* term: $toss \cdot (one \leftplus_{1/6} two \leftplus_{1/6} three \leftplus_{1/6} four \leftplus_{1/6} five \leftplus_{1/6} six)$ since it is a fair dice.

3.2.2 Basic Probabilistic Process Algebra

When considering concurrent processes the concept of non-determinism is necessary to describe the asynchronous character of interleaving parallel composition. One may argue that in the presence

[1] In some probabilistic models, the stratified model for example, this axiom does not hold.

of probabilistic choice every non-deterministic behaviour can be specified as a probabilistic one by taking some probability distribution (very often an uniform distribution is suggested) over the set of alternatives (see e.g. [98]). In the previous section we explained that in those cases where non-deterministic choice is used because of lack of more appropriate specification techniques this replacement is more than welcome (see Example 3.2.4). However, an attempt to describe interleaving of parallel components (in an asynchronous manner) with probability distribution has been done in [17], but probabilities assigned to possible alternatives have not been given any intuitive meaning.

Therefore we need a more expressive model which is able to describe both probabilistic and non-deterministic behaviour. To that purpose, we add the notion of alternative composition (non-determinism) to the fully probabilistic process algebra from the previous section by adding the alternative composition operator $+$.

The signature of *Basic Process Algebra with Probabilistic Choice* (without deadlock) *pBPA*$_{-\delta}$ consists of the signature of *fpBPA* and the non-deterministic choice operator $+$ (alternative composition). The laws for $+$ are given in Table 3.2. Basically (without axiom $PrAC5$) it is the set of axioms of *BPA* except that the $A3$ axiom is replaced by $AA3$ (see Remark 2.1.1). Axiom $A3$ is restricted because it does not hold anymore for processes involving the probabilistic choice operator as will be shown in Example 3.2.3. To conclude, the set of axioms of *pBPA*$_{-\delta}$ contains the axioms in Table 3.2 and the axioms of *fpBPA* given in Table 3.1.

$x + y$	=	$y + x$	$A1$
$(x + y) + z$	=	$x + (y + z)$	$A2$
$a + a$	=	a	$AA3$
$(x + y) \cdot z$	=	$x \cdot z + y \cdot z$	$A4$
$(x \leftplus_\pi y) + z$	=	$(x + z) \leftplus_\pi (y + z)$	$PrAC5$

Table 3.2: Axioms for non-determinism in probabilistic setting.

Remark 3.2.2. To repeat once again, the non-deterministic choice between processes p and q, $p + q$, is resolved at the same moment when one of the two processes performs the first action. Conversely, the probabilistic choice between processes p and q, $p \leftplus_\pi q$, is resolved before the first action of p or q is executed and the exact moment is not known. What is known is the expectation that the first action is performed by p (or by q). Thus, one expects to observe an action performed by p in $\pi \cdot 100\%$ of the cases and an action performed by q in $(1 - \pi) \cdot 100\%$ of the cases.

In fact, the statement above says that the probabilistic choice has priority over the non-deterministic choice. Namely, the summands u and z of the non-deterministic choice $u + z$ first have to resolve their probabilistic choices (if such exist) before the choice $u + z$ is resolved. In such a way, the non-deterministic choice appears to be a choice between the offered outcomes of the probabilistic behaviour of u and z. Thus, if $u \equiv x \leftplus_\pi y$ and for simplicity assume that z does not contain any probabilistic choice, then in a π fraction of the cases the non-deterministic choice $u + z$ becomes $x + z$ and in $1 - \pi$ cases it becomes $y + z$. This is exactly formulated by the axiom $PrAC5$: no distinction is made between $(x \leftplus_\pi y) + z$ and $(x + z) \leftplus_\pi (y + z)$ since in both cases the probabilistic choice has to be resolved before the non-deterministic choice(s). This approach to the interplay of the probabilistic and non-deterministic choice is also taken in [71]. The difference with that approach occurs in the interpretation of parallel composition (see Chapter 4).

3.2.3 Deadlock

This section introduces an extension of *pBPA*$_{-\delta}$ with the inaction process (sometimes called deadlock process). It is done by adding a new constant (as it was done in Chapter 2), denoted δ, which stands for a process which with probability 1 does nothing; neither executes an action, nor terminates successfully. The axioms that define δ are given in Table 3.3. One can note that the deadlock constant is defined in the same way as in the non-probabilistic setting. This shows that in our approach this constant does not have any special role with respect to the probabilistic choice, as opposed to the special role in *BPA*$_\delta$, where it is the zero element with respect to the non-deterministic choice operator. Since axiom $A6$ is included in the system, δ occurs as the zero element with respect to the non-deterministic choice operator in the probabilistic setting as well.

$x + \delta$	=	x	$A6$
$\delta \cdot x$	=	δ	$A7$

Table 3.3: Axioms for inaction.

Various interpretations of the deadlock process (fail) in combination with probabilistic and non-deterministic choice can be found in [72, 73].

At this point we have completed the introduction of the basic process algebra which will be the core of the extensions with parallel composition (Chapter 4) and time (Chapter 5). This process algebra will be denoted by *pBPA*. To conclude, *pBPA* has signature $\Sigma_{pBPA} = (A_\delta, \cdot, +, \leftthreetimes_\pi)$ and the axioms given in Table 3.1+3.2+3.3.

Algebra *fpBPA* can be extended with the deadlock constant in an obvious way, by adding the constant δ and the axiom $A7$.

Example 3.2.3. We have not explained yet the reason why axiom $A3$ is replaced by $AA3$. Let us consider the following term: $p \equiv a \leftthreetimes_{\frac{1}{2}} \delta$. It represents a process that deadlocks with probability $1/2$. If we consider the non-deterministic choice of two alternatives p and p, then we derive that

$$\begin{aligned} pBPA \vdash \quad & (a \leftthreetimes_{\frac{1}{2}} \delta) + (a \leftthreetimes_{\frac{1}{2}} \delta) \overset{PrAC5}{=} (a + (a \leftthreetimes_{\frac{1}{2}} \delta)) \leftthreetimes_{1/2} (\delta + (a \leftthreetimes_{\frac{1}{2}} \delta)) \overset{A1}{=} \\ & ((a \leftthreetimes_{\frac{1}{2}} \delta) + a) \leftthreetimes_{1/2} ((a \leftthreetimes_{\frac{1}{2}} \delta) + \delta) \overset{PrAC5,A6}{=} \big((a + a) \leftthreetimes_{\frac{1}{2}} (\delta + a)\big) \leftthreetimes_{1/2} (a \leftthreetimes_{\frac{1}{2}} \delta) \overset{AA3,A6}{=} \\ & (a \leftthreetimes_{\frac{1}{2}} a) \leftthreetimes_{1/2} (a \leftthreetimes_{\frac{1}{2}} \delta) \overset{PrAC3}{=} (a \leftthreetimes_{\frac{2}{3}} a) \leftthreetimes_{\frac{3}{4}} \delta \overset{PrAC3,PrAC2}{=} a \leftthreetimes_{\frac{3}{4}} \delta. \end{aligned}$$

Therefore, this process deadlocks with less probability than p does . So, we can not always consider p and $p + p$ to be equal. One can note that this phenomenon occurs due to the interplay of probabilistic and non-deterministic choice taken in our approach. □

Example 3.2.4. Consider again the communication channel from Example 2.1.2. What can be specified in *pBPA* is the failure behaviour of the channel but additionally the quantitative aspects of that behaviour can be modelled as well. Assume that the channel fails once in 100 trials. Moreover, assume that two different types of messages (0 and 1) can be sent through the channel. Of course, the channel has to accept any message no matter which type it is. The behaviour of this channel is specified by the following *pBPA* term: $Ch_p = (r_{f0} + r_{f1}) \cdot (s_t \leftthreetimes_{0.99} d)$ where r_{f0} means a receipt of a message of type 0. And similar for r_{f1}. The other constants have the same meaning as before. The choice between r_{f0} and r_{f1} is non-deterministic. Replacing this choice by a probabilistic one, say $\leftthreetimes_\pi$, would mean that the channel decides (with certain probability) which type of message to accept and pass on. Indeed, it leads to a situation in which the channel "refuses" to transmit a certain message and the whole process (including sending and receiving components) fails.

3.2.4 Projection in *pBPA* and recursion

In *pBPA* we introduce the notions of recursion and guardedness in a similar way as it is done in *BPA* (as briefly introduced in Chapter 2). Recall that we use recursion to introduce infinite processes. Presence of probabilities does not change the concept of guardedness significantly with respect to non-probabilistic methods. However, it is worth to mention that in many cases an unguarded recursive specification that contains probabilistic choice determines a unique process provided it is given the "right" and still intuitive characterization. Take, for example, the equation $X = a \leftthreetimes_\pi X$. Though it is not guarded, the solution of this equation cannot be anything else than a. Just to compare, the equation $X = a + X$ does not have a unique solution in a model of *BPA* (the graph model for instance). This positive character of equation $X = a \leftthreetimes_\pi X$, and similar equations, results from the mathematical interpretation of the equations. Seen as a discrete-time Markov chain, where a may mean a state in which event a will happen, we may profit from the Markov chain theory and explore a subset of unguarded specifications that have a unique solution (see [102] and also [3]). We will explore a similar question in Chapter 6 where again an equation like $X = a \leftthreetimes_\pi X$ will not be considered but a particular format of guarded recursive specifications resembling it. Therefore, although challenging to consider unguarded recursion we rule out it and consider only guarded recursive specifications.

Next we define projection by introducing a new operator, called the *projection operator*. Projection will be used to approximate infinite processes; namely the n-th projection of a process p is a process that behaves exactly like p till at most n steps are executed. In other words, if we picture process p as an infinite tree of transitions (transitions occur as edges of the tree), then the n-th projection is the finite subtree of it that contains all action transitions with depth at most n.

Probabilistic basic process algebra with projection, *pBPA* $+ PR$, is an extension of *pBPA* with the projection operator. The axioms for this operator are given in Table 3.4.

$\Pi_n(a)$	=	a	$PR1$
$\Pi_1(a \cdot x)$	=	a	$PR2$
$\Pi_{n+1}(a \cdot x)$	=	$a \cdot \Pi_n(x)$	$PR3$
$\Pi_n(x + y)$	=	$\Pi_n(x) + \Pi_n(y)$	$PR4$
$\Pi_n(x \leftthreetimes_\rho y)$	=	$\Pi_n(x) \leftthreetimes_\rho \Pi_n(y)$	$prPR$

Table 3.4: Axioms for projection operator, $n \geq 1$

Recursion In the following, we formally characterize the notion of *recursion*, *recursive specification* and *guardedness*. The given definitions refer to the *pBPA* $+ PR$ theory, but they can be easily adapted to other process algebras, the probabilistic process algebras *pBPA* and *pACP*$^+$ as well as non-probabilistic algebras *BPA*, *BPA* $+ PR$ and *ACP* $+ PR$ discussed in Chapter 2.

Definition 3.2.5. A *recursive equation* over *pBPA* $+ PR$ is an equation of the form $X = s(X)$ where $s(X)$ is a term over *pBPA* $+ PR$ containing variable X, but no other variables.

A *recursive specification* E over *pBPA* $+ PR$ is a set of recursive equations over *pBPA* $+ PR$. By this we mean that we have a set of variables $\mathcal{V}$ and an equation of the form $X = s_X(\mathcal{V})$ for each $X \in \mathcal{V}$, where $s_X(\mathcal{V})$ is a term over *pBPA* $+ PR$ containing variables from the set $\mathcal{V}$.

$\mathcal{V}$ contains one distinguished variable called the root variable. Usually, for the equation of X we write $X = s_X$ in short.

Definition 3.2.6. *A solution* of a recursive equation $X = s(X)$ in some model of ***pBPA*** $+ PR$ s a process p that satisfies the equation, that is $p = s(p)$ holds in the model. A process p is a solution of a recursive specification E in some model of ***pBPA*** $+ PR$ if after substituting p for the root variable of E, there exist other processes for the other variables of E such that all equations of E are satisfied. If E is a recursive specification with root variable X, then $\langle X|E\rangle$ denotes a solution of this specification.

Definition 3.2.7. A variable Y occurs *unguarded* in the term t in the following cases:

1. Y occurs unguarded in the term Y;
2. if Y occurs unguarded in s, then for any term r, Y occurs unguarded in $s \cdot r$, $\Pi_n(s)$, $s + r$, $r + s$, $s \leftthreetimes_\pi r$ and $r \leftthreetimes_\pi s$ as well.

Let $\mathcal{UV}(t)$ denote the set of all variables that occur unguarded in t.

Definition 3.2.8. *The set of guarded terms* $\mathbf{GT}$ over ***pBPA*** $+ PR$ is inductively defined in the following way:

1. $A \subseteq \mathbf{GT}$;
2. if g is a guarded term, then for any term t, $g \cdot t \in \mathbf{GT}$;
3. if g is a guarded term, then $\Pi_n(g) \in \mathbf{GT}$ for $n \geq 1$;
4. if g and h are guarded terms, then $g + h \in \mathbf{GT}$.
5. if g and h are guarded terms, then $g \leftthreetimes_\pi h \in \mathbf{GT}$.

Note that all closed terms are guarded. Moreover, it is easy to check that term g is guarded iff no variable occurs unguarded in g. Obviously we could have taken this as a definition of guarded terms. The reason not to do so lies in our intention to have an inductive definition of guarded terms. With the constructive definition of guarded terms, as basically Definition 3.2.8 is, many proofs concerning guarded terms can be carried out by means of induction. On the other hand, the notion of an unguarded occurrence of a variable is used in the definition of guarded recursive specification. In fact, the right-hand sides of the equations of a recursive specification E are not restricted to guarded terms; some of them may contain unguarded variables. But they have to be structured in such a way that every term that appears as a right-hand side of an equation of E can be transformed (rewritten) into a guarded term only by replacing every variable by the associated term according to the equations of E. Formally,

Definition 3.2.9. Let E be a recursive specification over variables $\mathcal{V}$.

1. We write $X \xrightarrow{u} Y$ (for $X, Y \in \mathcal{V}$) if Y occurs unguarded in the equation of X in E.
2. If the relation $\xrightarrow{u}$ is well-founded, E is called a *guarded recursive specification*.
3. If E does not contain unguarded occurrences of variables, E is called *completely guarded*.

Recall that a relation is well-founded if it does not have infinite sequences. In this case, this means sequences of the form $X_1 \xrightarrow{u} X_2 \xrightarrow{u} X_3 \xrightarrow{u} \ldots$. This implies absence of cycles. By $\xrightarrow{u}\!\!\!\!\rightarrow$ we denote the transitive closure of $\xrightarrow{u}$. Definition 3.2.9 clearly indicates that every guarded recursive specification contains at least one equation whose right-hand side is a guarded term.

In the literature very often the definitions of "unguarded occurrences", "guarded term", "guarded recursive specification" differ from the definitions we use. Below we formulate those definitions for *pBPA* + PR, but we claim that they are equivalent with our corresponding definitions.

Definition 3.2.10.

1. Let s be a term over *pBPA* + PR containing variable X. We call an occurrence of X in s guarded if s has a subterm of the form $a \cdot t$, where a is an atomic action and t a term containing this occurrence of X; otherwise we call the occurrence of X in s unguarded.

2. We call a term s completely guarded if all occurrences of all variables in s are guarded.

3. A recursive specification E is completely guarded if all right hand sides of all equations of E are completely guarded terms.

4. A term s is guarded if we can rewrite s to a completely guarded term by use of the axioms.

5. A recursive specification E is guarded if we can rewrite E to a completely guarded specification by use of the axioms and by (repeatedly) replacing variables by the right-hand side of their equations.

Note that in this definition of guarded recursive specification the axioms of the used process algebra may be applied in the procedure of rewriting specification E into a completely guarded specification. The difficulties in the probabilistic case with this definition occur in the proof of the claim that the probability distribution function, whose formal definition is given in Section 3.3, is well defined (Proposition 3.3.18). In fact, without having proved that the left-hand side and the right-hand side of each axiom have the same probability distribution over bisimulation equivalence classes (which proof comes later as a part of the soundness theorem of *pBPA* + PR) we cannot employ such a property to show the probability distribution function being well-defined.

The following lemmas can easily be proven. The first lemma expresses that if a variable X is substituted by a guarded term then the result term has less or equal unguarded occurrences of variables, and none of them is X. The second lemma is a generalized variant of the former one.

Lemma 3.2.11. If g is a guarded term and h is a term with $\mathcal{UV}(h) = \{X, Y_1, Y_2, \ldots, Y_n\}$, then the term $h(X := g)$ obtained by replacing all occurrences of X by g has $\mathcal{UV}(h(X := g)) \subseteq \mathcal{UV}(h) \backslash \{X\}$. □

Lemma 3.2.12. If h is a term with $\mathcal{UV}(h) = \{Y_1, Y_2, \ldots, Y_n\}$ and $g_1, g_2, \ldots, g_n$ are guarded terms, then $h(Y_1 := g_1, Y_2 := g_2, \ldots, Y_n := g_n)$ is a guarded term. □

Lemma 3.2.13. Every guarded recursive specification can be rewritten into a completely guarded recursive specification by repeatedly replacing unguarded occurrences of variables by the right-hand sides of the corresponding equations.

Proof. Let E be a guarded recursive specification with the root variable X. Furthermore, let us assume that $\{Y_1, Y_2, \ldots, Y_n\}$ are all variables in $\mathcal{V}$ such that $X \overset{u}{\twoheadrightarrow} Y_i$. It is clear that this is a finite set, possibly empty. In the case this is the empty set, E does not contain unguarded variables and therefore E is completely guarded. Otherwise, we can represent the relation $\overset{u}{\rightarrow}$ as a tree with the root X (see for instance the tree in Figure 3.3 on page 57). Then, there must be at least one i for which $Y_i \overset{u}{\not\rightarrow}$, namely Y_i is not $\overset{u}{\rightarrow}$ related with any variable. In other words, t_{Y_i} does not have unguarded variables, and so t_{Y_i} is a guarded term.

Let $\{Y_{m1}, Y_{m2}, \ldots, Y_{mn}\}$ be the set of all variables with guarded right-hand sides whose existence follows from above (all leaves in the tree). Then, there is at least one $Y \notin \{Y_{m1}, Y_{m2}, \ldots, Y_{mn}\}$ (a leaf but one) such that $\mathcal{UV}(t_Y) \subseteq \{Y_{m1}, Y_{m2}, \ldots, Y_{mn}\}$. From Lemma 3.2.12 follows that $t_Y(Y_{mi} := t_{Y_{mi}})$ becomes a guarded term. In that way, going backwards and in each step obtaining new guarded terms and replacing them in the right-hand sides of the remaining equations in E, due to finiteness of the tree (induced by the assumption of $\overset{u}{\rightarrow}$ being well-defined), this procedure terminates. The procedure results in a completely guarded recursive specification. □

Recursion principles One reason that unguarded recursive specifications are not taken into account is that they may have more than one solution. The next question that pops up immediately is: "Does every guarded recursive specification has a unique solution?". The answer of this question is "yes" and the proof of it, for the bisimulation model of *pBPA* + PR will be given in Section 3.3.2[2]. This property is exactly expressed by a combination of two principles: RDP$^-$ and RSP. RDP$^-$ can easily be made valid in the model simply by extending the set of processes with all possible solutions of guarded recursive specifications. Therefore, the main point is to prove RSP. Basically, the relation between an infinite process and its finite projections is established by the so-called AIP^- principle: it expresses that two infinite processes can be considered equivalent if all their finite projections with the same degree are equivalent. In [27], the authors show that in an arbitrary model in which the Projection theorem holds (see pg. 72), AIP$^-$ implies RSP. This is exactly the way we take in Section 3.3.2 where the recursion principles are discussed in a probabilistic setting.

In order to formulate the recursion principles the notion of boundedly branching (in [27] bounded non-determinism) needs to be defined. Informally, in a given model a process p is *boundedly branching* if for any finite sequence of atomic actions $s \equiv a_1 a_2 \ldots a_n (n \geq 1)$, by executing the sequence s, p can reach only finitely many different processes. (The formal definition can be found in [27] which is easily extended with the probabilistic choice operator.) Thus, we deal with the following principles:

The Restricted Recursion Definition Principle (RDP$^-$) Every guarded recursive specification has a solution.

The Restricted Approximation Induction Principle (AIP$^-$) A boundedly branching process is determined by its finite projections, that is, for any x and y

$$(\forall n \geq 1 : \Pi_n(x) = \Pi_n(y) \ \wedge \ x \text{ is boundedly branching}) \Rightarrow x = y.$$

The Recursion Specification Principle (RSP) Every guarded recursive specification has at most one solution.

[2]The proof of this property for non-probabilistic algebras *BPA* + PR and *ACP* + PR with recursion can be found in [27].

3.2.5 Properties of *pBPA* and *pBPA* + PR

The main aim of the study of *pBPA* is to build a complete model for the axiomatization based on a bisimulation equivalence. In fact, these results will be presented in Section 3.3.3 in the form of two theorems: the Soundness theorem and the Completeness theorem. Orthogonal to this is the study of *pBPA* + PR and a model of it that satisfies the recursion principles defined above. This will be the subject of Section 3.3.2. But before we come to these points we present several interesting properties of *pBPA* and *pBPA* + PR some of which are needed later on. A part of this section is devoted to the introduction of the set of basic terms followed by a proof of the elimination property. The Elimination theorem has a crucial role in the proof of the Completeness theorem.

Recall that in the non-probabilistic process algebra *BPA* one of the important notions used in the proof of the completeness property is the notion of summand of a term. It says that if $p = q + p$ then q is a summand of p. Besides, it provides a partial ordering on the set of *BPA* terms. On the contrary, the notion of a summand for the probabilistic choice operator cannot be defined (by simply replacing "+" by "$\uplus_\pi$") as the following proposition states. In fact, if equation $p = q \uplus_\pi p$ can be derived in *pBPA* it actually means that p and q represent the same processes. However, our axioms do not reason in terms of infinite sums and we cannot derive the equation $p = q$ in *pBPA*. On the other hand, this property will be proved valid in the bisimulation model (Lemma 3.3.54 on pg. 80) in a form of a cancellation law for the probabilistic choice operator and it will be one of the crucial results used in the proof of the completeness property of *pBPA*. From this property we can make one more observation. In [18], the authors propose a method for the verification of systems which is based on a partial ordering of terms. They introduce the so-called realization axiom $x \leq x \uplus y$, which says that x has less static non-determinism than $x \uplus y$. This proposition shows that this approach cannot be followed in the framework of *pBPA* because such a partial ordering cannot be defined in a non-trivial way if probabilities are involved. It is worth to notice that in [3] the authors consider a probabilistic axiomatization where one of the proposed axioms resembles Proposition 3.2.14. They, indeed, consider an axiom which, translated into our syntax, has the form $p = q \uplus_\pi p \Rightarrow p = q$.

Proposition 3.2.14. If *pBPA* $\vdash p = q \uplus_\pi p$ for $\pi \in \langle 0, 1\rangle$, then *pBPA* $\vdash p \approx q$, where $p \approx q$ denotes that p is equal to q with probability 1.

Proof. In *pBPA* the following equations are derivable:

$$p = q \uplus_\pi p = q \uplus_\pi (q \uplus_\pi p) = (q \uplus_{\frac{\pi}{\pi(2-\pi)}} q) \uplus_{\pi(2-\pi)} p = q \uplus_{\pi(2-\pi)} (q \uplus_{\pi(2-\pi)} p) = q \uplus_{\pi_1(2-\pi_1)} p,$$

where $\pi_1 = \pi(2 - \pi)$. After n repetitions of this procedure we obtain *pBPA* $\vdash p = q \uplus_{\pi_{n+1}} p$, where $\pi_{n+1} = \pi_n(2 - \pi_n)$. The solution of this recurrent equation is $\pi_n = 1 - (1 - \pi)^{2^n}$ and as $1 - \pi < 1$, $\lim\limits_{n\to\infty} 1 - (1 - \pi)^{2^n} = 1$. □

The next proposition expresses that the term obtained by the interchange of two summands x_i and x_j in the term $x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_i \uplus_{\pi_i} \ldots x_j \uplus_{\pi_j} x_{j+1} \ldots \uplus_{\pi_{n-1}} x_n$ together with assigned probabilities is equal to the original term; it is easy to derive the equality using axioms $PrAC1$ and $PrAC2$. For example for $n = 3$, *pBPA*$(+PR)$ $\vdash x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} x_3 = x_2 \uplus_{\pi_2} x_1 \uplus_{\pi_1} x_3 = x_1 \uplus_{\pi_1} x_3 \uplus_{1-\pi_1-\pi_2} x_2$. Furthermore, for $n = 2$ we simply have axiom $PrAC1$. We will use this proposition very often without indicating it explicitly.

Proposition 3.2.15. It can be easily proved that the following equations hold in *pBPA*$(+PR)$:

i. $x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_i \uplus_{\pi_i} \ldots x_j \uplus_{\pi_j} x_{j+1} \ldots \uplus_{\pi_{n-1}} x_n$
$= x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_j \uplus_{\pi_j} \ldots x_i \uplus_{\pi_i} x_{j+1} \ldots \uplus_{\pi_{n-1}} x_n$,
for each i, j, $1 \leq i \leq n-1$, $1 \leq j \leq n-1$, $i < j$ and $n \geq 3$;

ii. $x_1 \leftthreetimes_{\pi_1} x_2 \leftthreetimes_{\pi_2} \ldots \leftthreetimes_{\pi_{i-1}} x_i \leftthreetimes_{\pi_i} x_{i+1} \ldots \leftthreetimes_{\pi_{n-1}} x_n$
$= x_1 \leftthreetimes_{\pi_1} x_2 \leftthreetimes_{\pi_2} \ldots \leftthreetimes_{\pi_{i-1}} x_n \leftthreetimes_{1-\sum_{j=1}^{n-1}\pi_j} x_{i+1} \ldots \leftthreetimes_{\pi_{n-1}} x_i$,
for each $1 \leq i \leq n-1$ and $n \geq 2$. □

Next we define a special subset, denoted $\mathcal{D}(pBPA)$, of the set of closed terms of *pBPA*. All constants belong to this set. Besides, elements of this set are all closed *pBPA* terms with the outermost operator either sequential composition or alternative composition. Moreover, they cannot be rewritten by means of the *pBPA* axioms into terms with probabilistic choice as the outermost operator. Formally,

Definition 3.2.16. By $\mathcal{SP}(pBPA)$ we will denote the set of all closed terms over the signature Σ_{pBPA}. An auxiliary set of closed terms, $\mathcal{D}(pBPA)$, is defined as follows:

1. $A_\delta \subseteq \mathcal{D}(pBPA)$;
2. $s \in \mathcal{D}(pBPA), t \in \mathcal{SP}(pBPA) \Rightarrow s \cdot t \in \mathcal{D}(pBPA)$;
3. $t, s \in \mathcal{D}(pBPA) \Rightarrow t + s \in \mathcal{D}(pBPA)$.

As elaborated in Section 3.3, terms in $\mathcal{D}(pBPA)$ represent processes with a trivial probability distribution - only one process is assigned the non-zero probability 1. From the structure of the terms in $\mathcal{D}(pBPA)$ this interpretation comes naturally. Additionally, since the closed terms of *BPA* and BPA_δ can be seen as probabilistic terms that do not contain any probabilistic choice operator, the embedding of these two non-probabilistic process algebra into *pBPA* is done by mapping closed terms from *BPA* or BPA_δ into the set $\mathcal{D}(pBPA)$.

Proposition 3.2.17. $pBPA \vdash s = s + s$, for $s \in \mathcal{D}(pBPA)$

Proof. The proof is given by induction on the structure of s.

Case $s \equiv a, a \in A_\delta$. The result follows from axiom AA3;

Case $s \equiv s' \cdot t$. By the inductive hypothesis $pBPA \vdash s' = s' + s'$ and $pBPA \vdash s + s = s' \cdot t + s' \cdot t = (s' + s') \cdot t = s' \cdot t = s$;

Case $s \equiv s' + s''$. By the inductive hypothesis $pBPA \vdash s' = s' + s'$ and $pBPA \vdash s'' = s'' + s''$. Hence, $pBPA \vdash s + s = (s' + s'') + (s' + s'') = (s' + s') + (s'' + s'') = s' + s'' = s$.

□

In a similar way we define a set $\mathcal{D}(pBPA+PR)$ as a subset of the set of closed terms of $pBPA+PR$. An adapted version of Proposition 3.2.17 is valid for $\mathcal{D}(pBPA + PR)$ terms as well.

Definition 3.2.18. By $\mathcal{SP}(pBPA + PR)$ we will denote the set of all closed terms over the signature $\Sigma_{pBPA+PR}$. An auxiliary set of closed terms, $\mathcal{D}(pBPA + PR)$, is defined as follows:

1. $A_\delta \subseteq \mathcal{D}(pBPA + PR)$;
2. $s \in \mathcal{D}(pBPA), t \in \mathcal{SP}(pBPA + PR) \Rightarrow s \cdot t \in \mathcal{D}(pBPA + PR)$;
3. $s \in \mathcal{D}(pBPA + PR) \Rightarrow \Pi_n(s) \in \mathcal{D}(pBPA + PR)$, for $n \geq 1$;
4. $t, s \in \mathcal{D}(pBPA + PR) \Rightarrow t + s \in \mathcal{D}(pBPA + PR)$.

Basic terms An interesting property that is derived from the axioms of *pBPA* is that every term can be expressed in a normal form. The next step is to define a set of terms that are in normal form, which we call basic terms, and to prove that every terms is provably equal to a basic term. Because of the Elimination theorem, if some statement must be proved to be valid for all closed terms, it is sufficient to prove it valid for all basic terms, using structural induction as a proof method. This makes the core of the proof of the Completeness theorem.

Definition 3.2.19. The set of *basic terms* of *pBPA*, $\mathcal{B}(pBPA)$, is inductively defined with the help of an intermediate set $\mathcal{B}_+(pBPA)$.

1. $A \cup \{\delta\} \subseteq \mathcal{B}_+(pBPA) \subset \mathcal{B}(pBPA)$;
2. $a \in A,\ t \in \mathcal{B}(pBPA) \Rightarrow a \cdot t \in \mathcal{B}_+(pBPA)$;
3. $t, s \in \mathcal{B}_+(pBPA) \Rightarrow t + s \in \mathcal{B}_+(pBPA)$;
4. $t, s \in \mathcal{B}(pBPA) \Rightarrow t \between_\pi s \in \mathcal{B}(pBPA)$ for every $\pi \in \langle 0, 1\rangle$.

Remark 3.2.20. If terms that only differ in the order of the summands are considered to be identical (i.e. identification of terms is considered modulo axioms $A1$, $A2$, $PrAC1$ and $PrAC2$), then the basic terms are exactly the terms of the form

$$x \equiv x_1 \ \ (x \in \mathcal{B}_+(pBPA)) \text{ or} \tag{3.1}$$

$$x \equiv x_1 \between_{\pi_1} x_2 \between_{\pi_2} x_3 \ldots x_{n-1} \between_{\pi_{n-1}} x_n \text{ and } \ n > 1 \tag{3.2}$$

where $x_i \equiv \sum_{j<l_i} a_{ij} \cdot t_{ij} + \sum_{k<m_i} b_{ik}$ for certain $a_{ij}, b_{ik} \in A_\delta$, basic *pBPA* terms t_{ij} and $n, m_i, l_i \in \mathbb{N}$.

The terms in $\mathcal{D}(pBPA)$ are exactly of the form: $\sum_{i<m} s_i \cdot t_i + \sum_{j<n} a_j$ for some $n, m \in \mathbb{N}$, $a_i \in A_\delta$, $\mathcal{D}(pBPA)$ terms s_i and $\mathcal{SP}(pBPA)$ terms t_i. And $\mathcal{B}_+(pBPA) \subset \mathcal{D}(pBPA)$.

Elimination property of *pBPA* and *pBPA* + PR The proof of the Elimination theorem to basic terms in *pBPA* consists of two parts (as described in Section 2.3). In the first part we construct a TRS from the axioms of *pBPA* (with the rules given in Table 3.5) and show that it is a strongly normalizing TRS. In the second part we show that every normal form of the previously defined TRS is indeed a basic term of *pBPA*.

Lemma 3.2.21. The term rewrite system shown in Table 3.5 ($\pi \in \langle 0, 1\rangle$) is strongly normalizing.

Proof. In order to prove this claim we use the method of the lexicographical variant of the recursive path ordering. Suppose that the following ordering on the signature of *pBPA* is defined: $\cdot > + > \between_\pi$ and the symbol $\cdot$ is given the lexicographical status for the first argument. Then for each rewrite rule $p \to q$ in Table 3.5 relation $p >_{lpo} q$ can easily be proved. From Theorem 2.3.4 it follows that the given term rewrite system is strongly normalizing. □

Lemma 3.2.22. The normal forms of closed *pBPA* terms are basic *pBPA* terms.

$(x+y)\cdot z$	$\rightarrow$	$x\cdot z+y\cdot z$	$RA4$
$(x\cdot y)\cdot z$	$\rightarrow$	$x\cdot(y\cdot z)$	$RA5$
$\delta\cdot x$	$\rightarrow$	δ	$RA7$
$(x\leftthreetimes_\pi y)\cdot z$	$\rightarrow$	$x\cdot z\leftthreetimes_\pi y\cdot z$	$RPAC4$
$(x\leftthreetimes_\pi y)+z$	$\rightarrow$	$(x+z)\leftthreetimes_\pi(y+z)$	$RPAC5$
$x+(y\leftthreetimes_\pi z)$	$\rightarrow$	$(x+y)\leftthreetimes_\pi(x+z)$	$RPAC5'$

Table 3.5: Term rewrite system of *pBPA*.

Proof. Suppose that p is a normal form of some closed *pBPA* term and suppose that p is not a basic term. Let p' denote the smallest sub-term of p which is not a basic term. It implies that each sub-term of p' is a basic term. Then p can be proved not to be a term in normal form. The possible forms of p' give the following cases:

Case $p'\equiv a, a\in A_\delta$. p' is a basic term, which contradicts the assumption that p' is not a basic term. So this case does not occur.

Case $p'\equiv p_1\cdot p_2$. By case analysis on the structure of the basic term p_1 we have:

- *Subcase* $p_1\in A_\delta$. In this case p' would be a basic term, which contradicts the assumption that p' is not a basic term;
- *Subcase* $p_1\equiv a\cdot p_1'$. $RA5$ rewriting rule can be applied. So, p is not a normal form;
- *Subcase* $p_1\equiv p_1'+p_1''$. $RA4$ rewriting rule can be applied. So, p is not a normal form;
- *Subcase* $p_1\equiv p_1'\leftthreetimes_\pi p_1''$. $RPAC4$ rewriting rule can be applied. So, p is not a normal form.

Case $p'\equiv p_1+p_2$. By case analysis on the structure of both terms p_1 and p_2 we obtain:

- *Subcase both* p_1 *and* p_2 *are from* $\mathcal{B}_+(pBPA)$. p' would be a basic term, which contradicts the assumption that p' is not a basic term;
- *Subcase* $p_1\equiv p_1'\leftthreetimes_\pi p_1''$ *or* $p_2\equiv p_2'\leftthreetimes_\sigma p_2''$. One of rewriting rules $RPAC5$ or $RPAC5'$ is applicable. So p is not a normal form.

Case $p'\equiv p_1\leftthreetimes_\pi p_2$. In this case p' would be a basic term (since p_1 and p_2 are basic terms) which contradicts with the assumption that p' is not a basic term.

□

As a corollary of the previous two lemmas the Elimination theorem follows:

Theorem 3.2.23 (*Elimination theorem of pBPA*). Let p be a closed *pBPA* term. Then there is a basic *pBPA* term q such that *pBPA* $\vdash p=q$. □

One can notice that if s is a closed $\mathcal{D}(pBPA)$ term, then the associated basic term whose existence is guaranteed by the Elimination theorem is a basic term from $\mathcal{B}_+(pBPA)$.

Using the Elimination theorem of *pBPA* we can prove the elimination property of *pBPA* $+\ PR$. Basically, it is sufficient to prove that the projection operator can be eliminated from closed *pBPA* $+$ PR terms in favour of basic operators of *pBPA*. Then the elimination property of *pBPA* $+\ PR$ follows straightforwardly.

Lemma 3.2.24. (Elimination of the projection operator) If s is a basic *pBPA* term and $n \in \mathbf{N}$, $n \geq 1$, then there exists a closed *pBPA* term t such that *pBPA* $+ PR \vdash \Pi_n(s) = t$.

Proof. The proof is given by the double induction on n and the structure of s.

`Basis.` For $n = 1$ we have the following:

Case $s \equiv a, a \in A_\delta$. The conclusion follows from axiom $PR1$;

Case $s \equiv a \cdot s_1$. *pBPA* $+ PR \vdash \Pi_1(s) = a$ and a is a closed *pBPA* term;

Case $s \equiv s_1 \Box s_2$ *with* $\Box \in \{+, \leftthreetimes_\rho\}$. *pBPA* $+ PR \vdash \Pi_1(s) = \Pi_1(s_1) \Box \Pi_1(s_2)$. From the inductive hypothesis there are closed *pBPA* terms t_1 and t_2 such that *pBPA* $+ PR \vdash \Pi_1(s_1) = t_1$ and *pBPA* $+ PR \vdash \Pi_1(s_2) = t_2$. Hence, *pBPA* $+ PR \vdash \Pi_1(s) = t_1 \Box t_2$ and $t_1 \Box t_2$ is a closed *pBPA* term.

`Inductive step.` For $n > 1$ we have the following:

Case $s \equiv a \in A_\delta$. The conclusion follows from axiom $PR1$;

Case $s \equiv a \cdot s_1$. *pBPA* $+ PR \vdash \Pi_n(s) = a \cdot \Pi_{n-1}(s_1)$. By the inductive hypothesis there exists a closed *pBPA* term t_1 such that *pBPA* $+ PR \vdash \Pi_{n-1}(s_1) = t_1$. Thus, we obtain: *pBPA* $+ PR \vdash \Pi_n(s) = a \cdot t_1$ and $a \cdot t_1$ is a closed *pBPA* term;

Case $s \equiv s_1 \Box s_2$ *with* $\Box \in \{+, \leftthreetimes_\rho\}$. *pBPA* $+ PR \vdash \Pi_n(s) = \Pi_n(s_1) \Box \Pi_n(s_2)$. From the inductive hypothesis there are closed *pBPA* terms t_1 and t_2 such that *pBPA* $+ PR \vdash \Pi_n(s_1) = t_1$ and *pBPA* $+ PR \vdash \Pi_n(s_2) = t_2$. Thus, we obtain *pBPA* $+ PR \vdash \Pi_n(s) = t_1 \Box t_2$ and $t_1 \Box t_2$ is a closed *pBPA* term.

□

Theorem 3.2.25 (*Elimination theorem of pBPA* $+ PR$). Let s be a closed term over the signature of *pBPA* $+ PR$. Then there exists a closed *pBPA* term t such that *pBPA* $+ PR \vdash s = t$. □

3.3 Structured operational semantics of *pBPA* and *pBPA* $+ PR$

3.3.1 Introduction

For any concrete process algebra defined in the present thesis we will define a term-deduction system which gives the operational semantics of that theory. Then, using the concept of bisimulation equivalence (an equivalence relation that relates two processes if and only if they exhibit the same behaviour) we obtain a bisimulation model of the given process algebra (of the given axiomatization). The construction of the bisimulation models proposed in Chapter 3, 4 and 5 is based on the same concept and method. In all cases there is a pattern followed consisting of a few phases, even though, each model has its own characteristics that will be described in relevant sections. We start this section by giving a general framework of the main steps. We describe the main ingredients taken into account before a model of one process algebra is fixed. In the second part we give several definition schemas used in the sequel. For a particular process algebra these schemas will be used to come up with precise definitions.

Transitions A term-deduction system $\mathbf{T}_{PRA}$ that brings us towards a model of an untimed process algebra PRA is based on the alternating model of Hansson [71]. It contains two types of transitions, probabilistic transition(s) $\rightsquigarrow$, and action transitions labelled by an atomic action a, $\xrightarrow{a}$ and $\xrightarrow{a}\surd$. For both types of transitions a set of SOS rules (in Plotkin style) are given. The term-deduction system for the operational semantics of the probabilistic process algebra with discrete time introduced in Chapter 5 will have three types of transitions including these two.

An action transition $x \xrightarrow{a} p$ has the standard meaning; by performing action a process x evolves into p. $x \xrightarrow{a} \surd$ denotes that x performs an a action and then terminates.

$p \rightsquigarrow x$ denotes that process p with a non-zero probability, $\pi(> 0)$, chooses to behave like x. Due to uncertain internal behaviour, the process makes a probabilistic transition reaching a process which may continue by executing an atomic action. Note that $\rightsquigarrow$ is an unlabelled transition. The value of the probability π is determined by an additional function introduced later (pg. 51). To motivate why we split probabilistic transitions from the labels denoting probabilities, consider the following example. Let $p \equiv a \leftrightarrows_{1/2} a$. If labelled probabilistic transitions are used intuitively, (without formal semantics yet) due to the first subprocess a, p does a probabilistic transition to a process x labelled with probability $1/2$, and x is such that $x \xrightarrow{a} \surd$. Also, p can perform another probabilistic transition to the process x because of the second subprocess a which is labelled with probability $1/2$ as well. Thus, intuitively we expect that p behaves like x with total probability 1 (also expressed in axiom $PrAC3$). But written in terms of transition relations (presented as sets, but not as multisets), it turns out to be that p does a probabilistic transition to x with probability $1/2$. To avoid this situation we use unlabelled probabilistic transitions and calculate the probability assigned to one transition with the probability distribution function μ (to be introduced below).

Another way to avoid this ambiguity is to add an index to each transition. The index indicates the subprocess the transition of p is derived from (see [81, 56]). In other words, they help to distinguish different occurrences of the same probabilistic transition. For the process $p \equiv a \leftrightarrows_{1/2} a$, one transition to x will be marked by l denoting the left sub-term and the other one will be marked by r denoting the right sub-term. We find this approach technically difficult since the number of indices increases by each new transition. Yet another possibility is to consider a transition $x \rightarrow \alpha$ where α is an appropriate (discrete) probability distribution.

The interplay of the probabilistic and non-deterministic choice integrated in the process algebras from the previous sections (see Remark 3.2.2) has to be implemented in the model as well. For that purpose, every action transition is preceded by an probabilistic transition. It expresses exactly that the process exhibits some internal random behaviour before it performs any action. Moreover, in the model every process starts by executing a probabilistic transition. As shown later, for some processes it will be a trivial probabilistic transition (a probabilistic transition which is assigned probability 1). In a model of a fully probabilistic process algebra probabilistic and action transitions can be joined into one transition.

We use the following abbreviation: $p \not\rightsquigarrow x$ if $\neg(p \rightsquigarrow x)$ for some p and x; $p \xrightarrow{a} x$ if $\neg(p \xrightarrow{a} x)$ for some p and x; $p \xrightarrow{a}$ if $\forall x : p \xrightarrow{a} x$; $p \rightsquigarrow M$ if $\exists x \in M : p \rightsquigarrow x$.

Domain of model Let us summarize what has been said above. There are two types of transitions, probabilistic and action. Therefore, any process (different from the deadlock process) makes either a probabilistic or an action transition(s). In the alternating model, probabilistic transitions alternate with action transitions. Namely, one process makes a probabilistic transition and it reaches a process that makes an action transition or it may deadlock. Otherwise, a process makes an action transition and it terminates or it reaches a process that performs a probabilistic transition. This approach entails

that two types of processes should be distinguished; processes that make probabilistic transitions, will be called *static processes*, and processes that make action transitions or deadlock, called *dynamic processes*. It turns out that the set of static processes, $\mathbb{SP}^{(\infty)}(PRA)$, will be containing the interpretations of the terms (including guarded terms if recursion is considered) in our PRA. The set of dynamic processes, denoted $\mathbb{DP}^{(\infty)}(PRA)$, should contain all processes that do not make probabilistic transitions but may perform an action transition. For instance, $a \leftthreetimes_\pi b$ should not be considered as a $\mathbb{DP}^{(\infty)}(PRA)$ process. It contains a probabilistic choice that ought to be resolved. Thus, this process can make a probabilistic transition to a process x which does $x \xrightarrow{a} \surd$ and it can make a probabilistic transition to a process y which does $y \xrightarrow{b} \surd$. (Therefore, x (y) should be defined equivalent to any process that can do $\xrightarrow{a} \surd$ ($\xrightarrow{b} \surd$) and nothing else, but not to a (b).) And since x and y make only action transitions they should be classified as $\mathbb{DP}^{(\infty)}(PRA)$ processes.

To define $\mathbb{DP}^{(\infty)}(PRA)$ processes, one can think of the following solutions. First, simply $\mathbb{SP}^{(\infty)}(PRA)$ is split into two subsets. For instance if we treat *pBPA* without recursion, then the set of dynamic processes $\mathbb{DP}(\textit{pBPA})$ may be defined to coincide with the set $\mathcal{D}(\textit{pBPA})$. Then, the other subset, $\mathbb{SP}^{\infty}(PRA) \setminus \mathbb{DP}^{\infty}(PRA)$, defines the set of static processes. Thus, for the process above we will have that $a \leftthreetimes_\pi b \rightsquigarrow a \xrightarrow{a} \surd$ and $a \leftthreetimes_\pi b \rightsquigarrow b \xrightarrow{b} \surd$. Hence, it becomes obvious that the rule $a \xrightarrow{a} \surd, a \in A$ has to be included in the semantics. Now the question arises: do we need rule $a \rightsquigarrow a$ for $a \in A_\delta$ as well? If the rule $a \rightsquigarrow a$ is not included, then the structure of the deduction rules becomes misleading. To illustrate it, take the process $(a \leftthreetimes_\pi b) + c$. It is expected that the following transitions occur: $(a \leftthreetimes_\pi b) + c \rightsquigarrow a + c$ and $(a \leftthreetimes_\pi b) + c \rightsquigarrow b + c$. Hence, a rule in the following form has to be part of the semantics: $\dfrac{x \rightsquigarrow u, y \xrightarrow{a} \surd}{x + y \rightsquigarrow u + y}$. In our opinion this rule is not very intuitive since it "looks" ahead at action transitions of y which do not play a role in the first step of $x + y$.

If we do have the rule $a \rightsquigarrow a$, then a possibility of an infinite sequence of transitions for a finite process arises, for instance, $a \rightsquigarrow a \rightsquigarrow a \ldots$.

In [71] (see also [70]) a distinction between probabilistic and non-deterministic expressions is made already in the definition of the theory. This can be done there because the set of expressions is restricted in comparison to our set of terms. For instance, it does not allow expressions like $(a \leftthreetimes_\pi b) + (c \leftthreetimes_\rho d)$.

For the reasons mentioned above we choose another approach. Actually, we introduce an auxiliary notation for dynamic processes. These processes are involved only in the definition of the deduction rules (operational semantics), and they will not be considered as interpretations of terms in PRA.

To give a flavour, first in the set $\mathbb{SP}^{\infty}(PRA)$ we distinguish processes that perform only one trivial probabilistic transition (the set $\mathbb{D}^{\infty}(PRA)$) (e.g. $a + a$ but not $a \leftthreetimes_{1/2} a$) from processes with non-trivial probabilistic transitions. Then, for each process p which performs only a trivial probabilistic transition (e.g. $a + a$) we introduce a counterpart $\breve{p}$ which represents a dynamic process (e.g. $\breve{a} + \breve{a}$). And we assume that with probability 1, p does a probabilistic transition to $\breve{p}$. In other words, for every p from $\mathbb{D}^{\infty}(PRA)$ there is a $\breve{p}$ in $\mathbb{DP}^{\infty}(PRA)$ such that $p \rightsquigarrow \breve{p}$ with probability 1.

In order to realize this idea an enlarged signature of $\mathbf{T}_{PRA}$ is required. In return we obtain simpler and more intuitive deduction rules. The new signature, denoted $\breve{\Sigma}_{PRA}$, is the signature of PRA extended *only* by a set of new constants $\breve{A}_\delta = \{\breve{a} : a \in A_\delta\}$. Let us note that $A_\delta \subseteq \mathbb{SP}^{(\infty)}(PRA)$ and $\breve{A}_\delta \subseteq \mathbb{DP}^{(\infty)}(PRA)$ for any presented process algebra.

Back to the example above, the transitions of the process $(a \leftthreetimes_\pi b) + c$ become: $(a \leftthreetimes_\pi b) + c \rightsquigarrow \breve{a} + \breve{c} \xrightarrow{a} \surd$, $(a \leftthreetimes_\pi b) + c \rightsquigarrow \breve{a} + \breve{c} \xrightarrow{c} \surd$, $(a \leftthreetimes_\pi b) + c \rightsquigarrow \breve{b} + \breve{c} \xrightarrow{b} \surd$ and $(a \leftthreetimes_\pi b) + c \rightsquigarrow \breve{b} + \breve{c} \xrightarrow{c} \surd$.

Next, we give general frameworks of definitions of the just described sets. As any considered model will be an extension of the model of *pBPA*, the operators of *pBPA* are explicitly integrated

in these schemas. First we give the definition of the total domain that is generated by the signature $\breve{\Sigma}_{PRA}$. Then, we omit the processes not of any importance and produce the real domain that we use further on.

Definition 3.3.1. For signature $\breve{\Sigma}_{PRA}$ which contains $A_\delta \cup \breve{A}_\delta$ and the operators: $+$, $\cdot$, Π_n and $\leftthreetimes_\pi$ ($n \geq 1, \pi \in \langle 0, 1\rangle$) we define a set $TotalDomain^{(\infty)}(PRA)$ as the smallest set for which:

1. $A_\delta \subseteq TotalDomain^{(\infty)}(PRA), \breve{A}_\delta \subseteq TotalDomain^{(\infty)}(PRA)$;

2*. $< X|E > \in TotalDomain^{(\infty)}(PRA)$ where $< X|E >$ is a constant introduced for a solution of the guarded recursive specification E in PRA with root variable X;[3]

3. $TotalDomain^{(\infty)}(PRA)$ is closed under all operators in $\breve{\Sigma}_{PRA}$.

The $TotalDomain^{(\infty)}(PRA)$ is a very large set with respect to the set of processes defined by terms over PRA and recursion. Therefore, we are interested only in those processes from $TotalDomain(PRA)^{(\infty)}$ that can be reached, by the means of transitions, from the interpretation of a term in PRA (e.g. $\breve{a} \cdot \breve{a}$ is not such a process).

Definition 3.3.2. For a given process algebra PRA whose signature contains the $+$, $\cdot$, Π_n ($n \geq 1$) and $\leftthreetimes_\pi$ ($\pi \in \langle 0, 1\rangle$) operators, the set of *static processes* $\mathbb{SP}^{(\infty)}(PRA)$ is inductively defined in the following way:

1. $A_\delta \subseteq \mathbb{SP}^{(\infty)}(PRA)$;

2*. $< X|E > \in \mathbb{SP}^{\infty}(PRA)$; (see footnote 3)

3. if $p, q \in \mathbb{SP}^{(\infty)}(PRA)$, then $p \cdot q \in \mathbb{SP}^{(\infty)}(PRA)$;

4. if $p, q \in \mathbb{SP}^{(\infty)}(PRA)$, then $p + q \in \mathbb{SP}^{(\infty)}(PRA)$;

5. if $p, q \in \mathbb{SP}^{(\infty)}(PRA)$, then $p \leftthreetimes_\pi q \in \mathbb{SP}^{(\infty)}(PRA)$;

6. if $p \in \mathbb{SP}^{(\infty)}(PRA)$, then $\Pi_n(p) \in \mathbb{SP}^{(\infty)}(PRA), n \geq 1$;

7. new items can be added for the other operators of PRA.

Definition 3.3.3. A special subset of $\mathbb{SP}^{(\infty)}(PRA)$, the set of *trivial* static processes $\mathbb{D}^{(\infty)}(PRA)$, is inductively defined as:

1. $A_\delta \subseteq \mathbb{D}^{(\infty)}(PRA)$;

2. if $s \in \mathbb{D}^{(\infty)}(PRA)$ and $t \in \mathbb{SP}^{(\infty)}(PRA)$ then $s \cdot t \in \mathbb{D}^{(\infty)}(PRA)$;

3. if $s, t \in \mathbb{D}^{(\infty)}(PRA)$ then $s + t \in \mathbb{D}^{(\infty)}(PRA)$;

4. if $s \in \mathbb{D}^{(\infty)}(PRA)$ then $\Pi_n(s) \in \mathbb{D}^{(\infty)}(PRA), n \geq 1$;

5. this definition can be extended with additional statements for the other operators of PRA other than $\leftthreetimes_\pi$.

[3] These elements are added only for models with infinite processes.

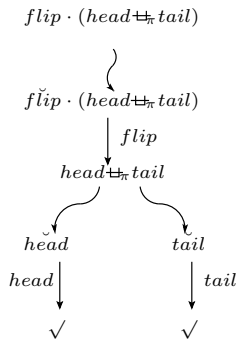


Figure 3.1: Operational semantics of the process s.

A set of *dynamic processes* $\mathbb{DP}^{(\infty)}(PRA)$ is defined on basis of $\mathbb{D}^{(\infty)}(PRA)$ in the following way:

Definition 3.3.4. Let $\varphi : \mathbb{D}^{(\infty)}(PRA) \to TotalDomain^{(\infty)}(PRA)$ be defined in the following way:

1. $\varphi(a) = \breve{a}$ for each $a \in A_\delta$;
2. $\varphi(s \cdot t) = \varphi(s) \cdot t$;
3. $\varphi(s + t) = \varphi(s) + \varphi(t)$;
4. $\varphi(\Pi_n(s)) = \Pi_n(\varphi(s)), n \geq 1$;
5. depending on the fifth item in the definition of $\mathbb{D}^{(\infty)}(PRA)$, additional equalities for φ may be stated.

$\mathbb{DP}^{(\infty)}(PRA) = \varphi(\mathbb{D}^{(\infty)}(PRA))$. Shortly, $\varphi(s)$ will be denoted by $\breve{s}$.

Thus, the domain $\mathbb{PT}^{(\infty)}(PRA)$ of the model of PRA is the set of all static and dynamic processes, that is, $\mathbb{PT}^{(\infty)}(PRA) = \mathbb{SP}^{(\infty)}(PRA) \cup \mathbb{DP}^{(\infty)}(PRA)$.

Example 3.3.5. The operational semantics of the process $s \equiv flip \cdot (head \leftthreetimes_\pi tail)$ (pg. 35) has the transitions shown in Figure 3.1. □

Finally, we give the notion of a *guarded process* that becomes important in models with infinite processes. It is clear that they present interpretations of the guarded terms of PRA.

Definition 3.3.6. If g is a (guarded) term in PRA and E is a guarded recursive specification such that $\mathcal{V}(g) \subseteq \mathcal{V}(E)$ then the (*guarded*) *process* $< g|E >$ in the bisimulation model of PRA is obtained from the interpretation of g when every variable Y in g is replaced by $< Y|E >$.

Remark 3.3.7. Instead writing all over again: "...g is a (guarded) term and E is a guarded recursive specification such that $\mathcal{V}(g) \subseteq \mathcal{V}(E)$, then $< g|E >$ is a (guarded) process ..." we say in short that "...$< g|E >$ is a (guarded) process ...". And it is clear that if g is a guarded term, then the inductive structure of g may be engaged in any inductive proof of a property of $< g|E >$. Also it is clear that $< g|E >$ does not contain any variable, that is $< g|E > \in \mathbb{SP}^{\infty}(PRA)$, since all variables are replaced by constants according to the specification E. In fact, the interpretation $< g|E >$ of the (guarded) term g does depend completely on E; it gives the context into which g is considered. However, many

properties of the guarded process $< g|E >$ (as we see later) do not depend on the values assigned to the variables of g, but rather on the structure of guarded processes. In that case we do not need to relate g to one particular E, but we need to focus only on the structure on g. And, if the proof of one property is based on the structure on g, then it is valid for any $< g|E >$ for any possible E. Then we talk about "guarded process g" only as interpretation of "guarded term g" (we do not introduce a new notation for it). And, once again, the inductive definition of guarded terms (Definition 3.2.8) induces the same structure on guarded processes. To justify this, let us consider the guarded term $g \equiv a \cdot X \leftthreetimes_{1/2} b \cdot Y$ where X and Y are variables. It is clear that g is a guarded term in ***pBPA***. $E_1 = \{X = c + d \cdot Y, Y = b \cdot X\}$ is a guarded recursive specification in ***pBPA***. Then $< g|E_1 >$ is the guarded process $a \cdot < X|E_1 > \leftthreetimes_{1/2} b \cdot < Y|E_1 >$ where $< X|E_1 >, < Y|E_1 >$ is a solution of E_1 in the considered model of ***pBPA***. But if we consider guarded term g in another context, for example, in the context of another guarded recursive specification $E_2 = \{X = c \cdot Y, Y = d \cdot X\}$, then we obtain another guarded process $< g|E_2 >= a \cdot < X|E_2 > \leftthreetimes_{1/2} b \cdot < Y|E_2 >$ and it is obvious that $< g|E_1 >$ and $< g|E_2 >$ are not equivalent.

Still there are some properties that do not depend on the interpretation of X and Y, but certainly depend on the structure of g. For example, whatever guarded recursive specification E with X and Y as variables is considered, we are certain that $< g|E >$ can reach only two processes with a non-zero probability.

Probability distribution function A *probability distribution function* (PDF) in the bisimulation model of a given process algebra PRA is a map $\mu : \mathbb{PT}^{(\infty)}(PRA) \times \mathbb{PT}^{(\infty)}(PRA) \to [0, 1]$ defined inductively on the structure of the processes. Namely, if $p \equiv q * r$ where $*$ is an operator in PRA, the probability by which p behaves in a certain way depends on the probabilistic behaviour of its sub-processes q and r. That is, $\mu(p, \_) = func(\mu(q, \_), \mu(r, \_))$ for some real function $func(\_, \_)$. This function shows the effect the sub-processes have on the total probability[4]. In Table 3.6 and 3.7 we give the equalities for the constants and the $+$, $\cdot$ and $\leftthreetimes_\pi$ operators. Additional equalities for the other operators of PRA (if there are such) may be stated to complete the definition of the PDF.

$\mu(a, \breve{a})$	$=$	1,	
$\mu(\delta, \breve{\delta})$	$=$	1, if δ is in the signature	

Table 3.6: Equalities that define PDF's (part 1 - constants)

$\mu(x \cdot y, x' \cdot y)$	$=$	$\mu(x, x')$,	
$\mu(x + y, x' + y')$	$=$	$\mu(x, x') \cdot \mu(y, y')$,	
$\mu(x \leftthreetimes_\pi y, z)$	$=$	$\pi\mu(x, z) + (1 - \pi)\mu(y, z)$,	
$\mu(x, u)$	$=$	0	$otherwise$

Table 3.7: Equalities that defined PDF's (part 2 - basic operators)

One can note that the probability by which process p behaves like process x depends at the first place on the structure of p and x. The equalities in Table 3.6 say that the constants can make only

[4]In mathematical terminology, $\mu(p, \_)$ is the distribution function of a random variable derived from the random variables with distribution functions $\mu(q, \_)$ and $\mu(r, \_)$.

a trivial probabilistic transition. The equality for the $+$ operator is obtained as a probability of the independent events: "p behaves like x" and "q behaves like y". And the equality for $\leftplus_\pi$ operator is obtained as a total probability of the events "p behaves like x" and "q behaves like x" taking into account the conditional probabilities by which p or q is chosen (π and $1-\pi$ resp.) (see [99]).

To define probabilistic bisimulation (a la Larsen-Skou [86]), we first need to define the cumulative probability distribution function which extends the PDF over a set of processes. For a given process p and a set of processes M it computes the total probability by which process p chooses to behaves like any element in M. The formal definition follows.

Definition 3.3.8. The *cumulative* probability distribution function (cPDF) is a map $\mu^* : \mathbb{PT}^{(\infty)}(PRA) \times \mathcal{P}(\mathbb{PT}^{(\infty)}(PRA)) \to [0,1]$ defined as: $\mu^*(p, M) = \sum_{x \in M} \mu(p, x)$ for each $p \in \mathbb{PT}^{(\infty)}(PRA)$ and $M \subseteq \mathbb{PT}^{(\infty)}(PRA)$.

From now on μ^* will be simply denoted as μ. And by "PDF" function we will mean a probability distribution function whose definition is based on the schema in Table 3.6 and 3.7 and for which μ^* is well defined. Two important features of the PDF's are stated in the following two propositions. The first property follows directly from the definition of probability measure. The second one is crucial for many proofs in the remainder of the thesis, in particular for the proof of the Soundness theorem. Informally, if M is a equivalence class that corresponds to the left-hand side of an axiom, then M' is the equivalence class corresponding to the right-hand side of the same axiom, and the bijection $'$ maps the left-hand side into the right-hand side. In that way the condition which is sufficient to be checked according to the proposition - for each $m \in M$ whether $\mu(p, m) = \mu(q, m')$ - becomes trivial.

Proposition 3.3.9. Let $M_i \subseteq \mathbb{PT}^{(\infty)}(PRA), i \in I$ for some finite or countably infinite index set I, such that $M_i \cap M_j = \emptyset$ for each $i, j \in I, i \neq j$. Then $\mu(p, \bigcup_{i \in I} M_i) = \sum_{i \in I} \mu(p, M_i)$. □

Proposition 3.3.10. Let $' : M \to M'$ be a bijection such that for each $m \in M$, $\mu(p, m) = \mu(q, m')$. Then $\mu(p, M) = \mu(q, M')$.

Proof. Since $' : M \to M'$ is a bijection such that $\mu(p, m) = \mu(q, m')$ for every $m \in M$:
$\mu(p, M) = \sum_{m \in M} \mu(p, m) = \sum_{m \in M} \mu(q, m') = \mu(q, \bigcup_{m \in M} \{m'\}) = \mu(q, M')$. □

Bisimulation After the term-deduction system $\mathbf{T}_{PRA}$ is defined the model of the process algebra PRA is obtained as a quotient set[5] of $\mathbb{SP}^{(\infty)}(PRA)$ by bisimulation equivalence. In Chapter 3, 4 and 5, the strong variant of probabilistic bisimulation is employed. In Chapter 6, where abstraction is introduced, the definition of bisimulation relation essentially differs from the present one. We leave that for later. Now, we give the definition of the strong probabilistic bisimulation relation [86] which is used in the following three chapters. (Note: in the chapter of timed process algebra the definition of the strong probabilistic bisimulation will be slightly modified.)

Definition 3.3.11. Let R be an equivalence relation on $\mathbb{PT}^{(\infty)}(PRA)$. R is a *probabilistic bisimulation* if:

1. if pRq and $p \rightsquigarrow s$ then there is a term t such that $q \rightsquigarrow t$ and sRt;
2. if sRt and $s \xrightarrow{a} p$ for some $a \in A$, then there is a term q such that $t \xrightarrow{a} q$ and pRq;

[5] The set of all equivalence classes.

3. if sRt and $s \xrightarrow{a} \surd$, then $t \xrightarrow{a} \surd$;

4. if pRq, then $\mu(p, M) = \mu(q, M)$ for each $M \in \mathbb{PT}^{(\infty)}(PRA)/R$.

If there is a probabilistic bisimulation R such that pRq, then p is *probabilistically bisimilar* to q, denoted by $p \underline{\leftrightarrow} q$.

Different from a bisimulation relation used in the construction of the bisimulation models of other *ACP*-like process algebras, here, a probabilistic bisimulation relation R is required to be an equivalence relation. This requirement is related with the fourth clause in Definition 3.3.11 which says that in addition to an existence of a bisimulation of probabilistic and action transitions between two processes considered as bisimilar, the cumulative probabilities of both processes for the R equivalence classes must be equal. For example, the processes presented by the transition systems $a)$ and $b)$ in Figure 3.2 are not probabilistically bisimilar but the processes $a)$ and $c)$ are bisimilar[6].

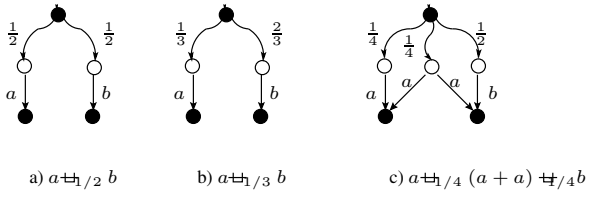


Figure 3.2: An example of (not) bisimilar processes.

Let us assume that a PDF function μ is defined on $\mathbb{PT}^{(\infty)}(PRA)$.

Proposition 3.3.12. If R_1 and R_2 are probabilistic bisimulation relations on $\mathbb{PT}^{(\infty)}(PRA)$, then $R = Eq(R_1 \circ R_2)$ is a probabilistic bisimulation relation on $\mathbb{PT}^{(\infty)}(PRA)$ as well[7].

Proof. Suppose that $(p, r) \in R$ for some $p, r \in \mathbb{PT}^{(\infty)}(PRA)$. We need to prove that p and r can mimic each other on every transition and on PDF as well (as given in the definition of probabilistic bisimulation). From the definition of R it follows that there exists $q \in \mathbb{PT}^{(\infty)}(PRA)$ such that $(p, q) \in R_1$ and $(q, r) \in R_2$. (1)

Probabilistic transitions. If $p \rightsquigarrow u$, then there exists v such that $q \rightsquigarrow v$ and uR_1v. Then there exists w such that $r \rightsquigarrow w$ and vR_2w, and uRw.

Action transitions. Let $p \xrightarrow{a} s$ for some $a \in A$ and s. Then there exists t such that $q \xrightarrow{a} t$ and sR_1t from which it follows that there exists o such that $r \xrightarrow{a} o$ and tR_2o. Thus, sRo.

Action termination. If $p \xrightarrow{a} \surd$ for some $a \in A$ then $q \xrightarrow{a} \surd$ and also $r \xrightarrow{a} \surd$.

PDF. Let be $M \in \mathbb{PT}^{(\infty)}(PRA)/R$. Since R_1 and R_2 are subsets of R (all of them are equivalence relations on $\mathbb{PT}^{(\infty)}(PRA)$) $M = \bigcup_{i \in I_1} M_{i1} = \bigcup_{j \in I_2} M_{j2}$ for $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ and for some equivalence classes $M_{i1} \in \mathbb{PT}^{(\infty)}(PRA)/R_1$, $i \in I_1$ and $M_{j2} \in \mathbb{PT}^{(\infty)}(PRA)/R_2$, $j \in I_2$. From Proposition 3.3.9 and (1) it follows that:

[6]The way processes are presented in this example is not very precise (it is informal), that is, it does not meet the formal definition given later.

[7]Once again $Eq(\alpha)$ denotes the equivalence closure of relation α.

$$\mu(p, M) = \mu(p, \bigcup_{i\in I_1} M_{i1}) = \sum_{i\in I_1} \mu(p, M_{i1}) = \sum_{i\in I_1} \mu(q, M_{i1}) = \mu(q, \bigcup_{i\in I_1} M_{i1}) =$$
$$\mu(q, M) = \mu(q, \bigcup_{j\in I_2} M_{j2}) = \sum_{j\in I_2} \mu(q, M_{j2}) = \sum_{j\in I_2} \mu(r, M_{j2}) = \mu(r, \bigcup_{j\in I_2} M_{j2}) = \mu(r, M).$$

□

Proposition 3.3.13. $\underline{\leftrightarrow}$ is a probabilistic bisimulation relation on $\mathbb{PT}^{(\infty)}(PRA)$.

Proof. The result that $\underline{\leftrightarrow}$ is a reflexive and symmetric relation is trivial and from Proposition 3.3.12 the transitivity of $\underline{\leftrightarrow}$ follows easily. Thus $\underline{\leftrightarrow}$ is an equivalence relation.

Now we need to prove that $\underline{\leftrightarrow}$ satisfies the four clauses of Definition 3.3.11. Suppose that $p \underline{\leftrightarrow} q$ for some $p, q \in \mathbb{PT}^{(\infty)}(PRA)$. From the definition of $\underline{\leftrightarrow}$ it follows that there exists a bisimulation relation R such that $(p, q) \in R$. The proofs that p and q simulate each other on probabilistic and action transitions are trivial.

PDF. Suppose that $M \in \mathbb{PT}^{(\infty)}(PRA)/\underline{\leftrightarrow}$. Since R and $\underline{\leftrightarrow}$ are equivalence relations defined on the same set and $R \subseteq \underline{\leftrightarrow}$, then $M = \bigcup_{i\in I} M_i$ for some $M_i \in \mathbb{PT}^{(\infty)}(PRA)/R$, $i \in I, I \neq \emptyset$. Hence,

$$\mu(p, M) = \mu(p, \bigcup_{i\in I} M_i) = \sum_{i\in I} \mu(p, M_i) = \sum_{i\in I} \mu(q, M_i) = \mu(q, \bigcup_{i\in I} M_i) = \mu(q, M).$$

□

From Definition 3.3.11 and Proposition 3.3.13 it follows that $\underline{\leftrightarrow}$ is the maximal probabilistic bisimulation relation on $\mathbb{PT}^{(\infty)}(PRA)$.

Model Finally, after proving that $\underline{\leftrightarrow}$ is a congruence on $\mathbb{PT}^{(\infty)}(PRA)$, the model of PRA has the quotient set of $\mathbb{SP}^{(\infty)}(PRA)$ by the equivalence relation $\underline{\leftrightarrow}$ as its domain, that is, $\mathcal{M}^{(\infty)}_{PRA} = \mathbb{SP}^{(\infty)}(PRA)/\underline{\leftrightarrow}$.

3.3.2 Model of *pBPA* + PR and properties of the model

Following the pattern described before, we construct the bisimulation model of *pBPA* + PR with infinite processes and prove some of its properties. First, we define the bisimulation model with infinite processes introduced as solutions of guarded recursion in *pBPA* + PR. Second, we reduce it to the bisimulation model with only finite processes, for which we prove the completeness property.

(Note: Even though in the previous section we presented several process algebras, *pBPA* + PR and *pBPA* which are extensions of $pBPA_{-\delta}$ which is obtained from *fpBPA*, in this section we deal only with *pBPA* + PR and *pBPA*. For the algebras left out, the semantics can easily be deduced.)

Let $A_{<X|E>}$ be the set of all constants $< X|E >$ for X a process variable and E a guarded recursive specification in *pBPA* + PR. The operational semantics of *pBPA* + PR is given by the term-deduction system $\mathbf{T}_{pBPA+PR} = (\breve{\Sigma}_{pBPA+PR}, \mathbf{DR}_{pBPA+PR})$ with $\breve{\Sigma}_{pBPA+PR} = (A_\delta \cup \breve{A}_\delta \cup A_{<X|E>}, +, \cdot, \leftthreetimes_\pi, \Pi_n)$ and with the deduction rules shown in Table 3.8+3.9 and the rules for action transitions given in Table 3.10+3.11. With PRA replaced by *pBPA* + PR the items 1-6 in Definition 3.3.2 (on pg. 49) define the set of static processes $\mathbb{SP}^\infty(pBPA + PR)$, and the items 1-4 in Definition 3.3.3 (on pg. 49) and 3.3.4 (on pg. 50) define the set of trivial static processes $\mathbb{D}^\infty(pBPA + PR)$ and the set of dynamic processes $\mathbb{DP}^\infty(pBPA + PR)$, respectively. The definition of the PDF function μ on $\mathbb{PT}^\infty(pBPA + PR)$ is given in Definition 3.3.14.

Definition 3.3.14. (PDF for *pBPA* + PR) The probability distribution function on $\mathbb{PT}^\infty(pBPA + PR)$ is defined by the equalities in Table 3.6 and 3.7 and 3.12.

$$a \rightsquigarrow \breve{a} \qquad \delta \rightsquigarrow \breve{\delta}$$

$$\frac{x \rightsquigarrow x'}{x \cdot y \rightsquigarrow x' \cdot y} \qquad \frac{x \rightsquigarrow x', y \rightsquigarrow y'}{x + y \rightsquigarrow x' + y'} \qquad \frac{x \rightsquigarrow z}{x \leftplus_\pi y \rightsquigarrow z, y \leftplus_\pi x \rightsquigarrow z}$$

Table 3.8: Probabilistic transitions for *pBPA*.

$$\frac{\langle t_X | E \rangle \rightsquigarrow u}{\langle X | E \rangle \rightsquigarrow u} \qquad \frac{x \rightsquigarrow x'}{\Pi_n(x) \rightsquigarrow \Pi_n(x')}$$

Table 3.9: Probabilistic transitions for recursion and projection.

Properties of the PDF Now, since the definition of the probability distribution function μ of *pBPA*+ PR is completed, we can prove that it is well defined. This proof goes in three steps. The third step is the main result and the other two are only auxiliary results used in its proof. In fact, they describe the part of the proof in the third step concerning $< X|E >$ constants. Having this result, it is easy to prove that μ is well defined on $\mathbb{PT}^\infty$(*pBPA* + PR) using the inductive structure of the elements of $\mathbb{PT}^\infty$(*pBPA* + PR).

Proposition 3.3.15. If t is a guarded process, then $\mu(t, u)$ is well defined for any $u \in \mathbb{PT}^\infty$(*pBPA* + PR).

Proof. The proof is given by induction on the structure of guarded terms (see Remark 3.3.7).

Case $t \equiv a, a \in A_\delta$. For any u, $\mu(a, u) = \begin{cases} 1, & if\ u \equiv \breve{a} \\ 0, & otherwise \end{cases}$. Hence, for $t \equiv a$, $\mu(t, u)$ is defined.

Case $t \equiv g \cdot s$. For any u, $\mu(g \cdot s, u) = \begin{cases} \mu(g, v), & if\ u \equiv v \cdot s \\ 0, & otherwise \end{cases}$. Since $\mu(g, v)$ is defined, it follows that $\mu(g \cdot s, u)$ is defined.

Case $t \equiv \Pi_n(g)$. For any u, $\mu(\Pi_n(g), u) = \begin{cases} \mu(g, v), & if\ u \equiv \Pi_n(v) \\ 0, & otherwise \end{cases}$. Since $\mu(g, v)$ is defined, $\mu(\Pi_n(g), u)$ is defined as well.

Case $t \equiv g + h$. For any u, $\mu(g+h, u) = \begin{cases} \mu(g, v) \cdot \mu(h, w), & if\ u \equiv v + w \\ 0, & otherwise \end{cases}$. Since $\mu(g, v)$ and $\mu(h, w)$ are defined, it follows that $\mu(g + h, u)$ is defined.

Case $t \equiv g \leftplus_\pi h$. For any u, $\mu(g \leftplus_\pi h, u) = \pi \cdot \mu(g, u) + (1 - \pi) \cdot \mu(h, w)$ and since $\mu(g, u)$ and $\mu(h, u)$ are defined, it follows that $\mu(g \leftplus_\pi h, u)$ is defined.

□

Proposition 3.3.16. Let E be a guarded recursive specification with the root variable X. Then $\mu(< X|E >, u)$ is defined for any u.

$$\breve{a} \xrightarrow{a} \surd \qquad \frac{x \xrightarrow{a} x'}{x \cdot y \xrightarrow{a} x' \cdot y} \qquad \frac{x \xrightarrow{a} \surd}{x \cdot y \xrightarrow{a} y}$$

$$\frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x', y + x \xrightarrow{a} x'} \qquad \frac{x \xrightarrow{a} \surd}{x + y \xrightarrow{a} \surd, y + x \xrightarrow{a} \surd}$$

Table 3.10: Deduction rules for action transitions for *pBPA*.

$$\frac{x \xrightarrow{a} x'}{\Pi_{n+1}(x) \xrightarrow{a} \Pi_n(x')} \qquad \frac{x \xrightarrow{a} \surd}{\Pi_n(x) \xrightarrow{a} \surd} \qquad \frac{x \xrightarrow{a} x'}{\Pi_1(x) \xrightarrow{a} \surd}$$

Table 3.11: Action transitions for projection.

Proof. We make the following observation. Lemma 3.2.13 and the definition of the μ function over $< Y|E >$ constants (Table 3.12) guarantee that it is sufficient to consider only completely guarded recursive specifications. Therefore, $\mu(< Y|E >, u)$ is well defined if $\mu(t_Y, u)$ is well defined. As t_Y is a guarded term $\mu(t_Y, u)$ is well defined according to Proposition 3.3.15. □

Example 3.3.17. Let us consider the following recursive specification:

$$E = \{Y = (Z_1 + Z_2) \leftthreetimes_{0.5} Z_3,\ Z_1 = a \cdot Z_1 + Z_2,\ Z_2 = c \cdot Z_2,\ Z_3 = b \cdot Z_3\}.$$

The relation $\xrightarrow{u}$ of E is shown in Figure 3.3. If $u \in \mathbb{PT}^{\infty}(\textit{pBPA} + PR)$, then the definition of μ induces the following system of equations in $\mathbb{R}$:

$\mu(< Y|E >, u) =$ $0.5 \cdot \mu(< Z_1|E >, u_1) \cdot \mu(< Z_2|E >, u_2)$
$+0.5 \cdot \mu(< Z_3|E >, u)$, if $u \equiv u_1 + u_2$
$\mu(< Z_1|E >, u_1) =$ $\mu(a \cdot < Z_1|E >, u_{11}) \cdot \mu(< Z_2|E >, u_{12})$, if $u_1 \equiv u_{11} + u_{12}$
$\mu(< Z_2|E >, u_2) =$ $\mu(c, \breve{c})$, if $u_2 \equiv \breve{c} \cdot < Z_2|E >$
$\mu(a \cdot < Z_1|E >, u_{11}) =$ $\mu(a, \breve{a})$, if $u_{11} \equiv \breve{a} \cdot < Z_1|E >$
$\mu(< Z_3|E >, u) =$ 0, if $u \equiv u_1 + u_2 \not\equiv \breve{b} \cdot < Z_3|E >$

Let us emphasize that since $t_{Z_2} \equiv c \cdot Z_2$ and $t_{Z_3} \equiv b \cdot Z_3$ are guarded terms, the values $\mu(t_{Z_2}, u)$ and $\mu(t_{Z_3}, u)$ are defined for every u according to Proposition 3.3.15. Also by the definition $\mu(< Z_2|E >, u) = \mu(t_{Z_2}, u)$ and $\mu(< Z_3|E >, u) = \mu(t_{Z_3}, u)$. It implies that $\mu(< Z_2|E >, u)$ and $\mu(< Z_3|E >, u)$ are defined as well.

Lemma 3.3.18. μ is well-defined on $\mathbb{PT}(\textit{pBPA} + PR)$.

Proof. Since $\mathbb{PT}^{\infty}(\textit{pBPA} + PR)$ is a disjoint union of $\mathbb{SP}^{\infty}(\textit{pBPA} + PR)$ and $\mathbb{DP}^{\infty}(\textit{pBPA} + PR)$ we split the proof into two parts, one which goes by induction on the structure of $\mathbb{SP}^{\infty}(\textit{pBPA} + PR)$ processes and the other one by induction on the structure of $\mathbb{DP}^{\infty}(\textit{pBPA} + PR)$ processes.

Case $\mathbb{SP}^{\infty}(\textit{pBPA} + PR)$ *processes.* Let p be a $\mathbb{SP}^{\infty}(\textit{pBPA} + PR)$ process.

$\mu(\Pi_n(x), \Pi_n(z))$	$=$	$\mu(x, z)$	$n \geq 1$
$\mu(< X\|E >, z)$	$=$	$\mu(< t_X\|E >, z)$	

Table 3.12: Equalities that complete PDF for *pBPA* $+ PR$ (part 3).

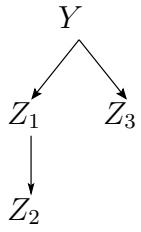


Figure 3.3: Tree representation of $\xrightarrow{u}$ relation.

Case $p \equiv a \in A_\delta$. For any u, $\mu(a, u) = \begin{cases} 1, & if\ u \equiv \breve{a} \\ 0, & otherwise \end{cases}$. Hence, for $p \equiv a$, $\mu(p, u)$ is defined;

Case $p \equiv < X|E >$ *for a guarded recursive specification* E *with the root* X. The result follows from Proposition 3.3.16;

Case $p \equiv q \cdot r$. For any u, $\mu(q \cdot r, u) = \begin{cases} \mu(q, v), & if\ u \equiv v \cdot r \\ 0, & otherwise \end{cases}$. Since $\mu(r, v)$ is defined by the induction hypothesis, it follows that $\mu(q \cdot r, u)$ is defined as well;

Case $p \equiv \Pi_n(q)$. For any u, $\mu(\Pi_n(p), u) = \begin{cases} \mu(q, v), & if\ u \equiv \Pi_n(v) \\ 0, & otherwise \end{cases}$. Since $\mu(q, v)$ is defined by the induction hypothesis, $\mu(\Pi_n(q), u)$ is defined as well;

Case $p \equiv q + r$. For any u, $\mu(q + r, u) = \begin{cases} \mu(q, v) \cdot \mu(r, w), & if\ u \equiv v + w \\ 0, & otherwise \end{cases}$. Since $\mu(q, v)$ and $\mu(r, w)$ are defined, it follows that $\mu(q + r, u)$ is defined as well;

Case $p \equiv q \leftthreetimes_\pi r$. For any u, $\mu(q \leftthreetimes_\pi r, u) = \pi \cdot \mu(q, u) + (1 - \pi) \cdot \mu(r, w)$. Since $\mu(q, u)$ and $\mu(r, u)$ are defined, it follows that $\mu(q \leftthreetimes_\pi r, u)$ is defined.

Case $\mathbb{DP}^\infty$(*pBPA* $+ PR$) *processes.* Let us suppose that $p \in \mathbb{DP}^\infty$(*pBPA* $+ PR$). Using induction we prove that $\mu(p, u) = 0$ which implies that it is well defined.

Case $p \equiv \breve{a}, a \in A_\delta$. By the definition of the PDF $\mu(\breve{a}, u) = 0$ for any u;

Case $p \equiv q \cdot r$. $\mu(q \cdot r, u) = \mu(\begin{cases} \mu(q, v), & if\ u \equiv v \cdot r \\ 0, & otherwise \end{cases}$. Since $\mu(q, v) = 0$, by the induction hypothesis it follows that $\mu(q \cdot r, u) = 0$ for any u;

Case $p \equiv \Pi_n(q)$. $\mu(\Pi_n(q), u) = \begin{cases} \mu(q, v), & if\ u \equiv \Pi_n(v) \\ 0, & otherwise \end{cases}$. Since $\mu(q, v) = 0$, by the induction hypothesis $\mu(\Pi_n(q), u) = 0$ for any u;

Case $p \equiv q + r$. $\mu(q + r, u) = \begin{cases} \mu(q, v) \cdot \mu(r, w), & if\ u \equiv v + w \\ 0, & otherwise \end{cases}$. Since $\mu(q, v) = 0$ and $\mu(r, w) = 0$, by the induction hypothesis it follows that $\mu(q + r, u) = 0$ for any u.

□

Remark 3.3.19. The strategy used in the proof of Proposition 3.3.16 makes it possible to assume without loss of generality that t_X is a guarded term, actually that the considered guarded specification E is completely guarded. (Clearly, if it is not then the transformation described in the proof of Lemma 3.2.13 will be applied until t_X, which is the right-hand side of the equation of X in a guarded recursive specification, becomes a guarded term after all its variables are replaced by guarded terms.) Moreover, if the proof of one property is based on induction on the structure on guarded terms, then it is obvious that it can easily be adapted into a proof of the same claim modified for all processes in $\mathbb{SP}^\infty(\textit{pBPA} + PR)$, simply because the inductive definitions of guarded terms and $\mathbb{SP}^\infty(\textit{pBPA} + PR)$ processes are very similar in the inductive steps. (See the proof of the previous proposition and similarities of it with the proof of Proposition 3.3.15.) For that reason we do not write the proof of a claim for $\mathbb{SP}^\infty(\textit{pBPA} + PR)$ processes if we have given the proof of the same claim for guarded processes.

Proposition 3.3.20. The cPDF μ is well defined on $\mathbb{PT}^\infty(\textit{pBPA} + PR)$.

Proof. We only need to prove that for each guarded process t and $M \subseteq \mathbb{PT}^\infty(\textit{pBPA}+PR)$, $\mu(t, M) \in [0, 1]$. The proof is given by induction on the structure of guarded terms.

Case $t \equiv a \in A_\delta$. $\mu(a, M) = \sum_{x \in M} \mu(a, x) = \begin{cases} 1, & if \breve{a} \in M \\ 0, & otherwise \end{cases}$;

Case $t \equiv g \cdot s$. $\mu(g \cdot s, M) = \sum_{x \in M} \mu(g \cdot s, x) = \sum_{x:x \in M \& \exists x':x \equiv x' \cdot s} \mu(g \cdot s, x) = \sum_{x':x' \cdot s \in M} \mu(g, x') = \mu(g, \{x' \ : \ x' \cdot s \in M\}) \in [0, 1]$ by the induction hypothesis;

Case $t \equiv \Pi_n(g), n \geq 1$. $\mu(\Pi_n(g), M) = \sum_{x \in M} \mu(\Pi_n(g), x) = \sum_{x:x \in M \& \exists x':x \equiv \Pi_n(x')} \mu(\Pi_n(g), x) = \sum_{x':\Pi_n(x') \in M} \mu(g, x') = \mu(g, \{x' \ : \ \Pi_n(x') \in M\}) \in [0, 1]$ by the induction hypothesis;

Case $t \equiv g + h$. $\mu(g + h, M) = \sum_{x \in M} \mu(g + h, x) = \sum_{x:x \in M \& \exists x', x'':x \equiv x' + x''} \mu(g, x')\mu(h, x'') \leq \mu(g, \{x' \ : \ \exists x'' : x' + x'' \in M\})\mu(h, \{x'' \ : \ \exists x' : x' + x'' \in M\}) \in [0, 1]$ by the induction hypothesis;

Case $t \equiv g \leftplus_\pi h$. $\mu(g \leftplus_\pi h, M) = \sum_{x \in M} \mu(g \leftplus_\pi h, x) = \sum_{x \in M} (\pi\mu(g, x) + (1 - \pi)\mu(h, x)) = \pi \sum_{x \in M} \mu(g, x) + (1 - \pi) \sum_{x \in M} \mu(h, x) = \pi\mu(g, M) + (1 - \pi)\mu(h, M) \in [0, 1]$ by the induction hypothesis.

□

Proposition 3.3.21. (Properties of PDF - part 1) Let be $K, L \subseteq \mathbb{PT}^\infty(\textit{pBPA} + PR)$.

i. $\mu(p \leftplus_\pi q, K) = \pi\mu(p, K) + (1 - \pi)\mu(q, K)$;

ii. $\mu(p + q, K + L) = \mu(p, K) \cdot \mu(q, L)$;

iii. $\mu(p \cdot q, K \cdot L) = \mu(p, K)$ if $q \in L$, and $\mu(p \cdot q, K \cdot L) = 0$ otherwise.

iv. $\mu(\Pi_n(p), \Pi_n(K)) = \mu(p, K)$.

Proof. We give the proof only for the second case. The other cases can be proved in a similar way.

$$\begin{aligned} ii.\quad \mu(p+q, K+L) &= \sum_{x \in K+L} \mu(p+q, x) = \sum_{x \equiv k+l \in K+L} \mu(p+q, k+l) \\ &= \sum_{k \in K, l \in L} \mu(p, K) \cdot \mu(q, L) = \sum_{k \in K} \left(\mu(p, k) \cdot \sum_{l \in L} \mu(q, l) \right) \\ &= \left(\sum_{k \in K} \mu(p, k) \right) \cdot \left(\sum_{l \in L} \mu(q, l) \right) = \mu(p, K) \cdot \mu(q, L). \end{aligned}$$

□

Our intention to have the alternating model has been realized by introducing two types of transitions: probabilistic and action transitions, and two types of processes: static and dynamic processes. Although this is rather obvious from the definition of the deduction rules of $\mathbf{T}_{pBPA+PR}$ and $\mathbf{T}_{pBPA}$ the next step is to justify that these rules define an alternating model. Together, Proposition 3.3.22 and Proposition 3.3.23 given below guarantee the alternation of probabilistic and action transitions.

Proposition 3.3.22. If p is an element in $\mathbb{SP}^\infty(pBPA + PR)$ and $p \rightsquigarrow u$, then $u \in \mathbb{DP}^\infty(pBPA + PR)$.

Proof. As explained in Remark 3.3.19 it is sufficient to prove the property for guarded processes. Using the inductive definition of guarded terms we proceed by structural induction (see Remark 3.3.7 on page 51). Assume that $g \rightsquigarrow u$ for g a guarded process.

Case $g \equiv a, a \in A_\delta$. $a \rightsquigarrow \breve{a}$ is the only possible probabilistic transition and $\breve{a} \in \mathbb{DP}^\infty(pBPA + PR)$;

Case $g \equiv h \cdot r$. h is a guarded process and r is an arbitrary process. From the assumption $g \rightsquigarrow u$ it follows that $h \rightsquigarrow v$ and $u \equiv v \cdot r$. From the inductive hypothesis $v \in \mathbb{DP}^\infty(pBPA + PR)$ and since $r \in \mathbb{SP}^\infty(pBPA + PR)$ it follows that $u \in \mathbb{DP}^\infty(pBPA + PR)$ as well;

Case $g \equiv \Pi_n(h)$. h is a guarded process. The assumption $g \rightsquigarrow u$ implies that $h \rightsquigarrow v$, where $u \equiv \Pi_n(v)$. From the inductive hypothesis $v \in \mathbb{DP}^\infty(pBPA + PR)$ and $u \in \mathbb{DP}^\infty(pBPA + PR)$ as well;

Case $g \equiv h + t$. h and t are guarded processes. The assumption $g \rightsquigarrow u$ implies that $h \rightsquigarrow v$ and $t \rightsquigarrow w$ and $u \equiv v + w$. From the inductive hypothesis $v \in \mathbb{DP}^\infty(pBPA + PR)$ and $w \in \mathbb{DP}^\infty(pBPA + PR)$ from which $u \in \mathbb{DP}^\infty(pBPA + PR)$;

Case $g \equiv h \leftplus_\alpha t$. h and t are guarded processes. From the assumption $g \rightsquigarrow u$ it follows that $h \rightsquigarrow u$ or $t \rightsquigarrow u$. In both cases from the inductive hypothesis it follows that $u \in \mathbb{DP}^\infty(pBPA + PR)$.

□

Proposition 3.3.23. If x is a $\mathbb{DP}^\infty(pBPA + PR)$ process and $x \xrightarrow{a} p$ for some $a \in A$, then $p \in \mathbb{SP}^\infty(pBPA + PR)$.

Proof. This is easy to prove by induction on the structure of $\mathbb{DP}^\infty(pBPA + PR)$ processes. □

Trivial static processes that form the set $\mathbb{D}^{\infty}(\textit{pBPA}(+PR))$ possess special properties. Especially, they inherit properties that $\textit{BPA}(+PR)$ processes have; for instance they obey the idempotency law - proved on page 43 (Proposition 3.2.17) for the set of terms $\mathcal{D}(\textit{pBPA})$ which basically contains all terms representing trivial static processes in $\mathbb{D}^{\infty}(\textit{pBPA})$. In particular, their essential importance can be found already in Remark 3.2.20 on page 44 (there, expressed in a syntactic way). To recall, every finite process (closed term) can be rewritten into a normal form (basic term), which can be expressed as a probability distribution (of course by use of the probability choice operator) over a set of trivial static processes. Several propositions given below show more characteristics of the $\mathbb{D}^{\infty}(\textit{pBPA}(+PR))$ processes that will be employed later in the proof of the Completeness theorem. Moreover, Proposition 3.3.31 states that even static processes that show non-trivial probabilistic behaviour, but that can reach only a single equivalence class, basically behave as a trivial static process. This applies, for example, to processes represented by the terms $a \leftrightarrows_{1/3} a$ or $a \leftrightarrows_{1/2} (a + a) \leftrightarrows_{1/3} a$.

Proposition 3.3.24. If u is a $\mathbb{D}^{\infty}(\textit{pBPA} + PR)$ process, then the only possible probabilistic transition of u is $u \rightsquigarrow \breve{u}$.

Proof. The proof is given by induction on the structure of u.

Case $u \equiv a, a \in A_{\delta}$. In this case the conclusion follows directly from the definition of the operational rules;

Case $u \equiv v \cdot t$. Since $v \in \mathbb{D}^{\infty}(\textit{pBPA} + PR)$, by the inductive hypothesis we obtain that $v \rightsquigarrow \breve{v}$ is the only possible probabilistic transition of v. Then $u \rightsquigarrow \breve{v} \cdot t$ and this is the only possible probabilistic transition of u;

Case $u \equiv v + w$. Since $v, w \in \mathbb{D}^{\infty}(\textit{pBPA} + PR)$, from the inductive hypothesis it follows that $v \rightsquigarrow \breve{v}$ and $w \rightsquigarrow \breve{w}$ are the only possible probabilistic transitions of v and w, respectively. Then $u \rightsquigarrow \breve{v} + \breve{w}$ and this is the only possible probabilistic transition of u;

Case $u \equiv \Pi_n(v)$. Since $v \in \mathbb{D}^{\infty}(\textit{pBPA} + PR)$, the inductive hypothesis implies that $v \rightsquigarrow \breve{v}$ is the only possible probabilistic transition of v. Then $u \rightsquigarrow \Pi_n(\breve{v})$ and this is the only possible probabilistic transition of u.

□

Corollary 3.3.25.

i. If u, v are $\mathbb{D}^{\infty}(\textit{pBPA} + PR)$ processes, then $u \rightsquigarrow \breve{v}$ iff $u \equiv v$.

ii. If p is an interpretation of a basic $\textit{pBPA} + PR$ term $\mathbf{p}$ and $p \rightsquigarrow \breve{x}$ for some $x \in \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$, then x is an interpretation of a basic $\textit{pBPA} + PR$ term $\mathbf{x}$. Moreover $\mathbf{x} \in \mathcal{B}_{+}(\textit{pBPA} + \mathcal{PR})$.

□

Proposition 3.3.26. If u is a $\mathbb{D}^{\infty}(\textit{pBPA} + PR)$ process, then $\mu(u, \breve{u}) = 1$. □

Proposition 3.3.27. Let x and y be $\mathbb{D}^{\infty}(\textit{pBPA} + PR)$ processes. Then $x \leftrightarrows y \Leftrightarrow \breve{x} \leftrightarrows \breve{y}$.

Proof. This result follows from Proposition 3.3.24. □

As pointed out in the introduction of this section the probability distribution function $\mu(p, \_)$ for a given process p is introduced to avoid ambiguous situations that may occur if labelled probabilistic transitions are used instead. Thus, the link between probabilistic transitions of p and the corresponding PDF is very obvious. In the sequel we treat this link and we show that every probabilistic transition of p, say $p \rightsquigarrow u$, is indicated by the non-zero value of $\mu(p, u)$. Consequently, one may conclude that the first clause in Definition 3.3.11 (page 53) carries redundant information in the presence of the fourth clause. In fact, we provide in Proposition 3.3.32 a new definition for a probabilistic bisimulation relation which will be proved equivalent to the one given earlier.

Proposition 3.3.28. Let be $p \in \mathbb{PT}^{\infty}(\mathit{pBPA} + PR)$. Then $\mu(p, x) > 0$ iff $p \rightsquigarrow x$. □

Proof. According to Remark 3.3.19 we only need to prove that the claim holds for guarded processes. We proceed by structural induction over guarded terms (see Remark 3.3.7 on page 51).

($\Rightarrow$) Let be $\mu(g, u) > 0$.

Case $g \equiv a, a \in A_\delta$. From the assumption $\mu(a, u) > 0$ it follows that $u \equiv \breve{a}$ from which clearly $g \rightsquigarrow u$;

Case $g \equiv h \cdot t$. h is a guarded process. From the definition of the probability distribution function and from the assumption $\mu(g, u) > 0$ follows that $u \equiv v \cdot t$ and $\mu(h, v) > 0$. From the inductive hypothesis it follows that $h \rightsquigarrow v$ and $g \rightsquigarrow u$ as well;

Case $g \equiv \Pi_n(h)$. h is a guarded process. From the definition of the probability distribution function and from the assumption $\mu(g, u) > 0$ follows that $u \equiv \Pi_n(v)$ and $\mu(h, v) > 0$. From the inductive hypothesis we obtain that $h \rightsquigarrow v$ and also $g \rightsquigarrow u$ as well;

Case $g \equiv h + t$. h and t are guarded processes. From the definition of the probability distribution function and from the assumption $\mu(g, u) > 0$ it follows that $u \equiv v + w$ and $\mu(h, v) \cdot \mu(t, w) > 0$. Therefore, $\mu(h, v) > 0$ and $\mu(t, w) > 0$. Then, from the inductive hypothesis $h \rightsquigarrow v$ and $t \rightsquigarrow w$. Hence $g \rightsquigarrow u$;

Case $g \equiv h \leftplus_\pi t$. h and t are guarded processes. From the definition of the probability distribution function and from the assumption $\mu(g, u) > 0$ it follows that $\pi \cdot \mu(h, u) + (1 - \pi) \cdot \mu(t, u) > 0$. Then either $\mu(h, u) > 0$ or $\mu(t, w) > 0$. From the inductive hypothesis it follows that either $h \rightsquigarrow u$ or $t \rightsquigarrow u$. In both cases $g \rightsquigarrow u$.

($\Leftarrow$) Let be $g \rightsquigarrow u$.

Case $g \equiv a, a \in A_\delta$. $u \equiv \breve{a}$ and $\mu(g, u) = 1 > 0$;

Case $g \equiv h \cdot t$. h is a guarded process. From the assumption $g \rightsquigarrow u$ it follows that $u \equiv v \cdot t$ and $h \rightsquigarrow v$. The inductive hypothesis gives that $\mu(h, v) > 0$. Since $\mu(g, u) = \mu(h, v)$, $\mu(g, u) > 0$ as well;

Case $g \equiv \Pi_n(h)$. h is a guarded process. From the assumption $g \rightsquigarrow u$ it follows that $u \equiv \Pi_n(v)$ and $h \rightsquigarrow v$. The inductive hypothesis gives that $\mu(h, v) > 0$. Since $\mu(g, u) = \mu(h, v)$, $\mu(g, u) > 0$ as well;

Case $g \equiv h + t$. h and t are guarded processes. According to the assumption $g \rightsquigarrow u$, $u \equiv v + w$ and $h \rightsquigarrow v$ and $t \rightsquigarrow w$. From the inductive hypothesis it follows that $\mu(h, v) > 0$ and $\mu(t, w) > 0$. Therefore, $\mu(g, u) > 0$ as well;

Case $g \equiv h \leftthreetimes_{\pi} t$. h and t are guarded processes. From the assumption $g \rightsquigarrow u$ it follows that either $h \rightsquigarrow u$ or $t \rightsquigarrow u$. From the inductive hypothesis we obtain that either $\mu(h, u) > 0$ or $\mu(t, u) > 0$. In both cases $\mu(g, u) > 0$.

□

Corollary 3.3.29. Let $p \in \mathbb{PT}^{\infty}(\textit{pBPA} + PR)$ and $M \subseteq \mathbb{PT}^{\infty}(\textit{pBPA} + PR)$. Then $\mu(p, M) > 0$ iff $\exists x \in M : p \rightsquigarrow x$. □

Proposition 3.3.30. If $p \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$, then $\mu(p, \mathbb{PT}^{\infty}(\textit{pBPA} + PR)) = 1$. □

Proof. From Proposition 3.3.22 and 3.3.28 it follows that it is sufficient to prove that $\mu(g, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) = 1$. The proof is given by induction on the structure of the guarded process g (see Remark 3.3.19 and Remark 3.3.7).

Case $g \equiv a, a \in A_{\delta}$. $\mu(a, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) = \sum_{u \in \mathbb{PT}^{\infty}(\textit{pBPA}+PR)} \mu(a, u) = \mu(a, \breve{a}) = 1$;

Case $g \equiv h \cdot r$. h is a guarded process and the inductive hypothesis is valid for h. Thus,

$$\begin{aligned} \mu(g, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) &= \mu(h \cdot r, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) = \mu(h \cdot r, \mathbb{DP}^{\infty}(\textit{pBPA} + PR) \cdot r) \\ &= \mu(h, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) = 1; \end{aligned}$$

Case $g \equiv \Pi_n(h)$. h is a guarded process and the inductive hypothesis is applicable on h. Thus,

$$\begin{aligned} \mu(g, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) &= \mu(\Pi_n(h), \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) \\ &= \mu(\Pi_n(h), \Pi_n(\mathbb{DP}^{\infty}(\textit{pBPA} + PR))) \\ &= \mu(h, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) = 1; \end{aligned}$$

Case $g \equiv h + t$. h and t are guarded processes and the inductive hypothesis is applicable on them. So,

$$\begin{aligned} \mu(g, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) &= \mu(h + t, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) \\ &= \mu(h + t, \mathbb{DP}^{\infty}(\textit{pBPA} + PR) + \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) \\ &= \mu(h, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) \cdot \mu(t, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) = 1; \end{aligned}$$

Case $g \equiv h \leftthreetimes_{\alpha} t$. h and t are guarded processes and the inductive hypothesis can be applied on them. Thus,

$$\begin{aligned} \mu(g, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) &= \alpha \cdot \mu(h, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) \\ &\qquad + (1 - \alpha) \cdot \mu(t, \mathbb{DP}^{\infty}(\textit{pBPA} + PR)) \\ &= \alpha \cdot 1 + (1 - \alpha) \cdot 1 = 1. \end{aligned}$$

□

Proposition 3.3.31. If $p \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$ and $u \in \mathbb{D}^{\infty}(\textit{pBPA} + PR)$ and $\mu(p, [\breve{u}]_{\leftrightarrows}) = 1$, then $p \leftrightarrows u$.

Proof. Let as assume that $\mu(p, [\breve{u}]_{\leftrightarrows}) = 1$ and $p \not\leftrightarrows u$. Since $u \rightsquigarrow \breve{u}$ and $\mu(u, \breve{u}) = 1$, from the latter assumption it follows that there is a $v \in \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$ such that $p \rightsquigarrow v$ and $v \not\leftrightarrows u$. (Note that the case in which $p \not\rightsquigarrow$ is not possible since $p \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$.) Then, from Proposition 3.3.28 we obtain that $\mu(p, \breve{v}) > 0$ and also $\mu(p, [\breve{v}]_{\leftrightarrows}) > 0$. Thus, since $[\breve{u}]_{\leftrightarrows} \neq [\breve{v}]_{\leftrightarrows}$ from Proposition 3.3.30 it follows that $\mu(p, [\breve{u}]_{\leftrightarrows}) < 1$ which contradicts the given assumption. □

Proposition 3.3.32. We define a relation $\leftrightarrows$ in the following way. Let R be an equivalence relation on the set $\mathbb{PT}^{\infty}(\textit{pBPA} + PR)$ such that:

1. If sRt and $s \xrightarrow{a} p$ for some $a \in A$, then there is a term q such that $t \xrightarrow{a} q$ and pRq;
2. If sRt and $s \xrightarrow{a} \surd$, then $t \xrightarrow{a} \surd$;
3. If pRq, then $\mu(p, M) = \mu(q, M)$ for each $M \in \mathbb{PT}^{\infty}(\textit{pBPA} + PR)/R$.

$p \rightleftharpoons q$ if there is a relation R that satisfies the three clauses and pRq. Then $p \leftrightarrows q$ iff $p \rightleftharpoons q$.

Proof. Straightforward from Proposition 3.3.28. □

Remark 3.3.33. Thus, Proposition 3.3.32 allows us to give shorter proofs, that is, the first clause of Definition 3.3.11 does not need to be investigated if the fourth is proved to hold. So it gives us freedom to use either relation. From now on we use the notation $\leftrightarrows$ for both. Since this (important) property is only a corollary of Proposition 3.3.28, for any model (to be presented later) in which Proposition 3.3.28 holds, Proposition 3.3.32 holds as well. Therefore, in any extension of $\textit{pBPA}(+PR)$ and its model we only need to prove an adapted version of Proposition 3.3.28 extended over the added operators. Then we have Proposition 3.3.32 for free.

Remark 3.3.34. From Proposition 3.3.22 and 3.3.23 and Corollary 3.3.29 it follows easily that we can simplify proofs by taking into account:

1. $\rightsquigarrow \subseteq \mathbb{SP}^{\infty}(\textit{pBPA} + PR) \times \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$,
2. $\xrightarrow{a} \subseteq \mathbb{DP}^{\infty}(\textit{pBPA} + PR) \times \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$,
3. $\xrightarrow{a} \surd \subseteq \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$,
4. for every probabilistic bisimulation R on $\mathbb{PT}^{\infty}(\textit{pBPA} + PR)$,
   $R \subseteq \mathbb{SP}^{\infty}(\textit{pBPA} + PR) \times \mathbb{SP}^{\infty}(\textit{pBPA} + PR) \cup \mathbb{DP}^{\infty}(\textit{pBPA} + PR) \times \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$,
5. $\mu(p, M) = 0$ if $p \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$ and $M \subseteq \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$. In any other case $\mu(p, M) \geq 0$. In particular, if M is a bisimulation equivalence class then $\mu(p, M) \geq 0$ if $p \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$ and $M \subseteq \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$.

Remark 3.3.35. In the sequel a bisimulation relation will be often defined as an union of several relations. If one of these relations is a bisimulation, then there is no need to investigate transitions for pairs belonging to that relation. According to the previous remark, if non-trivial pairs of these relations make a subset of $\mathbb{SP}^{\infty}(\textit{pBPA} + PR) \times \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$, then it is sufficient to investigate only probabilistic transitions for them. On the other hand, if it is a subset of $\mathbb{DP}^{\infty}(\textit{pBPA} + PR) \times \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$, only action transitions for the pairs in the relation need to be considered. Moreover, when we explore the values of the PDF function for a process p and an equivalence class M, it is sufficient to do so for p an element in $\mathbb{SP}^{\infty}(\textit{pBPA} + PR)$ and M a subset of $\mathbb{DP}^{\infty}(\textit{pBPA} + PR)$. In short, we write $M \in \mathbb{DP}^{\infty}(\textit{pBPA} + PR)/R$ instead of $M \in \mathbb{PT}^{\infty}(\textit{pBPA} + PR)/R$ and $M \subseteq \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$.

In the sequel we prove the congruence property of the probabilistic bisimulation with respect to the operators of $\textit{pBPA} + PR$ followed by the Soundness theorem.

Theorem 3.3.36 (*Congruence of pBPA* $+ PR$). $\leftrightarrows$ is a congruence relation on $\mathbb{PT}^{\infty}(\textit{pBPA} + PR)$ with respect to the operators: $+, \cdot, \Pi_n, \ (n \geq 1)$ and $\leftthreetimes_{\pi}, \ (\pi \in \langle 0, 1\rangle)$.

Proof. Since $\underline{\leftrightarrow}$ is an equivalence relation (Proposition 3.3.13) we only need to prove that $\underline{\leftrightarrow}$ is preserved by the operators.

Sequential composition. Let x, y, z and w be $\mathbb{PT}^{\infty}(\textit{pBPA} + PR)$ processes such that $x \underline{\leftrightarrow} y$ and $z \underline{\leftrightarrow} w$. So, there exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. Take the relation R:

$$R = Eq(\alpha \cup \beta \cup R_2),$$

where

$\alpha = \{(p \cdot s, q \cdot t) \ : \ p, q, s, t \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR),\ (p, q) \in R_1,\ (s, t) \in R_2\}$ and

$\beta = \{(u \cdot s, v \cdot t) \ : \ u, v \in \mathbb{DP}^{\infty}(\textit{pBPA}+PR), s, t \in \mathbb{SP}^{\infty}(\textit{pBPA}+PR),\ (u, v) \in R_1,\ (s, t) \in R_2\}$.

Using the definitions of α and β it is easy to validate the following statements:

S1: α and β are equivalence relations; α and R_2 contain pairs of static processes relevant to R. For every static process r, $[r]_{\beta} = \{r\}$;

S2: if $(p \cdot s, q \cdot t) \in \alpha$ and $K \in \mathbb{PT}^{\infty}(\textit{pBPA} + PR)/\beta$, then $p \cdot s \rightsquigarrow K$ iff $q \cdot t \rightsquigarrow K$ (simply by applying the deduction rule for the sequential composition in Table 3.8 on page 55);

S3: if $p \cdot s \rightsquigarrow K$ for $K \in \mathbb{PT}^{\infty}(\textit{pBPA} + PR)/\beta$, then $K = [u \cdot s]_{\beta}$ for some u such that $p \rightsquigarrow u$. Moreover, from the definition of β we have that $K = [u]_{R_1} \cdot [s]_{R_2}$;

S4: since R_2 and β are subsets of R and they are equivalence relations themselves, if $M \in \mathbb{PT}^{\infty}(\textit{pBPA} + PR)/R$, then $M = \bigcup\limits_{i \in I} M_i$, $M = \bigcup\limits_{j \in J} K_j$ for some non-empty index sets I and J and for some equivalence classes $M_i, i \in I$ and $K_j, j \in J$ of R_2 and β respectively.

Now, suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}^{\infty}(\textit{pBPA}+PR)$, and $M \in \mathbb{DP}^{\infty}(\textit{pBPA}+PR)/R$. Then

1. if $(r, r_1) \in R_2$, having that $\mu(r, M_i) = \mu(r_1, M_i)$ for all $i \in I$ and using Proposition 3.3.9 we obtain:
$$\mu(r, M) = \mu(r, \bigcup_{i \in I} M_i) = \sum_{i \in I} \mu(r, M_i) = \sum_{i \in I} \mu(r_1, M_i) = \mu(r_1, \bigcup_{i \in I} M_i) = \mu(r_1, M). \quad (1)$$

2. if $(r, r_1) \in \alpha$, then $r \equiv p \cdot s, r_1 \equiv q \cdot t$, for some p, q, s, t such that $(p, q) \in R_1$ and $(s, t) \in R_2$. According to **S3** and **S4**, $M = \bigcup\limits_{j \in J} K_j$ and $K_j = [u_j]_{R_1} \cdot [s]_{R_2}$ and $p \cdot s \rightsquigarrow u_j \cdot s$ and $p \rightsquigarrow u_j$. Then from Proposition 3.3.21*iii.* we obtain:
$$\begin{aligned} \mu(p \cdot s, K_j) &= \mu(p \cdot s, [u_j]_{R_1} \cdot [s]_{R_2}) = \mu(p, [u_j]_{R_1}) = \mu(q, [u_j]_{R_1}) \\ &= \mu(q \cdot t, [u_j]_{R_1} \cdot [t]_{R_2}) = \mu(q \cdot t, K_j), \end{aligned}$$
where $[u_j \cdot t]_{\beta} = [u_j \cdot s]_{\beta} = K_j$ because $(t, s) \in R_2$ and $(u_j \cdot t, u_j \cdot s) \in \beta$. Finally, from Proposition 3.3.9 it follows that $\mu(r, M) = \mu(p \cdot s, M) = \mu(p \cdot s, \bigcup\limits_{j \in J} K_j) = \sum\limits_{j \in J} \mu(p \cdot s, K_j) = \sum\limits_{j \in J} \mu(q \cdot t, K_j) = \mu(q \cdot t, \bigcup\limits_{j \in J} K_j) = \mu(q \cdot t, M) = \mu(r_1, M)$. (2)

Alternative composition. Let x, y, z and w be $\mathbb{PT}^{\infty}(\textit{pBPA} + PR)$ processes such that $x \underline{\leftrightarrow} y$ and $z \underline{\leftrightarrow} w$. There exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. Take the relation R:

$$R = Eq(\alpha \cup \beta \cup R_1 \cup R_2),$$

where
$\alpha = \{(p+s, q+t) \ : \ p,q,s,t \in \mathbb{SP}^{\infty}(\textbf{\textit{pBPA}} + PR),\ (p,q) \in R_1,\ (s,t) \in R_2\}$ and
$\beta = \{(u+l, v+m) \ : \ u,v,l,m \in \mathbb{DP}^{\infty}(\textbf{\textit{pBPA}} + PR),\ (u,v) \in R_1,\ (l,m) \in R_2\}$.
Easily we can conclude that:

N1: α and β are equivalence relations; α, R_1 and R_2 contain pairs of static processes relevant to R. Moreover, β equivalence classes of static processes are singletons.

N2: if $(p+s, q+t) \in \alpha$ and $K \in \mathbb{PT}^{\infty}(\textbf{\textit{pBPA}} + PR)/\beta$, then $p+s \rightsquigarrow K$ iff $q+t \rightsquigarrow K$;

N3: if $p+s \rightsquigarrow K$ for $K \in \mathbb{PT}^{\infty}(\textbf{\textit{pBPA}} + PR)/\beta$, then $K = [u+l]_{\beta}$ for some u and l such that $p \rightsquigarrow u$ and $s \rightsquigarrow l$. Moreover, from the definition of β we have that $K = [u]_{R_1} + [l]_{R_2}$;

N4: since R_1, R_2 and β are all subsets of R and they are equivalence relations themselves, if $M \in \mathbb{PT}^{\infty}(\textbf{\textit{pBPA}} + PR)/R$, then $M = \bigcup_{i_1 \in I_1} M^1_{i_1}$, $M = \bigcup_{i_2 \in I_2} M^2_{i_2}$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I_1, I_2 and J and for some equivalence classes $M^1_{i_1}, (i_1 \in I_1)$, $M^2_{i_2}, (i_2 \in I_2)$ and $K_j, (j \in J)$ of R_1, R_2 and β, respectively.

Now, suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}^{\infty}(\textbf{\textit{pBPA}}+PR)$ and $M \in \mathbb{DP}^{\infty}(\textbf{\textit{pBPA}}+PR)/R$. We discuss the following possibilities:

1. if $(r, r_1) \in R_k, k = 1, 2$, then the fact that $\mu(r, M^k_{i_k}) = \mu(r_1, M^k_{i_k})$ for all $i_k \in I_k$ $(k = 1, 2)$ yields $\mu(r, M) = \mu(r_1, M)$ in a similar way as in (1) (in the case of sequential composition);

2. if $(r, r_1) \in \alpha$, then $r \equiv p+s$ and $r_1 \equiv q+t$ for some $p, q, s, t \in \mathbb{SP}^{\infty}(\textbf{\textit{pBPA}} + PR)$ such that $(p, q) \in R_1$ and $(s, t) \in R_2$. According to **N3** and **N4**, $M = \bigcup_{j \in J} K_j$ and $K_j = [u_j + l_j]_{\beta} = [u_j]_{R_1} + [l_j]_{R_2}$ and $p \rightsquigarrow u_j$ and $s \rightsquigarrow l_j$. Then from Proposition 3.3.21*ii.* we obtain:
$$\begin{aligned} \mu(p+s, K_j) &= \mu(p+s, [u_j]_{R_1} + [l_j]_{R_2}) = \mu(p, [u_j]_{R_1}) \cdot \mu(s, [l_j]_{R_2}) \\ &= \mu(q, [u_j]_{R_1}) \cdot \mu(t, [l_j]_{R_2}) = \mu(q+t, K_j). \end{aligned}$$
Proposition 3.3.9 yields the conclusion $\mu(p+s, M) = \mu(q+t, M)$ in a similar way as in (2) (in the case of sequential composition).

Probabilistic choice. Let x, y, z and w be $\mathbb{PT}^{\infty}(\textbf{\textit{pBPA}}+PR)$ processes such that $x \leftrightarrow y$ and $z \leftrightarrow w$. So, there exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. Take the relation R:
$$R = Eq(\alpha \cup R_1 \cup R_2),$$
where
$\alpha = \{(p \leftplus_{\pi} s, q \leftplus_{\pi} t) \ : \ p,q,s,t \in \mathbb{PT}^{\infty}(\textbf{\textit{pBPA}} + PR), (p,q) \in R_1, (s,t) \in R_2\}$.
From the definition of α and R the following conclusions can easily be made:

PC1: α is an equivalence relation. α equivalence classes of dynamic processes are singletons;

PC2: since R_1 and R_2 are subsets of R and they are equivalence relations themselves, if $M \in \mathbb{PT}^{\infty}(\textbf{\textit{pBPA}} + PR)/R$, then $M = \bigcup_{i \in I} N_i$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I and J, and for some equivalence classes $N_i, (i \in I)$, $K_j, (j \in J)$ of R_1 and R_2, respectively.

Now, suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}^{\infty}(\textbf{\textit{pBPA}}+PR)$ and $M \in \mathbb{DP}^{\infty}(\textbf{\textit{pBPA}}+PR)/R$. We need to consider the following cases:

1. if $(r, r_1) \in R_k, k = 1, 2$, then the result follows from Proposition 3.3.9 (see previous cases).

2. if $(r, r_1) \in \alpha$, then $r \equiv p \leftrightarrows_\pi s$ and $r_1 \equiv q \leftrightarrows_\pi t$ for some $p, q, s, t \in \mathbb{SP}^\infty(\textit{pBPA} + PR)$ such that $(p, q) \in R_1$ and $(s, t) \in R_2$. According to **PC2**, Proposition 3.3.9 yields the equalities:
   $\mu(p, M) = \sum\limits_{i \in I} \mu(p, N_i) = \sum\limits_{i \in I} \mu(q, N_i) = \mu(q, M)$ and
   $\mu(s, M) = \sum\limits_{j \in J} \mu(s, K_j) = \sum\limits_{j \in J} \mu(t, K_j) = \mu(t, M)$.
   Using Proposition 3.3.21*i.* we obtain
   $\mu(r, M) = \pi\mu(p, M) + (1 - \pi)\mu(s, M) = \pi\mu(q, M) + (1 - \pi)\mu(t, M) = \mu(r_1, M)$.

Projection. Let x and y be $\mathbb{PT}^\infty(\textit{pBPA} + PR)$ processes such that $x \leftrightarrows y$. So, there exist a bisimulation relation R such that $(x, y) \in R$. We need to construct a relation $R_n, n \geq 1$ such that $(\Pi_n(x), \Pi_n(y)) \in R_n$ which is a bisimulation. We consider the relation

$$R_n = Eq\big(\alpha \cup \beta\big),$$

where
$\alpha = \{(\Pi_n(p), \Pi_n(q)) \ : \ p, q \in \mathbb{SP}^\infty(\textit{pBPA} + PR) \ \& \ (p, q) \in R\}$ and
$\beta = \{(\Pi_n(u), \Pi_n(v)) \ : \ u, v \in \mathbb{DP}^\infty(\textit{pBPA} + PR) \ \& \ (u, v) \in R\}$.
Let us note that:

P1: α and β are equivalence relations; only α contains the relevant pairs of static processes for R_n;

P2: if $(\Pi_n(p), \Pi_n(q)) \in \alpha$ and $K \in \mathbb{PT}^\infty(\textit{pBPA} + PR)/\beta$, then $\Pi_n(p) \rightsquigarrow K$ iff $\Pi_n(q) \rightsquigarrow K$;

P3: if $\Pi_n(p) \rightsquigarrow K$ for $K \in \mathbb{PT}^\infty(\textit{pBPA} + PR)/\beta$, then $K = [\Pi_n(u)]_\beta$ for some u such that $p \rightsquigarrow u$. Moreover, from the definition of β follows that $K = \Pi_n([u]_R)$.

Let us assume that $(\Pi_n(p), \Pi_n(q)) \in \alpha$ for $p, q \in \mathbb{SP}^\infty(\textit{pBPA} + PR)$ and $M \in \mathbb{DP}^\infty(\textit{pBPA} + PR)/\beta$. From the definition of α it follows that $(p, q) \in R$. Using Proposition 3.3.21*iv.* according to **P3** we obtain:

$$\begin{aligned} \mu(\Pi_n(p), M) &= \mu(\Pi_n(p), [\Pi_n(u)]_\beta) = \mu(\Pi_n(p), \Pi_n([u]_R)) = \mu(p, [u]_R) \\ &= \mu(q, [u]_R) = \mu(\Pi_n(q), \Pi_n([u]_R)) = \mu(\Pi_n(q), [\Pi_n(u)]_\beta) = \mu(\Pi_n(q), M). \end{aligned}$$

□

In the proof of the Soundness theorem for every axiom of $\textit{pBPA} + PR$ we should compose a probabilistic bisimulation on $\mathbb{PT}^\infty(\textit{pBPA}+PR)$ that relates processes represented by the left-hand side and the right-hand side of the axiom. This means that for every constructed relation we have to look at probabilistic and action transitions of related processes, as well as action terminations and the values of PDFs. In any case, we will not go into many details. In particular, for the axioms of $\textit{pBPA} + PR$ which occur as axioms of $\textit{BPA} + PR$ we do not write down the part(s) of the proof concerning action transitions and action termination. We claim that these cases very much resemble the proof of the Soundness theorem of $\textit{BPA} + PR$ and we direct the reader to look at [27] for instance. Furthermore, we will use the alternative definition of the probabilistic bisimulation given on page 63 (as a part of Proposition 3.3.32). Therefore, we can omit the part(s) of the proof regarding probabilistic transitions: it is sufficient to justify the validity only of the fourth clause of Definition 3.3.11 in order to confirm that the considered equivalence relation (associated to an axiom) is a probabilistic bisimulation.

Theorem 3.3.37 (*Soundness of* $\textit{pBPA} + PR$). Let $\mathbf{x}$ and $\mathbf{y}$ be $\textit{pBPA} + PR$ terms. If $\textit{pBPA} + PR \vdash \mathbf{x} = \mathbf{y}$ then $x \leftrightarrows y$.

Proof.

Axiom A1. Relation R is defined in the following way:

$$R = Eq\Big(\{(p+q, q+p) : p, q \in \mathbb{SP}^\infty(\textit{pBPA} + PR)\} \cup \{(u+v, v+u) : u, v \in \mathbb{DP}^\infty(\textit{pBPA} + PR)\}\Big).$$

Suppose that $(p+q, q+p) \in R$ for some $p, q \in \mathbb{SP}^\infty(\textit{pBPA} + PR)$ and $M \in \mathbb{DP}^\infty(\textit{pBPA} + PR)/R$. Then

$$\mu(p+q, u+v) = \mu(p,u) \cdot \mu(q,v) = \mu(q,v)\mu(p,u) = \mu(q+p, v+u).$$

Moreover $u+v \in M$ iff $v+u \in M$. From Proposition 3.3.10 it follows that $\mu(p+q, M) = \mu(q+p, M)$.

Axiom A2. Relation R is defined in the following way:

$$R = Eq\Big(\{((p+q)+s, p+(q+s)) : p, q, s \in \mathbb{SP}^\infty(\textit{pBPA} + PR)\} \cup \{((u+v)+w, u+(v+w)) : u, v, w \in \mathbb{DP}^\infty(\textit{pBPA} + PR)\}\Big).$$

Suppose that $\big((p+q)+s, p+(q+s)\big) \in R$ for some $p, q, s \in \mathbb{SP}^\infty(\textit{pBPA} + PR)$ and $M \in \mathbb{DP}^\infty(\textit{pBPA} + PR)/R$. The following equalities hold:

$$\mu((p+q)+s, (u+v)+w) = \mu(p+q, u+v) \cdot \mu(s,w) = \mu(p,u) \cdot \mu(q,v) \cdot \mu(s,w)$$

and

$$\mu(p+(q+s), u+(v+w)) = \mu(p,u) \cdot \mu(q+s, v+w) = \mu(p,u) \cdot \mu(q,v) \cdot \mu(s,w).$$

Moreover, $(u+v)+w \in M$ iff $u+(v+w) \in M$. From Proposition 3.3.10 it follows that $\mu((p+q)+s, M) = \mu(p+(q+s), M)$.

Axiom AA3. Relation R is defined in the following way:

$$R = Eq\Big(\{(a+a, a), (\breve{a}+\breve{a}, \breve{a})\}\Big).$$

It is sufficient to note that $\mu(a+a, [\breve{a}]_R) = 1 = \mu(a, [\breve{a}]_R)$ and $\mu(a+a, M) = 0 = \mu(a, M)$ for any other R-equivalence class M different from $[\breve{a}]_R$.

Axiom A4. Relation R is defined in the following way:

$$R = Eq\Big(\{((p+q)\cdot s, p\cdot s + q\cdot s) : p, q, s \in \mathbb{SP}^\infty(\textit{pBPA} + PR)\} \cup \{((u+v)\cdot s, u\cdot s + v\cdot s) : u, v \in \mathbb{DP}^\infty(\textit{pBPA} + PR), s \in \mathbb{SP}^\infty(\textit{pBPA} + PR)\}\Big).$$

Suppose that $\big((p+q)\cdot s, p\cdot s + q\cdot s\big) \in R$ for some $p, q, s \in \mathbb{SP}^\infty(\textit{pBPA} + PR)$ and $M \in \mathbb{DP}^\infty(\textit{pBPA} + PR)/R$. Then

$$\mu((p+q)\cdot s, (u+v)\cdot s) = \mu(p+q, u+v) = \mu(p,u) \cdot \mu(q,v)$$

and

$$\mu(p\cdot s+q\cdot s,u\cdot s+v\cdot s)=\mu(p\cdot s,u\cdot s)\cdot\mu(q\cdot s,v\cdot s)=\mu(p,u)\mu(q,v).$$

Moreover, $(u+v)\cdot s\in M$ iff $u\cdot s+v\cdot s\in M$. From Proposition 3.3.10 it follows that $\mu((p+q)\cdot s,M)=\mu(p\cdot s+q\cdot s,M)$.

Axiom A5. Relation R is defined in the following way:

$$\begin{array}{rcll} R & = & Eq\Big(& \{((p\cdot q)\cdot s,p\cdot(q\cdot s)): \quad p,q,s\in\mathbb{SP}^\infty(\textit{pBPA}+PR)\}\\ & & & \cup\{((u\cdot q)\cdot s,u\cdot(q\cdot s)): \quad u\in\mathbb{DP}^\infty(\textit{pBPA}+PR),\\ & & & \qquad\qquad\qquad\qquad\quad q,s\in\mathbb{SP}^\infty(\textit{pBPA}+PR)\}\Big). \end{array}$$

If $\big((p\cdot q)\cdot s,p\cdot(q\cdot s)\big)\in R$ for $p,q,s\in\mathbb{SP}^\infty(\textit{pBPA}+PR)$ and $M\in\mathbb{DP}^\infty(\textit{pBPA}+PR)/R$, then

$$\mu((p\cdot q)\cdot s,(u\cdot q)\cdot s)=\mu(p\cdot q,u\cdot q)=\mu(p,u)$$

and

$$\mu(p\cdot(q\cdot s),u\cdot(q\cdot s))=\mu(p,u).$$

Since, $(u\cdot q)\cdot s\in M$ iff $u\cdot(q\cdot s)\in M$, $\mu((p\cdot q)\cdot s,M)=\mu(p\cdot(q\cdot s),M)$ by Proposition 3.3.10.

Axiom A6. Relation R is defined in the following way:

$$R=Eq\Big(\{(p+\delta,p)\ :\ p\in\mathbb{SP}^\infty(\textit{pBPA}+PR)\}\ \cup\ \{(u+\breve{\delta},u)\ :\ u\in\mathbb{DP}^\infty(\textit{pBPA}+PR)\}\Big).$$

Notice that $\mu(p+\delta,u+\breve{\delta})=\mu(p,u)\cdot\mu(\delta,\breve{\delta})=\mu(p,u)$ and ($u+\breve{\delta}\in M$ iff $u\in M$). According to Proposition 3.3.10 we obtain that $\mu(p+\delta,M)=\mu(p,M)$ for each $M\in\mathbb{DP}^\infty(\textit{pBPA}+PR)/R$.

Axiom A7. Relation R is defined in the following way:

$$R=Eq\Big(\{(\delta\cdot p,\delta)\ :\ p\in\mathbb{SP}^\infty(\textit{pBPA}+PR)\}\ \cup\ \{(\breve{\delta}\cdot p,\breve{\delta})\ :\ p\in\mathbb{SP}^\infty(\textit{pBPA}+PR)\}\Big).$$

For any $p\in\mathbb{SP}^\infty(\textit{pBPA}+PR)$, $\mu(\delta\cdot p,[\breve{\delta}]_R)=\mu(\delta,[\breve{\delta}]_R)=1$. Moreover, for any other $M\in\mathbb{DP}^\infty(\textit{pBPA}+PR)/R$, $\mu(\delta\cdot p,M)=\mu(\delta,M)=0$.

Axiom PrAC1. Relation R is defined in the following way:

$$R=Eq\Big(\{(p\leftthreetimes_\pi q,q\leftthreetimes_{1-\pi}p)\ :\ p,q\in\mathbb{SP}^\infty(\textit{pBPA}+PR)\}\Big).$$

Observe that all R equivalence classes of dynamic processes are singletons. Therefore, the investigation of the action transitions and action termination for pairs of dynamic processes is trivial (see also Remark 3.3.35 on page 63).

Suppose that $(p\leftthreetimes_\pi q,q\leftthreetimes_{1-\pi}p)\in R$ for some $p,q\in\mathbb{SP}^\infty(\textit{pBPA}+PR)$ and $M\in\mathbb{DP}^\infty(\textit{pBPA}+PR)/R$. From Proposition 3.3.21*ii.* it follows that:

$$\begin{array}{rcl}\mu(p\leftthreetimes_\pi q,M) & = & \pi\cdot\mu(p,M)+(1-\pi)\cdot\mu(q,M)\\ & = & (1-\pi)\cdot\mu(q,M)+(1-(1-\pi))\cdot\mu(p,M)=\mu(q\leftthreetimes_{1-\pi}p,M).\end{array}$$

Axiom PrAC2. Relation R is defined in the following way:

$$R = Eq\Big(\{(p \leftthreetimes_{\pi} (q \leftthreetimes_{\rho} s), (p \leftthreetimes_{\frac{\pi}{\pi+\rho-\pi\rho}} q) \leftthreetimes_{\pi+\rho-\pi\rho} s) \ : \ p, q, s \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)\}\Big).$$

Let us denote $\alpha = \pi + \rho - \pi \cdot \rho$ in short. Suppose that $\big(p \leftthreetimes_{\pi} (q \leftthreetimes_{\rho} s), (p \leftthreetimes_{\frac{\pi}{\alpha}} q) \leftthreetimes_{\alpha} s\big) \in R$ and $M \in \mathbb{DP}^{\infty}(\textit{pBPA} + PR)/R$. From Proposition 3.3.21*ii.* the following equalities hold:

$$\begin{array}{rcl} \mu(p \leftthreetimes_{\pi} (q \leftthreetimes_{\rho} s), M) & = & \pi \cdot \mu(p, M) + (1-\pi) \cdot \mu(q \leftthreetimes_{\rho} s, M) \\ & = & \pi \cdot \mu(p, M) + (1-\pi) \cdot (\rho \cdot \mu(q, M) + (1-\rho) \cdot \mu(s, M)) \\ & = & \pi \cdot \mu(p, M) + (1-\pi) \cdot \rho \cdot \mu(q, M) + (1-\pi) \cdot (1-\rho) \cdot \mu(s, M) \end{array}$$

and

$$\begin{array}{rcl} \mu\left(\left(p \leftthreetimes_{\frac{\pi}{\alpha}} q\right) \leftthreetimes_{\alpha} s, M\right) & = & \alpha \cdot \mu\left(p \leftthreetimes_{\frac{\pi}{\alpha}} q, M\right) + (1-\alpha) \cdot \mu(s, M) \\ & = & \pi \cdot \mu(p, M) + (1-\pi) \cdot \rho \cdot \mu(q, M) + (1-\pi) \cdot (1-\rho) \cdot \mu(s, M). \end{array}$$

Thus, we have that $\mu(p \leftthreetimes_{\pi} (q \leftthreetimes_{\rho} s), M) = \mu\left(\left(p \leftthreetimes_{\frac{\pi}{\pi+\rho-\pi\rho}} q\right) \leftthreetimes_{\pi+\rho-\pi\rho} s, M\right)$.

For action transitions and action termination see the remark in the case of axiom $PrAC1$.

Axiom PrAC3. Relation R is defined in the following way:

$$R = Eq\Big(\{(p \leftthreetimes_{\pi} p, p) \ : \ p \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)\}\Big).$$

Using Proposition 3.3.21*ii.* we derive that

$$\mu(p \leftthreetimes_{\pi} p, M) = \pi \cdot \mu(p, M) + (1-\pi) \cdot \mu(p, M) = \mu(p, M)$$

holds for every $M \in \mathbb{DP}^{\infty}(\textit{pBPA} + PR)/R$.

For action transitions and action termination see the remark in the case of axiom $PrAC1$.

Axiom PrAC4. Relation R is defined in the following way:

$$R = Eq\Big(\{((p \leftthreetimes_{\pi} q) \cdot s, p \cdot s \leftthreetimes_{\pi} q \cdot s) \ : \ p, q, s \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)\}\Big).$$

Suppose that $\big((p \leftthreetimes_{\pi} q) \cdot s, p \cdot s \leftthreetimes_{\pi} q \cdot s\big) \in R$ and $M \in \mathbb{DP}^{\infty}(\textit{pBPA} + PR)/R$. Then:

$$\mu((p \leftthreetimes_{\pi} q) \cdot s, u \cdot s) = \mu(p \leftthreetimes_{\pi} q, u) = \pi \cdot \mu(p, u) + (1-\pi) \cdot \mu(q, u)$$

and

$$\mu(p \cdot s \leftthreetimes_{\pi} q \cdot s, u \cdot s) = \pi \cdot \mu(p \cdot s, u \cdot s) + (1-\pi) \cdot \mu(q \cdot s, u \cdot s) = \pi \cdot \mu(p, u) + (1-\pi) \cdot \mu(q, u).$$

From Proposition 3.3.10 it follows that $\mu((p \leftthreetimes_{\pi} q) \cdot s, M) = \mu(p \cdot s \leftthreetimes_{\pi} q \cdot s, M)$.

For action transitions and action termination see the remark in the case of axiom $PrAC1$.

Axiom PrAC5. Relation R is defined in the following way:

$$R = Eq\Big(\{((p \leftthreetimes_\pi q) + s, p + s \leftthreetimes_\pi q + s) \ : \ p, q, s \in \mathbb{SP}^\infty(\textbf{\textit{pBPA}} + PR)\}\Big).$$

Suppose that $\big((p \leftthreetimes_\pi q) + s, p + s \leftthreetimes_\pi q + s\big) \in R$ and $M \in \mathbb{DP}^\infty(\textbf{\textit{pBPA}} + PR)/R$. Then from the definition of the PDF the following equalities are derived:

$$\mu\big((p \leftthreetimes_\pi q) + s, u + w\big) = \mu(p \leftthreetimes_\pi q, u) \cdot \mu(s, w) = \big(\pi \cdot \mu(p, u) + (1 - \pi) \cdot \mu(q, u)\big) \cdot \mu(s, w)$$

and

$$\begin{array}{rcl} \mu(p + s \leftthreetimes_\pi q + s, u + w) & = & \pi \cdot \mu(p + s, u + w) + (1 - \pi) \cdot \mu(q + s, u + w) \\ & = & \pi \cdot \mu(p, u) \cdot \mu(s, w) + (1 - \pi) \cdot \mu(q, u) \cdot \mu(s, w). \end{array}$$

Finally from Proposition 3.3.10 it follows that $\mu((p \leftthreetimes_\pi q) + s, M) = \mu(p + s \leftthreetimes_\pi q + s, M)$.

For action transitions and action termination see the remark in the case of axiom $PrAC1$.

Axiom PR1. Relation R_n $(n \geq 1)$ is defined in the following way:

$$R_n = Eq\Big(\{(\Pi_n(a), a), (\Pi_n(\breve{a}), \breve{a})\}\Big).$$

From the definition of the PDF we have: $\mu(a, \breve{a}) = 1$ and $\mu(\Pi_n(a), \Pi_n(\breve{a})) = 1$ and also $\mu(a, [\breve{a}]_{R_n}) = \mu(\Pi_1(a), [\Pi_1(\breve{a})]_{R_n}) = 1$. Moreover, for every other R_n equivalence class M different from $[\breve{a}]_{R_n}$ we have $\mu(a, M) = \mu(\Pi_1(a), M) = 0$.

Axiom PR2. Relation R is defined in the following way:

$$R = Eq\Big(\{(\Pi_1(a \cdot p), a), (\Pi_1(\breve{a} \cdot p), \breve{a}) \ : \ p \in \mathbb{SP}^\infty(\textbf{\textit{pBPA}} + PR)\}\Big).$$

From the definition of the PDF we have: $\mu(a, \breve{a}) = 1$ and $\mu(\Pi_1(a \cdot p), \Pi_1(\breve{a} \cdot p)) = 1$ and also $\mu(a, [\breve{a}]_R) = \mu(\Pi_1(a \cdot p), [\Pi_1(\breve{a} \cdot p)]_R) = 1$. For any other R equivalence class M different from $[\breve{a}]_R$ we have $\mu(a, M) = \mu(\Pi_1(a \cdot p), M) = 0$.

Axiom PR3. Relation R_n $(n \geq 1)$ is defined in the following way:

$$\begin{array}{rcl} R_n & = & Eq\Big(\{(\Pi_{n+1}(a \cdot p), a \cdot \Pi_n(p)) \ : \ p \in \mathbb{SP}^\infty(\textbf{\textit{pBPA}} + PR)\} \\ & & \cup\{(\Pi_{n+1}(\breve{a} \cdot p), \breve{a} \cdot \Pi_n(p)) \ : \ p \in \mathbb{SP}^\infty(\textbf{\textit{pBPA}} + PR)\}\Big). \end{array}$$

From the definition of the PDF we have: $\mu(\Pi_{n+1}(a \cdot p), \Pi_{n+1}(\breve{a} \cdot p)) = 1$ and $\mu(a \cdot \Pi_n(p), \breve{a} \cdot \Pi_n(p)) = 1$ and also $\mu(\Pi_{n+1}(a \cdot p), [\Pi_{n+1}(\breve{a} \cdot p)]_{R_n}) = \mu(a \cdot \Pi_n(p), [\breve{a} \cdot \Pi_n(p)]_{R_n}) = 1$. For any other R_n equivalence class M different from $[\Pi_{n+1}(\breve{a} \cdot p)]_{R_n}$ we have $\mu(a \cdot \Pi_n(p), M) = \mu(\Pi_{n+1}(a \cdot p), M) = 0$.

Axiom PR4. Relation R_n $(n \geq 1)$ is defined in the following way:

$$\begin{array}{rcl} R_n & = & Eq\Big(\{(\Pi_n(p + q), \Pi_n(p) + \Pi_n(q)) \ : \ p, q \in \mathbb{SP}^\infty(\textbf{\textit{pBPA}} + PR)\} \\ & & \cup\{(\Pi_n(u + v), \Pi_n(u) + \Pi_n(v)) \ : \ u, v \in \mathbb{DP}^\infty(\textbf{\textit{pBPA}} + PR)\}\Big). \end{array}$$

Suppose that $(\Pi_n(p), \Pi_n(q)) \in R_n$ and $M \in \mathbb{DP}^\infty(\textit{pBPA} + PR)/R_n$. Then,

$$\mu(\Pi_n(p+q), \Pi_n(u+v)) = \mu(p+q, u+v) = \mu(p,u) \cdot \mu(q,v)$$

and

$$\mu(\Pi_n(p) + \Pi_n(q), \Pi_n(u) + \Pi_n(v)) = \mu(\Pi_n(p), \Pi_n(u))\mu(\Pi_n(q), \Pi_n(v)) = \mu(p,u) \cdot \mu(q,v).$$

Using the fact that $\Pi_n(u+v) \in M$ iff $\Pi_n(u) + \Pi_n(v) \in M$, the result follows from Proposition 3.3.10.

Axiom prPR. Relation R_n $(n \geq 1)$ is defined in the following way:

$$R_n = Eq\Big(\{(\Pi_n(p \leftthreetimes_\rho q), \Pi_n(p) \leftthreetimes_\rho \Pi_n(q)) \ : \ p, q \in \mathbb{SP}^\infty(\textit{pBPA} + PR)\}\Big).$$

Suppose that $\big(\Pi_n(p \leftthreetimes_\rho q), \Pi_n(p) \leftthreetimes_\rho \Pi_n(q)\big) \in R_n$ and $M \in \mathbb{DP}^\infty(\textit{pBPA} + PR)/R_n$. From the definition of the PDF it follows that:

$$\mu(\Pi_n(p \leftthreetimes_\rho q), \Pi_n(u)) = \mu(p \leftthreetimes_\rho q, u) = \rho\mu(p,u) + (1-\rho)\mu(q,u)$$

and

$$\begin{array}{rcl} \mu(\Pi_n(p) \leftthreetimes_\rho \Pi_n(q), \Pi_n(u)) & = & \rho\mu(\Pi_n(p), \Pi_n(u)) + (1-\rho)\mu(\Pi_n(q), \Pi_n(u)) \\ & = & \rho\mu(p,u) + (1-\rho)\mu(q,u). \end{array}$$

The result follows from Proposition 3.3.10.

For action transitions and action termination see the remark in the case of axiom $PrAC1$.

□

Proving RSP in the model of *pBPA* + PR Now since we have a model with infinite processes of *pBPA* + PR we define a head normal form for processes in $\mathbb{PT}^\infty(\textit{pBPA} + PR)$ and we can look into the recursive principles. The main goal is to prove that RSP holds in $\mathcal{M}^\infty_{\textit{pBPA}+PR}$. To do so, we will see that it is sufficient to prove that AIP$^-$ holds. The first two propositions can easily be proved and they show that each process in our model has finitely branching. Then, we give the notion of head normal form (HNF) and using the Soundness theorem we prove that each process in $\mathbb{PT}^\infty(\textit{pBPA} + PR)$ has a head normal form. Knowing the form of infinite processes makes easier to work with them.

That processes of $\mathbb{PT}^\infty(\textit{pBPA} + PR)$ are boundedly branching is guaranteed by the following results:

Proposition 3.3.38. If $p \in \mathbb{PT}^\infty(\textit{pBPA} + PR)$, then the set $\{u \ : \ p \rightsquigarrow u\}$ is finite. □

Proposition 3.3.39. If $u \in \mathbb{DP}^\infty(\textit{pBPA} + PR)$ then the set $\{p \ : \ u \xrightarrow{a} p, a \in A\}$ is finite. □

Definition 3.3.40. We say a process p has a *head normal form* if there is an $n \in \mathbb{N}$, processes p_i and probabilities ρ_i, $1 \leq i \leq n$ such that

$$p \leftrightarrows p_1 \leftthreetimes_{\rho_1} p_2 \ldots p_{n-1} \leftthreetimes_{\rho_{n-1}} p_n$$

and for each i,

$$p_i \leftrightarrows \sum_{j<s_i} a_{ij} \cdot p_{ij} + \sum_{k<t_i} b_{ik}$$

for certain $s_i, t_i \in \mathbb{N}$ with $s_i + t_i > 0$, $a_{ij}, b_{ik} \in \boldsymbol{A}_\delta$ and processes p_{ij}.

A process p is *definable* if p can be obtained from the atomic actions in A and δ by means of the operators of *pBPA* + PR and guarded recursion.

A process p is *finite* if it is the interpretation of a closed term in *pBPA* + PR.

Lemma 3.3.41. Each process in $\mathbb{PT}^{\infty}(\textit{pBPA} + PR)$ has a head normal form.

Proof. The proof is quite similar to the proof of Lemma 2.4.7 in [27] which says that each definable process in the bisimulation model of *BPA* has HNF. The only differences in our proof are: for probabilistic choice for which the conclusion follows directly from the definition of HNF, for nondeterministic choice where the distribution law $PrAC5$ should be applied and for sequential composition where the axiom $PrAC4$ should be applied and the result follows straightforwardly. □

It is easy to see that each $\mathbb{D}^{\infty}(\textit{pBPA} + PR)$ process p has a head normal form as follows:

$$p \leftrightarrows \sum_{j<s_i} a_{ij} \cdot p_{ij} + \sum_{k<t_i} b_{ik}$$

for certain $s_i, t_i \in \mathbb{N}$ with $s_i + t_i > 0$, $a_{ij}, b_{ij} \in A_{\delta}$ and processes p_{ij}. And each dynamic process $u \in \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$ has the form:

$$u \leftrightarrows \sum_{j<s_i} \breve{a}_{ij} \cdot p_{ij} + \sum_{k<t_i} \breve{b}_{ik}$$

for certain $s_i, t_i \in \mathbb{N}$ with $s_i + t_i > 0$, $a_{ij}, b_{ij} \in A_{\delta}$ and processes p_{ij}.
We will refer to this special HNF as dynamic HNF, for both.

From the construction of the model and its domain described on page 47 and Definition 3.3.2 the following result is straightforward.

Lemma 3.3.42. RDP^{-} holds in $\mathbb{PT}^{\infty}(\textit{pBPA} + PR)$. □

Using Lemma 3.3.41 it is easy to prove the following results. They are essential to prove the Projection theorem. The proofs of all following properties are easy to derive using the normal form of processes. We direct the reader to [27] for the complete proof of Lemma 3.3.47 obtained as a corollary of the Projection theorem.

Proposition 3.3.43. Let $p \in \mathbb{SP}^{\infty}(\textit{pBPA} + PR)$. All finite projections of p are bisimilar with finite processes in $\mathbb{SP}^{\infty}(\textit{pBPA} + PR)$. □

Proposition 3.3.44. Let $u \in \mathbb{D}^{\infty}(\textit{pBPA} + PR)$. All finite projections of u are bisimilar with finite processes in $\mathbb{D}^{\infty}(\textit{pBPA} + PR)$. □

Proposition 3.3.45. Let p and q be processes such that for some $n \in \mathbb{N}$, $n \geq 1$, $\Pi_n(p) \leftrightarrows \Pi_n(q)$. Then for each $k \leq n$, $\Pi_k(p) \leftrightarrows \Pi_k(q)$. □

Theorem 3.3.46 (*Projection theorem*). Let E be a guarded recursive specification with solutions p and q. Then for all $n \geq 1$, $\Pi_n(p) \leftrightarrows \Pi_n(q)$.

Lemma 3.3.47. ([27] Theorem 2.4.19) AIP^{-} implies RSP. □

We have come to the main theorem in this section; it states that the recursive principle AIP^{-} is valid in $\mathcal{M}_{\textit{pBPA}+PR}$. According to Lemma 3.3.47, consequently, we conclude that every guarded recursive specification in *pBPA* + PR has at most one solution in $\mathcal{M}_{\textit{pBPA}+PR}$.

Theorem 3.3.48 (AIP$^-$ *in* $\mathbb{PT}^\infty(pBPA + PR)$). If for all $n \geq 1$, $\Pi_n(p) \leftrightarrows \Pi_n(q)$, then $p \leftrightarrows q$[8].

Proof. Let us consider the following relation on $\mathbb{PT}^\infty(pBPA + PR)$:

$$R = Eq\Big(\{(p,q) \,:\, p,q \in \mathbb{SP}^\infty(pBPA + PR) \,\&\, \forall n \geq 1 : \Pi_n(p) \leftrightarrows \Pi_n(q)\} \cup \{(u,v) \,:\, u,v \in \mathbb{DP}^\infty(pBPA + PR) \,\&\, \forall n \geq 1 : \Pi_n(u) \leftrightarrows \Pi_n(v)\}\Big). \quad (3.3)$$

Basically, R relates two processes iff they have bisimilar n-th projections for all possible n.

Let $(p,q) \in R$ for some $p,q \in \mathbb{SP}^\infty(pBPA + PR)$. p and q have HNFs[9], i.e., for some $n \in \mathbb{N}$, processes p_i and probabilities ρ_i, $1 \leq i \leq n$,

$$p \equiv p_1 \leftthreetimes_{\rho_1} p_2 \ldots p_{n-1} \leftthreetimes_{\rho_{n-1}} p_n \quad (3.4)$$

where for each i,

$$p_i \equiv \sum_{j<g_i} a_{ij} \cdot p_{ij} + \sum_{k<h_i} b_{ik}$$

for certain $g_i, h_i \in \mathbb{N}$ with $g_i + h_i > 0$, $a_{ij}, b_{ij} \in A_\delta$ and processes p_{ij},
and for some $s \in \mathbb{N}$, processes q_i and probabilities σ_i, $1 \leq i \leq s$,

$$q \equiv q_1 \leftthreetimes_{\sigma_1} q_2 \ldots q_{s-1} \leftthreetimes_{\sigma_{s-1}} q_s \quad (3.5)$$

where for each i,

$$q_i \equiv \sum_{j<e_i} c_{ij} \cdot q_{ij} + \sum_{k<f_i} d_{ik}$$

for certain $e_i, f_i \in \mathbb{N}$ with $e_i + f_i > 0$, $c_{ij}, d_{ij} \in A_\delta$ and processes q_{ij}. Due to $(p,q) \in R$,

$$\forall m \geq 1 : \Pi_m(p) \leftrightarrows \Pi_m(q).$$

The remainder of the proof shows that $p \leftrightarrows q$.

Probabilistic transitions. Let us suppose that $p \rightsquigarrow u$ for some u. From the definition of the operational rules and from (3.4) follows that $u \equiv \breve{p}_i$ for some $i, 1 \leq i \leq n$. Now define, for $m \geq 1$

$$S^i_m = \{v \,:\, q \rightsquigarrow v \,\&\, \Pi_m(\breve{p}_i) \leftrightarrows \Pi_m(v)\}.$$

We can make the following observations:

P1. Because $\Pi_m(p) \leftrightarrows \Pi_m(q)$ and $\Pi_m(p) \rightsquigarrow \Pi_m(\breve{p}_i)$ it follows that there exists v such that $\Pi_m(q) \rightsquigarrow \Pi_m(v)$ and $\Pi_m(v) \leftrightarrows \Pi_m(\breve{p}_i)$. But from (3.5) we have that $\Pi_m(v) \equiv \Pi_m(\breve{q}_t)$ for certain $t, 1 \leq t \leq s$. Moreover, from (3.5) we also get that $q \rightsquigarrow \breve{q}_t$. Combining these results we obtain that $\breve{q}_t \in S^i_m$. By this we have proved that $S^i_m \neq \emptyset$ for each $m \geq 1$.

P2. For each $m \geq 1$, $S^i_m \subseteq \{\breve{q}_1, \ldots, \breve{q}_s\}$ from which it follows that S^i_m are finite sets.

P3. $\Pi_{m+1}(\breve{p}_i) \leftrightarrows \Pi_{m+1}(\breve{q}_t)$ implies $\Pi_m(\breve{p}_i) \leftrightarrows \Pi_m(\breve{q}_t)$. Hence, $S^i_1 \supseteq S^i_2 \supseteq \ldots$.

[8] Since $p,q \in \mathbb{PT}^\infty(pBPA + PR)$ according to Proposition 3.3.43 and 3.3.44 they have finite branching.

[9] Actually we should write $\leftrightarrows$ instead of $\equiv$. But without loss of generality using the Congruence theorem we can write $\equiv$.

Due to the fact that S^i_m is a decreasing sequence of finite sets it follow that there exists an $\overline{m} \in \mathbb{N}$ such that

$$S^i_{\overline{m}} = \bigcap_{m \geq 1} S^i_m \neq \emptyset.$$

Therefore, there is a $v \in \bigcap_{m \geq 1} S^i_m$ such that $q \rightsquigarrow v$ and $\Pi_m(v) \leftrightarrow \Pi_m(u)$ for each $m \geq 1$. In other words, $q \rightsquigarrow v$ and $(u, v) \in R$.

Action transitions. Let $(u, v) \in R$ for some $u, v \in \mathbb{DP}^\infty(\textbf{\textit{pBPA}} + PR)$. Then u and v have dynamic HNFs, i.e.,

$$u \equiv \sum_{j<g} \breve{a}_j \cdot s_j + \sum_{k<h} \breve{b}_k$$

for certain $g, h \in \mathbb{N}$ with $g + h > 0$, $a_j, b_j \in A_\delta$ and processes s_j, and

$$v \equiv \sum_{j<e} \breve{c}_j \cdot r_j + \sum_{k<f} \breve{d}_k$$

for certain $e, f \in \mathbb{N}$ with $e + f > 0$, $c_j, d_j \in A_\delta$ and processes r_j. Since $(u, v) \in R$, from the definition of R it follows that:

$$\forall m \geq 1 : \Pi_m(u) \leftrightarrow \Pi_m(v).$$

Let us suppose that $u \xrightarrow{a} p$ for some p and atomic action a. From the definition of the operational rules and the form of u it follows that $a \equiv a_j$ and $p \equiv s_j$ for some $j, 1 \leq j \leq g$. In a similar way as before for each $m \geq 1$ we define a set:

$$S^i_m = \{q \ : \ v \xrightarrow{a} q \ \& \ \Pi_m(\breve{a} \cdot s_j) \leftrightarrow \Pi_m(q)\},$$

and we conclude that:

A1. $\Pi_m(u) \xrightarrow{a} \Pi_{m-1}(s_j)$ for $m \geq 1$. Since $\Pi_m(u) \leftrightarrow \Pi_m(v)$ it follows that $\Pi_m(v) \xrightarrow{a} \Pi_{m-1}(r_k)$ and $\Pi_{m-1}(r_k) \leftrightarrow \Pi_{m-1}(s_j)$ for some r_k. In fact, $v \xrightarrow{a} r_k$ for some $k < e$ (according to the form of v). Hence, $r_k \in S^j_m$ which implies $S^j_m \neq \emptyset$.

A2. For each $m \geq 1$, $S^j_m \subseteq \{r_1, \ldots, r_e\}$ from which it follows that S^j_m are finite sets.

A3. $\Pi_{m+1}(p) \leftrightarrow \Pi_{m+1}(q)$ implies $\Pi_m(p) \leftrightarrow \Pi_m(q)$. Therefore, $S^j_1 \supseteq S^j_2 \supseteq \ldots$.

Thus we have that $\bigcap_{j \geq 1} S^j_m$ is a non-empty set. Thus, if $q \in \bigcap_{j \geq 1} S^j_m$, then $v \xrightarrow{a} q$ and $\Pi_m(p) \leftrightarrow \Pi_m(q)$ for all $m \geq 1$. It gives us the conclusion $(p, q) \in R$.

Action termination. Let be $(u, v) \in R$ for some $u, v \in \mathbb{DP}^\infty(\textbf{\textit{pBPA}} + PR)$. Assume that $u \xrightarrow{a} \surd$. Then $\Pi_1(u) \xrightarrow{a} \surd$ according to the deduction rules. Since $\Pi_1(u) \leftrightarrow \Pi_1(v)$ we obtain that $\Pi_1(v) \xrightarrow{a} \surd$. From the deduction rules we conclude that $v \xrightarrow{a} \surd$.

PDF. Finally, we need to prove that for an arbitrary equivalence class $M \in \mathbb{PT}^\infty(\textbf{\textit{pBPA}} + PR)/R$ and a pair $(p, q) \in R$ for $p, q \in \mathbb{SP}^\infty(\textbf{\textit{pBPA}} + PR)$, it holds that $\mu(p, M) = \mu(q, M)$. Again we consider only reachable classes, i.e., we assume that there are elements $u, v \in M$ such that $p \rightsquigarrow u$ and $q \rightsquigarrow v$. We write $M = [u]_R = [v]_R$. The previous discussion about probabilistic transitions provides that u exists if and only if v exists; in other words M is reachable from p

iff it is reachable from q. Moreover, for u and v we have that for each $m \geq 1$, $\Pi_m(u) \underline{\leftrightarrow} \Pi_m(v)$ because $(u, v) \in R$. Therefore, $[\Pi_m(u)]_{\underline{\leftrightarrow}} = [\Pi_m(v)]_{\underline{\leftrightarrow}}$.

The idea of the proof is to find a link between the probability to reach the n-th projection of an R equivalence class, say $\Pi_n([u]_R)$ from p and the probability to reach the $\underline{\leftrightarrow}$ equivalence class of $\Pi_n(u)$ also from p. Clearly, we are only interested in these elements of the two classes that p can reach.

From the previous results and from the definition of R we have that:

N1. $\mu(p, [u]_R) = \mu(\Pi_m(p), \Pi_m([u]_R))$ by Proposition 3.3.21*iv.*,

N2. $\mu(q, [u]_R) = \mu(\Pi_m(q), \Pi_m([u]_R))$ also by Proposition 3.3.21*iv.*,

N3. Since $\Pi_m(p) \underline{\leftrightarrow} \Pi_m(q)$ for all $m \geq 1$, the definition of $\underline{\leftrightarrow}$ implies $\mu(\Pi_m(p), [\Pi_m(u)]_{\underline{\leftrightarrow}}) = \mu(\Pi_m(q), [\Pi_m(u)]_{\underline{\leftrightarrow}})$.

We claim that (the proof is given below):

Claim There is an $\overline{m}_p \in \mathbb{N}, \overline{m}_p \geq 1$ such that

$$\mu(\Pi_{\overline{m}_p}(p), \Pi_{\overline{m}_p}([u]_R)) = \mu(\Pi_{\overline{m}_p}(p), [\Pi_{\overline{m}_p}(u)]_{\underline{\leftrightarrow}}).$$

Then, if $\overline{m}_p$ and $\overline{m}_q$ are such that: $\mu(\Pi_{\overline{m}_p}(p), \Pi_{\overline{m}_p}([u]_R)) = \mu(\Pi_{\overline{m}_p}(p), [\Pi_{\overline{m}_p}(u)]_{\underline{\leftrightarrow}})$ and $\mu(\Pi_{\overline{m}_q}(q), \Pi_{\overline{m}_q}([u]_R)) = \mu(\Pi_{\overline{m}_q}(q), [\Pi_{\overline{m}_q}(u)]_{\underline{\leftrightarrow}})$ (the existence of $\overline{m}_p$ and $\overline{m}_q$ is guaranteed by the claim above) and if $\overline{m} = \max\{\overline{m}_p, \overline{m}_q\}$ (the reason we take max value among these two is elaborated in the proof of the claim), it follows easily that:

$$\begin{aligned}\mu(p, M) &= \mu(p, [u]_R) \overset{\mathbf{N1}}{=} \mu(\Pi_{\overline{m}}(p), \Pi_{\overline{m}}([u]_R) \overset{\mathbf{Claim}}{=} \mu(\Pi_{\overline{m}}(p), [\Pi_{\overline{m}}(u)]_{\underline{\leftrightarrow}}) \\ &\overset{\mathbf{N3}}{=} \mu(\Pi_{\overline{m}}(q), [\Pi_{\overline{m}}(u)]_{\underline{\leftrightarrow}}) \overset{\mathbf{Claim}}{=} \mu(\Pi_{\overline{m}}(q), \Pi_{\overline{m}}([u]_R) \overset{\mathbf{N2}}{=} \mu(q, [u]_R) = \mu(q, M).\end{aligned}$$

This finishes the proof of the theorem. Next we give the proof of the claim.

□

Proof of the Claim. Using the definition of R it is easy to prove that for a process u reachable from p, $\Pi_m([u]_R) \subseteq [\Pi_m(u)]_{\underline{\leftrightarrow}}$, for each $m \geq 1$. This implies that:

$$\mu(\Pi_m(p), \Pi_m([u]_R)) \leq \mu(\Pi_m(p), [\Pi_m(u)]_{\underline{\leftrightarrow}}).$$

We will create a procedure that finds the smallest $\overline{m}$ for which $\mu(\Pi_m(p), \Pi_m([u]_R)) = \mu(\Pi_m(p), [\Pi_m(u)]_{\underline{\leftrightarrow}})$. Informally, if the degree of projection m is not high enough the m-th projection of two processes can be bisimilar even though the processes themselves are not bisimilar. But since they are not bisimilar, there must exist a finite projection that "distinguishes" them. The idea of the proof is the following: First we detect that the projection we cope with is not high enough since $[\Pi_m(u)]_{\underline{\leftrightarrow}} \setminus \Pi_m([u]_R) \neq \emptyset$. This means that if we look at some higher projection Π_{n_u} it will refine the class $[\Pi_m(u)]_{\underline{\leftrightarrow}}$ by removing all processes that are not bisimilar to u. To end the proof, we explain that if a set of processes Z is considered instead of one single process, then it is sufficient to take the highest projection among all projections Π_{n_u} for the elements of Z.

Let us suppose that for $m \geq 1$, $\mu(\Pi_m(p), \Pi_m([u]_R)) < \mu(\Pi_m(p), [\Pi_m(u)]_{\underline{\leftrightarrow}})$. (3.8)
Let $D_m(u) = \{w : w \in [\Pi_m(u)]_{\underline{\leftrightarrow}} \setminus \Pi_m([u]_R)$ and w is reachable from $\Pi_m(p)\}$. From the assumption (3.8) follows that $D_m(u) \neq \emptyset$. Otherwise $\mu(\Pi_m(p), \Pi_m([u]_R)) = \mu(\Pi_m(p), [\Pi_m(u)]_{\underline{\leftrightarrow}})$ which contradicts the assumption.

Now, if $w \in D_m(u)$, then $\Pi_m(p) \rightsquigarrow w$. Furthermore, there exist $z \in \mathbb{DP}^{\infty}(\textit{pBPA} + PR)$ and a natural number n_z such that:

1. $w \equiv \Pi_m(z)\ \&\ p \rightsquigarrow z$ (by the SOS rules);
2. $\Pi_m(z) \underline{\leftrightarrow} \Pi_m(u)$ (since $\Pi_m(z) \in D_m(u)$ and therefore $\Pi_m(z) \in [\Pi_m(u)]_{\underline{\leftrightarrow}}$);
3. $z \notin [u]_R$ (since $\Pi_m(z) \notin \Pi_m([u]_R)$);
4. $\Pi_{n_z}(z) \underline{\not\leftrightarrow} \Pi_{n_z}(u)$ (from 3.) and $\Pi_{n_z}(z) \notin [\Pi_{n_z}(u)]_{\underline{\leftrightarrow}}$ (from the definition of R as follows: $(u,z) \notin R$ iff $\neg(\forall n \geq 1 : \Pi_n(z) \underline{\leftrightarrow} \Pi_n(u))$ iff $\exists n_z : \Pi_{n_z}(z) \underline{\not\leftrightarrow} \Pi_{n_z}(u)$);
5. $\forall k \leq m : \Pi_k(z) \underline{\leftrightarrow} \Pi_k(u)$ (from 2. and Proposition 3.3.45)
6. $n_z > m$ (from 4. and 5.);
7. $\Pi_{n_z}(z) \notin D_{n_z}(u)$ (from 4).

Moreover, from the definition of $\Pi_m([u]_R)$ we have that

8. $\forall v :\ \forall k : \Pi_k(v) \in \Pi_k([u]_R) \Leftrightarrow v \in [u]_R$, i.e., $\forall v :\ \forall k : \Pi_k(v) \notin \Pi_k([u]_R) \Leftrightarrow v \notin [u]_R$.

Then from Proposition 3.3.45 and (8) follows that

$$\forall v : \forall m \geq 1 :\ \Pi_{m+1}(v) \in D_{m+1}(u) \Rightarrow \Pi_m(v) \in D_m(u). \tag{9}$$

Thus having that the set of reachable processes from p, say $Z = \{z_i : p \rightsquigarrow z_i\}$, such that $\Pi_1(z_i) \in D_1(u)$ is a finite set, from the previous discussion follows that for each $z_i \in Z$ there is a natural number n_{z_i} such that $\Pi_{n_{z_i}}(z_i) \underline{\not\leftrightarrow} \Pi_{n_{z_i}}(u)$. Let $\overline{n}_{z_i}$ be the least of all such numbers that exist for z_i. From the conclusion 7. we have that $\Pi_{\overline{n}_{z_i}}(z_i) \notin D_{\overline{n}_{z_i}}(u)$. And moreover from (9) follows that if $\overline{n}_{z_i} \leq \overline{n}_{z_j}$, then $\Pi_{\overline{n}_{z_i}}(z_i) \notin D_{\overline{n}_{z_j}}(u)$. Taking

$$\overline{m} = \max_{z_i}\{\overline{n}_{z_i} : \Pi_1(z_i) \in D_1(u)\ \&\ p \rightsquigarrow z_i\}$$

we obtain that $\forall z_i \in Z : \Pi_1(z_i) \in D_1(u)\ \&\ p \rightsquigarrow z_i\ \Rightarrow\ \Pi_{\overline{m}}(z_i) \notin D_{\overline{m}}(u)$. Or in other words, if $\Pi_{\overline{m}}(p) \rightsquigarrow \Pi_{\overline{m}}(z)$ then ($\Pi_{\overline{m}}(z) \in [\Pi_{\overline{m}}(u)]_{\underline{\leftrightarrow}}$ iff $\Pi_{\overline{m}}(z) \in \Pi_{\overline{m}}([u]_R)$). □

Example 3.3.49. Let R be the relation defined in (3.3) and consider process p which is the solution of $X = a \uplus_{\frac{1}{2}} a \cdot a \uplus_{\frac{1}{6}} a \cdot X \uplus_{\frac{1}{4}} a \cdot a \cdot X$, for $a \in A$. Then, the set of reachable processes from p is $\mathcal{RP}(p) = \{\breve{a}, \breve{a} \cdot a, \breve{a} \cdot p, \breve{a} \cdot a \cdot p\}$ and it is clear that $[\breve{a}]_R \neq [\breve{a} \cdot a]_R \neq [\breve{a} \cdot p]_R \neq [\breve{a}]_R$ but $[\breve{a} \cdot p]_R = [\breve{a} \cdot a \cdot p]_R$. Hence, for all $n \geq 1$: $\Pi_n([\breve{a}]_R) \neq \Pi_n([\breve{a} \cdot a]_R) \neq \Pi_n([\breve{a} \cdot p]_R) \neq \Pi_n([\breve{a}]_R)$ but $\Pi_n([\breve{a} \cdot p]_R) = \Pi_n([\breve{a} \cdot a \cdot p]_R)$.
From the definition of the PDF we calculate that: $\mu(\Pi_n(p), \Pi_n([\breve{a}]_R) = 1/2$, $\mu(\Pi_n(p), \Pi_n([\breve{a} \cdot a]_R) = 1/6$ and $\mu(\Pi_n(p), \Pi_n([\breve{a} \cdot p]_R) = \mu(\Pi_n(p), \Pi_n([\breve{a} \cdot a \cdot p]_R) = 1/3$.

n=1. Let us now investigate the classes $[\Pi_1(z)]_{\underline{\leftrightarrow}}$, for $z \in \mathcal{RP}(p)$. We know that $[\Pi_1(\breve{a})]_{\underline{\leftrightarrow}} = [\Pi_1(\breve{a} \cdot a)]_{\underline{\leftrightarrow}} = [\Pi_1(\breve{a} \cdot p)]_{\underline{\leftrightarrow}} = [\Pi_1(\breve{a} \cdot a \cdot p)]_{\underline{\leftrightarrow}}$. Therefore for all $z \in \mathcal{RP}(p)$, $\mu(\Pi_1(p), [\Pi_1(z)]_{\underline{\leftrightarrow}}) = 1$. Consequently, $\mu(\Pi_1(p), \Pi_1([z]_R)) < \mu(\Pi_1(p), [\Pi_1(z)]_{\underline{\leftrightarrow}})$. Since the first projection does not give the desired result: $\mu(\Pi_1(p), \Pi_1([z]_R)) = \mu(\Pi_1(p), [\Pi_1(z)]_{\underline{\leftrightarrow}})$ as described in the proof of the Claim we build the set $D_(z)$. We find that:

$D_1(\breve{a}) = \{\Pi_1(\breve{a} \cdot a), \Pi_1(\breve{a} \cdot p), \Pi_1(\breve{a} \cdot a \cdot p)\}$

$D_1(\breve{a} \cdot a) = \{\Pi_1(\breve{a}), \Pi_1(\breve{a} \cdot p), \Pi_1(\breve{a} \cdot a \cdot p)\}$

$D_1(\breve{a} \cdot p) = D_1(\breve{a} \cdot a \cdot p) = \{\Pi_1(\breve{a}), \Pi_1(\breve{a} \cdot a)\}$

and in the next step we investigate $[\Pi_2(z)]_{\underline{\leftrightarrow}}$.

n=2. We have that: $[\Pi_2(\breve{a})]_{\underline{\leftrightarrow}} \neq [\Pi_2(\breve{a}\cdot a)]_{\underline{\leftrightarrow}} = [\Pi_2(\breve{a}\cdot p)]_{\underline{\leftrightarrow}} = [\Pi_2(\breve{a}\cdot a\cdot p)]_{\underline{\leftrightarrow}}$, and thus $D_2(\breve{a}) = \emptyset$ and $\mu(\Pi_2(p), \Pi_2([\breve{a}]_R)) = \mu(\Pi_2(p), [\Pi_2(\breve{a})]_{\underline{\leftrightarrow}})$. From this we conclude that $\overline{n}_{\breve{a}} = 2$. Further we find that:

$D_2(\breve{a}\cdot a) = \{\Pi_2(\breve{a}\cdot p), \Pi_2(\breve{a}\cdot a\cdot p)\}$ and

$D_2(\breve{a}\cdot p) = D_2(\breve{a}\cdot a\cdot p) = \{\Pi_2(\breve{a}\cdot a)\}$

Thus, for $z \in \{\breve{a}\cdot a, \breve{a}\cdot p, \breve{a}\cdot a\cdot p\}$ we still have that: $\mu(\Pi_2(p), \Pi_2([z]_R)) < \mu(\Pi_2(p), [\Pi_2(z)]_{\underline{\leftrightarrow}})$. So, we go one projection higher.

n=3. Finally, for the third projection we obtain: $D_3(\breve{a}\cdot a) = \emptyset$ and $D_3(\breve{a}\cdot p) = D_3(\breve{a}\cdot a\cdot p) = \emptyset$ which says that $\overline{n}_{\breve{a}\cdot a} = 3$ and $\overline{n}_{\breve{a}\cdot p} = 3$ and $\overline{n}_{\breve{a}\cdot a\cdot p} = 3$. Thus we have derived that $\overline{m} = 3$ and for all $z \in \mathcal{RP}(p)$, and for all $k \geq 3$, $\mu(\Pi_k(p), \Pi_k([z]_R)) = \mu(\Pi_k(p), [\Pi_k(z)]_{\underline{\leftrightarrow}})$. □

3.3.3 Model of finite processes of *pBPA* and the properties of the model

One way to obtain the finite model of *pBPA* is to restrict the $\mathcal{M}_{pBPA+PR}$ model presented in Section 3.3.2, namely to restrict the domain on finite processes and the other constitutive elements of the model which are related to the infinite processes. Thus, the set of static processes, $\mathbb{SP}(pBPA)$, is defined by the clauses 1, 3-5 in Definition 3.3.2 (pg. 49). The set $\mathbb{D}(pBPA)$ is defined by the clauses 1-3 in Definition 3.3.3 (pg. 49). The set of dynamic processes $\mathbb{DP}(pBPA)$ is defined by the clauses 1-3 in Definition 3.3.4 (pg. 50). Thus, the domain becomes $\mathbb{PT}(pBPA) = \mathbb{SP}(pBPA) \cup \mathbb{DP}(pBPA)$. The set of deduction rules is equal to $\mathbf{DR}_{pBPA+PR})$ (pg. 54 without the rules in Table 3.9 and 3.11. The probability distribution function on $\mathbb{PT}(pBPA)$ is defined by the equalities given in Table 3.6+3.7 (pg. 51). The definition of bisimulation relation is given in Definition 3.3.11 (pg. 53) with PRA replaced by *pBPA*.

Many properties remain correct in $\mathbb{PT}(pBPA)$ and we just list them without proofs. Thus, we claim that the propositions: 3.3.18, 3.3.20, 3.3.21*i-iii*, 3.3.22, 3.3.23, 3.3.24, 3.3.26, 3.3.27, 3.3.28, 3.3.30, 3.3.31 and 3.3.32 hold when restricted on $\mathbb{PT}(pBPA)$. The corollaries 3.3.25 and 3.3.29 hold as well. The proofs can be easily obtained by the proofs given in the previous two sections.

Theorem 3.3.50 (*Congruence of* $\mathbb{PT}(pBPA)$). $\underline{\leftrightarrow}$ is a congruence relation on $\mathbb{PT}(pBPA)$ with respect to the operators: $+$, $\cdot$ and $\leftrightarrows_\pi$, $\pi \in \langle 0, 1\rangle$. □

Theorem 3.3.51 (*Soundness of pBPA*). Let $\mathbf{x}$ and $\mathbf{y}$ be closed *pBPA* terms. If $pBPA \vdash \mathbf{x} = \mathbf{y}$, then $x \underline{\leftrightarrow} y$. □

Completeness of *pBPA*

To prove completeness for *pBPA* with respect to the presented model $\mathcal{M}_{pBPA}$, we use the direct method. In order to do this, we first derive some results which relate transitions in the model with equalities in the algebra. Some results guarantee the decrease of the number of operators or the decrease of the number of occurrences of the probabilistic choice operator, n_{pc}, for terms connected by a transition. It gives us a possibility to use induction on these numbers (based on the structure of terms) in the proofs of the Completeness theorem and two lemmas towards it.

The direct method for proving the completeness property of non-probabilistic process algebras PRA ([26, 108]) with respect to its bisimulation model $\mathcal{M}$ usually is based on the proof of the following implication: for all closed terms s and t of PRA we have that

$$\mathcal{M} \models s + t \underline{\leftrightarrow} t \Rightarrow PRA \vdash s + t = t. \tag{3.6}$$

This implication usually is proved by induction. Then using the idempotency law of the non-deterministic choice operator the completeness is directly obtained. In the case of probabilistic process algebras this condition is not sufficient since the idempotency law does not hold for an arbitrary term. But still it gives an idea about the directions of the proof. Namely, the implication used to prove completeness in non-probabilistic process algebras, which is:

$$((s + t \leftrightarrows t \Rightarrow s + t = t) \,\&\, s \leftrightarrows t) \Rightarrow s = t,$$

in probabilistic process algebras is valid only for $\mathcal{D}(PRA)$ terms (see Proposition 3.2.17). Thus, partly this approach can be followed.

One more problem arises in the proof of (3.6) in the probabilistic setting. The use of the induction method in this proof leads to a situation in which an application of the induction hypothesis for non-$\mathcal{D}(PRA)$ terms is required. In other words, as a consequence of the inductive definition of the basic terms in which the definition of basic $\mathcal{B}_+(PRA)$ terms and $\mathcal{B}(PRA)$ terms interleaves, "interleaving" of two hypothesis, one for basic $\mathcal{B}(PRA) \setminus \mathcal{B}_+(PRA)$ terms and the other for basic $\mathcal{B}_+(PRA)$ terms, is necessary. For these reasons, two lemmas are given. The first one pertains to the part of the Completeness theorem about basic $\mathcal{B}(PRA) \setminus \mathcal{B}_+(PRA)$ terms, but it needs a hypothesis concerning basic $\mathcal{B}_+(PRA)$ terms. Later the second lemma considers basic $\mathcal{B}_+(PRA)$ terms and in the proof the first lemma is used.

The strategy taken in the given proofs is based on the Elimination theorem and the form of the *pBPA* basic terms as described in Remark 3.2.20. The Elimination theorem (Theorem 3.2.23) yields that it is enough to consider only basic terms instead of closed terms in general. By doing so, we can benefit from the special form that basic terms of *pBPA* have. We know that a basic term is an element of $\mathcal{B}_+(pBPA) \subset \mathcal{D}(pBPA)$ in which case we can use all properties of these terms given in the previous section. Or it is a probabilistic choice of $\mathcal{B}_+(pBPA)$ basic terms in which case we can employ an inductive proof on the number of probabilistic choice operators occurring in the basic term.

Proposition 3.3.52. If $\mathbf{p}$ is a basic *pBPA* term in the form (3.2) (Remark 3.2.20), then $p \rightsquigarrow x$ with $\mu(p, x) = \rho$ iff $x \equiv x_i$ for some $i,\ 1 \leq i \leq n$ and $\rho = \sum_{j \in Q_{\mathbf{x_i}}} \pi_j$, where $Q_{\mathbf{x_i}} = \{j \ :\ 1 \leq j \leq n, \mathbf{x_i} \equiv \mathbf{x_j}\}$ and $\pi_n = 1 - \sum_{j=1}^{n-1} \pi_j$.

Proof. Let $\mathbf{p}$ be a basic term in the form $\mathbf{p} \equiv \mathbf{x_1} \between_{\pi_1} \mathbf{x_2} \between_{\pi_2} \mathbf{x_3} \ldots \mathbf{x_{n-1}} \between_{\pi_{n-1}} \mathbf{x_n}$, for $n \geq 2$. Informally, the claim says that if $\mu(p, \breve{x}) = \rho > 0$, then $\mathbf{x}$ may appear more than once as a sub-term of $\mathbf{p}$ and the indices of all occurrences of $\mathbf{x}$ are placed in the set $Q_{\mathbf{x}}$. Moreover, ρ is the sum of all probabilities assigned to these occurrences. It is clear that the set $\{Q_{\mathbf{x}} \ :\ \mathbf{x} \text{ is a sub-term of } \mathbf{p}\}$ is a partition of the set $\{1, 2, \ldots, n\}$. Instead of $Q_{\mathbf{x_i}}$ we write Q_i in short. The proof of both directions is given by induction on n.

($\Leftarrow$)

`Basis` Let $n = 2$, that is, $\mathbf{p} \equiv \mathbf{x_1} \between_{\pi_1} \mathbf{x_2}$. By Proposition 3.3.24 we have that the only possible probabilistic transitions of x_1 and x_2 are $x_1 \rightsquigarrow \breve{x}_1$ and $x_2 \rightsquigarrow \breve{x}_2$, respectively. Besides, $\mu(x_1, \breve{x}_1) = 1$ and $\mu(x_2, \breve{x}_2) = 1$. From Corollary 3.3.25 *i.* and the definition of the operational rules follows that

Case $\mathbf{x_1} \not\equiv \mathbf{x_2}$. $p \rightsquigarrow \breve{x}_1$ and $p \rightsquigarrow \breve{x}_2$ with $\mu(p, \breve{x}_1) = \pi_1$ and $\mu(p, \breve{x}_2) = 1 - \pi_1$. The result holds because $Q_1 = \{1\}$ and $Q_2 = \{2\}$;

Case $\mathbf{x_1} \equiv \mathbf{x_2}$. $Q_1 = Q_2 = \{1,2\}$ and $\sum_{j \in Q_1} \pi_j = 1$. Therefore, $p \rightsquigarrow \breve{x}_1$ with $\mu(p, \breve{x}_1) = \pi + (1 - \pi) = 1$.

`Inductive step` Let be $\mathbf{p} \equiv \mathbf{x_1} \leftthreetimes_{\pi_1} \mathbf{x_2} \leftthreetimes_{\pi_2} \ldots \leftthreetimes_{\pi_{n-1}} \mathbf{x_n} \equiv \mathbf{x_1} \leftthreetimes_{\pi_1} (\mathbf{x_2} \leftthreetimes_{\frac{\pi_2}{1-\pi_1}} \mathbf{x_3} \ldots \mathbf{x_{n-1}} \leftthreetimes_{\frac{\pi_{n-1}}{1-\pi_1}} \mathbf{x_n})$ for $n \geq 3$. Let us write $\mathbf{q}$ for $\mathbf{x_2} \leftthreetimes_{\frac{\pi_2}{1-\pi_1}} \mathbf{x_3} \ldots \mathbf{x_{n-1}} \leftthreetimes_{\frac{\pi_{n-1}}{1-\pi_1}} \mathbf{x_n}$. From Proposition 3.3.24 it follows that the only possible probabilistic transition of x_1 is $x_1 \rightsquigarrow \breve{x}_1$ and $\mu(x_1, \breve{x}_1) = 1$. From the inductive hypothesis for k, $2 \leq k \leq n$ we have that $q \rightsquigarrow \breve{x}_k$ and $\mu(q, \breve{x}_k) = \rho'_k$, where $\rho'_k = \sum_{j \in Q'_k} \frac{\pi_j}{1-\pi_1}$ and $Q'_k = \{j \,:\, 2 \leq j \leq n, \mathbf{x_k} \equiv \mathbf{x_j}\}$. Combining these two results it follows that two cases should be investigated:

Case $\mathbf{x_1} \equiv \mathbf{x_k}$ *for some* k, $2 \leq k \leq n$. $Q_1 = Q'_k \cup \{1\}$ and also $p \rightsquigarrow \breve{x}_1$ with $\mu(p, \breve{x}_1) = \pi_1 + (1 - \pi_1) \cdot \rho'_k = \rho_k$, where $\rho_k = \sum_{j \in Q_1} \pi_j$. Moreover, for all l, $2 \leq l \leq n$, such that $\mathbf{x_1} \not\equiv \mathbf{x_l}$ we have that $Q_l = Q'_l$. Then from the definition of the operational rules we obtain $p \rightsquigarrow \breve{x}_l$ and $\mu(p, \breve{x}_l) = (1 - \pi_1)\rho'_l = \rho_l$ where $\rho_l = \sum_{j \in Q_l} \pi_j$;

Case $\mathbf{x_1} \not\equiv \mathbf{x_k}$ *for each* k, $2 \leq k \leq n$. $Q'_k = Q_k$ and $Q_1 = \{1\}$. From the definition of the operational rules we have $p \rightsquigarrow \breve{x}_1$ and $p \rightsquigarrow \breve{x}_k$. And also $\mu(p, \breve{x}_1) = \pi_1$ and $\mu(p, \breve{x}_k) = (1 - \pi_1)\rho'_k = \rho_k$ where $\rho_k = \sum_{j \in Q_k} \pi_j$.

($\Rightarrow$)

`Basis` Let $n = 2$, that is, $\mathbf{p} \equiv \mathbf{x_1} \leftthreetimes_{\pi_1} \mathbf{x_2}$ and $p \rightsquigarrow \breve{x}$ for some $\breve{x} \in \mathbb{DP}(\textit{pBPA})$. One of the following cases occurs:

Case $x_1 \rightsquigarrow \breve{x}$ *and* $\neg(x_2 \rightsquigarrow \breve{x})$. Then $\mu(x_2, \breve{x}) = 0$ and $\mu(p, \breve{x}) = \pi_1 \cdot \mu(x_1, \breve{x})$. By Proposition 3.3.24 we have that $\mu(x_1, \breve{x}) = 1$ and $x_1 \equiv x$. From Corollary 3.3.25 *i.* follows that $x_1 \not\equiv x_2$. This means that $Q_1 = \{1\}$ and $\mu(p, \breve{x}) = \sum_{j \in Q_1} \pi_j$;

Case $x_2 \rightsquigarrow \breve{x}$ *and* $\neg(x_1 \rightsquigarrow \breve{x})$. Then $\mu(x_1, \breve{x}) = 0$ and $\mu(p, \breve{x}) = (1 - \pi_1) \cdot \mu(x_2, \breve{x})$. In a similar way as in the first case we obtain that $\mu(x_2, \breve{x}) = 1$, $x_2 \equiv x$ and $\mu(p, \breve{x}) = \sum_{j \in Q_2} \pi_j$;

Case $x_1 \rightsquigarrow \breve{x}$ *and* $x_2 \rightsquigarrow \breve{x}$. Then $\mu(p, \breve{x}) = \pi_1 \cdot \mu(x_1, \breve{x}) + (1 - \pi_1) \cdot \mu(x_2, \breve{x})$. From Proposition 3.3.24 follows that $\mu(x_1, \breve{x}) = 1$, $x \equiv x_1$ and $\mu(x_2, \breve{x}) = 1$ and $x \equiv x_2$. Hence, $Q_1 = Q_2 = \{1,2\}$ and $\mu(p, \breve{x}) = \sum_{j \in Q_1} \pi_j = 1$.

`Inductive step` Let be $\mathbf{p} \equiv \mathbf{x_1} \leftthreetimes_{\pi_1} \mathbf{x_2} \leftthreetimes_{\pi_2} \ldots \leftthreetimes_{\pi_{n-1}} \mathbf{x_n} \equiv \mathbf{x_1} \leftthreetimes_{\pi_1} (\mathbf{x_2} \leftthreetimes_{\frac{\pi_2}{1-\pi_1}} \mathbf{x_3} \ldots \mathbf{x_{n-1}} \leftthreetimes_{\frac{\pi_{n-1}}{1-\pi_1}} \mathbf{x_n})$ for $n \geq 3$ and $p \rightsquigarrow \breve{x}$ for some $\breve{x} \in \mathbb{DP}(\textit{pBPA})$. Let us use the abbreviation $\mathbf{y} \equiv \mathbf{x_2} \leftthreetimes_{\frac{\pi_2}{1-\pi_1}} \mathbf{x_3} \ldots \mathbf{x_{n-1}} \leftthreetimes_{\frac{\pi_{n-1}}{1-\pi_1}} \mathbf{x_n}$. From the definition of operational rules one of the following situations can occur:

Case $x_1 \rightsquigarrow \breve{x}$ *and* $\neg(y \rightsquigarrow \breve{x})$. Then $\mu(p, \breve{x}) = \pi_1 \cdot \mu(x_1, \breve{x})$. From Proposition 3.3.24 follows that $\mu(x_1, \breve{x}) = 1$ and $x \equiv x_1$. Moreover, $\neg(x_k \rightsquigarrow \breve{x})$ and $x_1 \not\equiv x_k$, for each k, $2 \leq k \leq n$. Therefore, $Q_1 = \{1\}$ and $\mu(p, \breve{x}) = \sum_{j \in Q_1} \pi_j$;

Case $y \rightsquigarrow \breve{x}$ *and* $\neg(x_1 \rightsquigarrow \breve{x})$. Then $\mu(x_1, \breve{x}) = 0$ and $\mu(p, \breve{x}) = (1 - \pi_1) \cdot \mu(y, \breve{x})$. From the inductive hypothesis follows that there exists k, $2 \leq k \leq n$ such that $x \equiv x_k$ and $\mu(y, \breve{x}) = \sum\limits_{j \in Q'_k} \frac{\pi_j}{1-\pi_1}$ where $Q'_k = \{j \ : \ 2 \leq j \leq n, \mathbf{x_k} \equiv \mathbf{x_j}\}$. From $\neg(x_1 \rightsquigarrow \breve{x})$ using Corollary 3.3.25 *i.* we have that $x_1 \not\equiv x_k$ and $Q_k = \{j \ : \ 1 \leq j \leq n, \mathbf{x_k} \equiv \mathbf{x_j}\} = Q'_k$. Thus, $\mu(p, \breve{x}) = (1 - \pi_1) \cdot \mu(y, \breve{x}) = (1 - \pi_1) \cdot \sum\limits_{j \in Q'_k} \frac{\pi_j}{1-\pi_1} = \sum\limits_{j \in Q_k} \pi_j$;

Case $x_1 \rightsquigarrow \breve{x}$ *and* $y \rightsquigarrow \breve{x}$. Then $\mu(p, \breve{x}) = \pi_1 \cdot \mu(x_1, \breve{x}) + (1 - \pi_1) \cdot \mu(y, \breve{x})$. From Proposition 3.3.24 follows that $\mu(x_1, \breve{x}) = 1$ and $x \equiv x_1$. Moreover, from the inductive hypothesis we have that there exists k, $2 \leq k \leq n$ such that $x \equiv x_k$ and $\mu(y, \breve{x}) = \sum\limits_{j \in Q'_k} \frac{\pi_j}{1-\pi_1}$ with $Q'_k = \{j \ : \ 2 \leq j \leq n, \mathbf{x_k} \equiv \mathbf{x_j}\}$. Then $x_1 \equiv x_k$ and also $Q_k = \{j \ : \ 1 \leq j \leq n, x_k \equiv x_j\} = Q'_k \cup \{1\}$. Thus, $\mu(p, \breve{x}) = \pi_1 \cdot \mu(x_1, \breve{x}) + (1 - \pi_1) \cdot \mu(y, \breve{x}) = \pi_1 + (1 - \pi_1) \cdot \sum\limits_{j \in Q'_k} \frac{\pi_j}{1-\pi_1} = \pi_1 + \sum\limits_{j \in Q'_k} \pi_j = \sum\limits_{j \in Q_k} \pi_j$.

□

Corollary 3.3.53. Let $\mathbf{p}$ be a basic *pBPA* term and $M \in \mathbb{PT}(\textit{pBPA})/\leftrightarrow$. If $x \rightsquigarrow \breve{x}_i$, $1 \leq i \leq n$, $n \in I\!N$, are all possible probabilistic transitions of x to the equivalence class M with $\mu(p, \breve{x}_i) = \sigma_i \in \langle 0, 1]$, then either $n \geq 2$ and

$$\mathbf{p} \equiv \mathbf{x'_1} \uplus_{\rho_1} \mathbf{x'_2} \uplus_{\rho_2} \mathbf{x'_3} \ldots \uplus_{\rho_{m-1}} \mathbf{x'_m},$$

for some $m \in I\!N, m \geq n$ and $\rho_k \in \langle 0, 1\rangle$, $1 \leq k \leq m$, $(\rho_m = 1 - \sum\limits_{j=1}^{m-1} \rho_j)$, and for some partition $Q_1, Q_2, \ldots, Q_n$ of $\{1, 2, \ldots, m\}$ such that $Q_i = \{j \ : \ 1 \leq j \leq m, \mathbf{x_i} \equiv \mathbf{x'_j}\}$ and $\sum\limits_{j \in Q_i} \rho_j = \sigma_i$, or

$$\mathbf{p} \equiv \mathbf{x'_1} \uplus_{\rho_1} \mathbf{x'_2} \uplus_{\rho_2} \mathbf{x'_3} \ldots \uplus_{\rho_{m-1}} \mathbf{x'_m} \uplus_{\rho_m} (\mathbf{y_1} \uplus_{\alpha_1} \mathbf{y_2} \uplus_{\alpha_2} \ldots \uplus_{\alpha_{r-1}} \mathbf{y_r})$$

for some $m, r \in I\!N$, $m \geq 1$, $r \geq 1$ and $\rho_k, \alpha_l \in \langle 0, 1\rangle$, $1 \leq k \leq m$, $1 \leq l \leq r$ and for some partition $Q_1, Q_2, \ldots, Q_n$ of the set $\{1, 2, \ldots, m\}$ such that $Q_i = \{j \ : \ 1 \leq j \leq m, \mathbf{x_i} \equiv \mathbf{x'_j}\}$ and $\sum\limits_{j \in Q_i} \rho_j = \sigma_i$ and for some basic $\mathcal{B}_+$ terms $\mathbf{y_l}$, $y_l \notin M$ or

$n = 1$ and $\sigma_1 = 1$ and

$$\mathbf{p} \equiv \mathbf{x_1} \uplus_{\rho_1} \mathbf{x_1} \uplus_{\rho_2} \mathbf{x_1} \ldots \uplus_{\rho_{m-1}} \mathbf{x_1},$$

for some $m \in I\!N$, $m \geq 1$ and $\rho_k \in \langle 0, 1]$, $1 \leq k \leq m$, $(\rho_m = 1 - \sum\limits_{j=1}^{m-1} \rho_j)$.

Lemma 3.3.54. (Cancellation law) If p, q and r are $\mathbb{PT}(\textit{pBPA})$ processes and $\pi \in \langle 0, 1\rangle$ such that $p \uplus_\pi q \leftrightarrows p \uplus_\pi r$, then $q \leftrightarrows r$.

Proof. Suppose $p \uplus_\pi q \leftrightarrows p \uplus_\pi r$. Then there exists a bisimulation R such that $(p \uplus_\pi q, p \uplus_\pi r) \in R$. Take the relation:

$$R' = Eq(R \cup \{(q, r)\}).$$

In order to prove that R' is a bisimulation we only need to investigate the pair (q, r). First, let us note that if $M \subseteq \mathbb{DP}(\textit{pBPA})$ is an R equivalence class, then M is an R' equivalence class as well because $(R' \setminus R) \cap (\mathbb{DP}(\textit{pBPA}) \times \mathbb{DP}(\textit{pBPA})) = \emptyset$. Namely, $\mathbb{DP}(\textit{pBPA})/R' = \mathbb{DP}(\textit{pBPA})/R$. Moreover, since

$M \in \mathbb{PT}(pBPA)/R$ and $(p \leftthreetimes_\pi r, q \leftthreetimes_\pi r) \in R$ we have that $\mu(p \leftthreetimes_\pi q, M) = \mu(p \leftthreetimes_\pi r, M)$. It implies $\mu(q, M) = \mu(r, M)$ by applying Proposition 3.3.21 *i*. To conclude, for each R' equivalence class M, $\mu(q, M) = \mu(r, M)$. □

Proposition 3.3.55. Let be $x \in \mathbb{D}(pBPA)$ and $a \in A$. Then:

i. if $\breve{x} \xrightarrow{a} \surd$, then $pBPA \vdash \mathbf{x} = \mathbf{a} + \mathbf{x}$;

ii. if $\breve{x} \xrightarrow{a} u$, then $pBPA \vdash \mathbf{x} = \mathbf{a} \cdot \mathbf{u} + \mathbf{x}$ and $op(u) < op(x)$.

Proof.

i. Let us suppose that $\breve{x} \xrightarrow{a} \surd$. The proof is given by induction on the structure of x.

Case $x \equiv b, b \in A_\delta, b \not\equiv a$. It does not apply;

Case $x \equiv a$. $pBPA \vdash \mathbf{x} = \mathbf{a} + \mathbf{a} = \mathbf{a} + \mathbf{x}$;

Case $x \equiv y \cdot z$. It does not apply;

Case $x \equiv y + z$. From the assumption $\breve{x} \xrightarrow{a} \surd$ follows that $\breve{y} \xrightarrow{a} \surd$ or $\breve{z} \xrightarrow{a} \surd$. By the inductive hypothesis $pBPA \vdash \mathbf{y} = \mathbf{a} + \mathbf{y}$ or $pBPA \vdash \mathbf{z} = \mathbf{a} + \mathbf{z}$. In each of these cases $pBPA \vdash \mathbf{x} = \mathbf{y} + \mathbf{z} = \mathbf{a} + \mathbf{y} + \mathbf{z} = \mathbf{a} + \mathbf{x}$.

ii. Let us suppose that $\breve{x} \xrightarrow{a} u$ for some $u \in \mathbb{SP}(pBPA)$. The proof is given by induction on x.

Case $x \equiv b, b \in A_\delta$. It does not apply;

Case $x \equiv y \cdot z$. One of the following situations is possible:

Subcase $\breve{y} \xrightarrow{a} v$. Then $u \equiv v \cdot z$. By the inductive hypothesis we have that $pBPA \vdash \mathbf{y} = \mathbf{a} \cdot \mathbf{v} + \mathbf{y}$ and $op(v) < op(y)$. Therefore, $pBPA \vdash \mathbf{x} = \mathbf{y} \cdot \mathbf{z} = (\mathbf{a} \cdot \mathbf{v} + \mathbf{y}) \cdot \mathbf{z} = \mathbf{a} \cdot \mathbf{v} \cdot \mathbf{z} + \mathbf{y} \cdot \mathbf{z} = \mathbf{a} \cdot \mathbf{u} + \mathbf{x}$ and $op(u) = op(v) + op(z) < op(x)$;

Subcase $\breve{y} \xrightarrow{a} \surd$. Then $u \equiv z$. From *i.* we have that $pBPA \vdash \mathbf{y} = \mathbf{a} + \mathbf{y}$. Therefore, $pBPA \vdash \mathbf{x} = (\mathbf{a} + \mathbf{y}) \cdot \mathbf{z} = \mathbf{a} \cdot \mathbf{z} + \mathbf{y} \cdot \mathbf{z} = \mathbf{a} \cdot \mathbf{u} + \mathbf{x}$ and $op(u) = op(z) < op(x)$;

Case $x \equiv y + z$. Then $\breve{y} \xrightarrow{a} u$ or $\breve{z} \xrightarrow{a} u$. By the inductive hypothesis follows that $pBPA \vdash \mathbf{y} = \mathbf{a} \cdot \mathbf{u} + \mathbf{y}$ and $op(u) < op(y)$ or $pBPA \vdash \mathbf{z} = \mathbf{a} \cdot \mathbf{u} + \mathbf{z}$ and $op(u) < op(z)$. In any of these cases $pBPA \vdash \mathbf{x} = \mathbf{y} + \mathbf{z} = \mathbf{a} \cdot \mathbf{u} + \mathbf{y} + \mathbf{z} = \mathbf{a} \cdot \mathbf{u} + \mathbf{x}$ and $op(u) < op(x)$

□

Proposition 3.3.56. If $p, q \in \mathbb{SP}(pBPA)$ and $v \in \mathbb{D}(pBPA)$, then $p \leftthreetimes_\pi q \leftrightarrow v$ iff ($p \leftrightarrow v$ and $q \leftrightarrow v$).

Proof. We have that $\mu(p \leftthreetimes_\pi q, \breve{v}) = \pi \cdot \mu(p, \breve{v}) + (1 - \pi) \cdot \mu(q, \breve{v}) = 1$, since $p \leftthreetimes_\pi q \leftrightarrow v$ and $\mu(v, \breve{v}) = 1$. Hence, $\mu(p, \breve{v}) = 1$ and $\mu(q, \breve{v}) = 1$ and applying Proposition 3.3.31 we obtain the conclusion. The other direction follows from the Congruence theorem. □

Lemma 3.3.57. If $x, y, z \in \mathbb{D}(pBPA)$, then $z \leftrightarrow x + y$ implies $z \leftrightarrow x + z$.

Proof. Let us assume that $z \leftrightarrows x + y$ for $x, y, z \in \mathbb{D}(pBPA)$ and let R be a bisimilation relation such that $(z, x + y) \in R$. We prove that relation R' given below is a bisimulation.

$$R' = Eq\Big(R \cup \{(z, x + z), (\breve{z}, \breve{x} + \breve{z})\}\Big).$$

We investigate only the "new" pairs in R'.

Probabilistic transitions and PDF. Since $z \rightsquigarrow \breve{z}$ and $x \rightsquigarrow \breve{x}$ are the only possible probabilistic transitions of z and x, respectively, with $\mu(z, \breve{z}) = 1$ and $\mu(x, \breve{x}) = 1$, the only possible probabilistic transition of $x + z$ is $x + z \rightsquigarrow \breve{x} + \breve{z}$. Moreover $\mu(x + z, \breve{x} + \breve{z}) = 1$. Hence, by the definition of R' we have $(\breve{z}, \breve{x} + \breve{z}) \in R'$.

Action transitions. If $\breve{z} \xrightarrow{a} u$, then also $\breve{x} + \breve{z} \xrightarrow{a} u$ and moreover $uR'u$.
Assume that $\breve{x} + \breve{z} \xrightarrow{a} u$. Then either $\breve{x} \xrightarrow{a} u$ or $\breve{z} \xrightarrow{a} u$. If $\breve{x} \xrightarrow{a} u$ then $\breve{x} + \breve{y} \xrightarrow{a} u$ and also $\breve{z} \xrightarrow{a} v$ for some v such that $(u, v) \in R$. Then $(u, v) \in R'$ as well. The second case where $\breve{z} \xrightarrow{a} u$ is trivial.

Action termination. If $\breve{z} \xrightarrow{a} \surd$, then also $\breve{x} + \breve{z} \xrightarrow{a} \surd$. Assume that $\breve{x} + \breve{z} \xrightarrow{a} \surd$. Then either $\breve{x} \xrightarrow{a} \surd$ or $\breve{z} \xrightarrow{a} \surd$. If $\breve{x} \xrightarrow{a} \surd$ then $\breve{x} + \breve{y} \xrightarrow{a} \surd$ and also $\breve{z} \xrightarrow{a} \surd$. The second case is trivial.

By this we have proved that R' is a bisimulation relation such that $(z, x + z) \in R'$ which means that $z \leftrightarrows x + z$. □

Lemma 3.3.58. If $\mathbf{u}$ and $\mathbf{z}$ are basic terms such that at least one of them belongs to $\mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$ and if

$$\forall \mathbf{x}, \mathbf{y} \in \mathcal{B}_+ \ : \ op(\mathbf{x}) + op(\mathbf{y}) < op(\mathbf{u}) + op(\mathbf{z}) \Rightarrow (x + y \leftrightarrows y \Rightarrow \mathbf{x} + \mathbf{y} = \mathbf{y}), \tag{3.7}$$

then $u \leftrightarrows z \Rightarrow pBPA \vdash \mathbf{u} = \mathbf{z}$.

Proof. Let us assume that $\mathbf{u} \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$ or $\mathbf{z} \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$ and that (3.7) holds.

Case $\mathbf{u} \in \mathcal{B}_+(pBPA)$ *and* $\mathbf{z} \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$. From Corollary 3.3.53 we have that

$$\mathbf{z} \equiv \mathbf{z'_1} \between_{\sigma_1} \mathbf{z'_2} \between_{\sigma_2} \mathbf{z'_3} \dots \between_{\sigma_{n-1}} \mathbf{z'_n}$$

for some $n \geq 2$, $\sigma_i \in \langle 0, 1 \rangle$ and $\mathbf{z'_i} \in \mathcal{B}_+(pBPA)$. From Lemma 3.3.56 it follows that for each $i,\ 1 \leq i \leq n,\ z'_i \leftrightarrows u$. And from the Congruence theorem $z'_i + u \leftrightarrows u$ and $u + z'_i \leftrightarrows z'_i$. Now, $op(z'_i) + op(u) < op(z) + op(u)$ and from (3.7) it follows that $pBPA \vdash \mathbf{z'_i} = \mathbf{u}$ for any $i, 1 \geq i \geq n$. Thus, $pBPA \vdash \mathbf{z} = \mathbf{z'_1} \between_{\sigma_1} \mathbf{z'_2} \between_{\sigma_2} \mathbf{z'_3} \dots \between_{\sigma_{n-1}} \mathbf{z'_n} = \mathbf{u} \between_{\sigma_1} \mathbf{u} \between_{\sigma_2} \mathbf{u} \dots \between_{\sigma_{n-1}} \mathbf{u} = \mathbf{u}$;

Case if $\mathbf{z} \in \mathcal{B}_+(pBPA)$ *and* $\mathbf{u} \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$. This can be proved in a similar way as the first case;

Case $u, z \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$. We proceed by induction on the number of probabilistic choices occurring in u and z

`Basis` $\mathbf{u} \equiv \mathbf{v} \between_\rho \mathbf{w}$ and $\mathbf{z} \equiv \mathbf{x} \between_\pi \mathbf{y}$, for $\mathbf{v}, \mathbf{w}, \mathbf{x}, \mathbf{y} \in \mathcal{B}_+(pBPA)$. Let us note that it must be the case that either $v \leftrightarrows x$ or $v \leftrightarrows y$. Without loss of generality we assume that $v \leftrightarrows x$.

Case $\rho = \pi$. Since $v \leftarrow\!\!\!\!\!\!\sqcup_\pi w \underline{\leftrightarrow} x \leftarrow\!\!\!\!\!\!\sqcup_\pi y$ and $v \underline{\leftrightarrow} x$ from Lemma 3.3.54 it follows that $y \underline{\leftrightarrow} w$. Because $op(v)+op(x) < op(u)+op(z)$, $v+x \underline{\leftrightarrow} x$ and $x+v \underline{\leftrightarrow} v$ from (3.7) follows that *pBPA* $\vdash \mathbf{x} = \mathbf{v}+\mathbf{x} = \mathbf{x}+\mathbf{v} = \mathbf{v}$. (1)
In a similar way we can derive that *pBPA* $\vdash \mathbf{y} = \mathbf{w}$ as well. Finally, we obtain *pBPA* $\vdash \mathbf{u} = \mathbf{z}$;

Case $\rho > \pi$. *pBPA* $\vdash \mathbf{u} = \mathbf{v} \leftarrow\!\!\!\!\!\!\sqcup_\pi (\mathbf{v} \leftarrow\!\!\!\!\!\!\sqcup_{\frac{\rho-\pi}{1-\rho}} \mathbf{w})$ and $v \leftarrow\!\!\!\!\!\!\sqcup_\pi (v \leftarrow\!\!\!\!\!\!\sqcup_{\frac{\rho-\pi}{1-\rho}} w) \underline{\leftrightarrow} x \leftarrow\!\!\!\!\!\!\sqcup_\pi y$. In a similar way as above, we can obtain that *pBPA* $\vdash \mathbf{x} = \mathbf{v}$ (since $x \underline{\leftrightarrow} v$). From Lemma 3.3.54 we obtain $v \leftarrow\!\!\!\!\!\!\sqcup_{\frac{\rho-\pi}{1-\rho}} w \underline{\leftrightarrow} y$. Now from Proposition 3.3.56 it follows that $v \underline{\leftrightarrow} y$ and $w \underline{\leftrightarrow} y$. Thus, in a similar way like in (1) we obtain *pBPA* $\vdash \mathbf{v} = \mathbf{y}$ and *pBPA* $\vdash \mathbf{w} = \mathbf{y}$. Now it is easy to derive that *pBPA* $\vdash \mathbf{u} = \mathbf{z}$.

`Inductive step` Consider arbitrary basic terms from $\mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$ $\mathbf{u}$ and $\mathbf{z}$. There are v and x such that $u \rightsquigarrow v$, $z \rightsquigarrow x$ and $x \underline{\leftrightarrow} v$. Let $K = [v]_{\underline{\leftrightarrow}} = [x]_{\underline{\leftrightarrow}}$. From Corollary 3.3.53 we obtain that:

$$\begin{array}{lll} \mathbf{Cu_1} & \mathbf{u} \equiv \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_1} \mathbf{u'_2} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_2} \mathbf{u'_3} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\rho_{m-1}} \mathbf{u'_m} & m \geq 2 \quad \text{or} \\ \mathbf{Cu_2} & \mathbf{u} \equiv \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_1} \mathbf{u'_2} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_2} \mathbf{u'_3} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\rho_{m-1}} \mathbf{u'_m} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_m} \mathbf{w}, & m \geq 1 \end{array}$$

for $m \in \mathbb{N}$, $\rho_i \in \langle 0,1\rangle$, $u'_i \in K$, $1 \leq i \leq m$ and for a basic term $\mathbf{w} \equiv \mathbf{w_1} \leftarrow\!\!\!\!\!\!\sqcup_{\alpha_1} \mathbf{w_2} \leftarrow\!\!\!\!\!\!\sqcup_{\alpha_2} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\alpha_{r-1}} \mathbf{w_r}$, where $r \in \mathbb{N}, r \geq 1$, $\alpha_l \in \langle 0,1\rangle$, $\mathbf{w_l} \in \mathcal{B}_+(pBPA)$ and $w_l \notin K$ for $1 \leq l \leq r$
and

$$\begin{array}{lll} \mathbf{Cz_1} & \mathbf{z} \equiv \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_1} \mathbf{z'_2} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_2} \mathbf{z'_3} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_{n-1}} \mathbf{z'_n}, & n \geq 2 \quad \text{or} \\ \mathbf{Cz_2} & \mathbf{z} \equiv \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_1} \mathbf{z'_2} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_2} \mathbf{z'_3} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_{n-1}} \mathbf{z'_n} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_n} \mathbf{y}, & n \geq 1 \end{array}$$

for $n \in \mathbb{N}$, $\sigma_j \in \langle 0,1\rangle$, $z'_j \in K$ $j, 1 \leq j \leq n$ and for some basic term $\mathbf{y} \equiv \mathbf{y_1} \leftarrow\!\!\!\!\!\!\sqcup_{\beta_1} \mathbf{y_2} \leftarrow\!\!\!\!\!\!\sqcup_{\beta_2} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\beta_{s-1}} \mathbf{y_s}$, where $s \in \mathbb{N}, s \geq 1$, $\beta_k \in \langle 0,1\rangle$, $\mathbf{y_k} \in \mathcal{B}_+(pBPA)$ and $w_k \notin K$ for $1 \leq k \leq s$. Thus, $u'_i \underline{\leftrightarrow} z'_j$ and $u'_i + z'_j \underline{\leftrightarrow} z'_j$ and $u'_i + z'_j \underline{\leftrightarrow} u'_i$.
In the case of $\mathbf{Cu_1}$ and $\mathbf{Cz_1}$ since $op(u'_i)+op(z'_j) < op(u)+op(z)$ we obtain that *pBPA* $\vdash \mathbf{u'_i} + \mathbf{z'_j} = \mathbf{z'_j}$ and *pBPA* $\vdash \mathbf{u'_i} + \mathbf{z'_j} = \mathbf{u'_i}$. Therefore, *pBPA* $\vdash \mathbf{u'_i} = \mathbf{z'_j}$ for every i, j, $1 \leq i \leq n$, $1 \leq j \leq m$. Then we easily derive:

$$pBPA \vdash \mathbf{z} \equiv \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_1} \mathbf{z'_2} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_2} \mathbf{z'_3} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_{n-1}} \mathbf{z'_n} = \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_1} \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_2} \mathbf{u'_1} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_{n-1}} \mathbf{u'_1} = \mathbf{u'_1}$$

and also

$$pBPA \vdash \mathbf{u} \equiv \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_1} \mathbf{u'_2} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_2} \mathbf{z'_3} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\rho_{m-1}} \mathbf{u'_m} = \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_1} \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_2} \mathbf{z'_1} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\rho_{m-1}} \mathbf{z'_1} = \mathbf{z'_1}.$$

Hence, *pBPA* $\vdash \mathbf{z} = \mathbf{u}$.
In the case of $\mathbf{Cu_2}$ and $\mathbf{Cz_2}$ we also have that *pBPA* $\vdash \mathbf{u'_i} = \mathbf{z'_j}$ for every i, j, $1 \leq i \leq m$ and $1 \leq j \leq n$. Then

$$\begin{array}{rcl} pBPA \vdash \mathbf{u} & \equiv & \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_1} \mathbf{u'_2} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_2} \mathbf{u'_3} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\rho_{m-1}} \mathbf{u'_m} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_m} \mathbf{w} \\ & = & \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_1} \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_2} \mathbf{u'_1} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\rho_{m-1}} \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\rho_m} \mathbf{w} \\ & = & \mathbf{u'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sum_{j=1}^{m} \rho_j} \mathbf{w} \end{array}$$

and

$$\begin{array}{rcl} pBPA \vdash \mathbf{z} & \equiv & \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_1} \mathbf{z'_2} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_2} \mathbf{z'_3} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_{n-1}} \mathbf{z'_n} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_n} \mathbf{y} \\ & = & \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_1} \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_2} \mathbf{z'_1} \ldots \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_{n-1}} \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sigma_n} \mathbf{y} \\ & = & \mathbf{z'_1} \leftarrow\!\!\!\!\!\!\sqcup_{\sum_{i=1}^{n} \sigma_i} \mathbf{y} \end{array}$$

Using the Soundness theorem we have: $u \leftrightarrow u'_1 \leftplus_{\sum_{i=1}^{m}\rho_i} w$ and $z \leftrightarrow z'_1 \leftplus_{\sum_{j=1}^{n}\sigma_j} y$. From the assumption $z \leftrightarrow u$ it follows that $u'_1 \leftplus_{\sum_{i=1}^{m}\rho_i} w \leftrightarrow u \leftrightarrow z \leftrightarrow z'_1 \leftplus_{\sum_{j=1}^{n}\sigma_j} y$. Moreover, $\mu(y, K) = 0 = \mu(w, K)$. Thus, $\mu(u'_1 \leftplus_{\sum_{i=1}^{m}\rho_i} w, K) = \sum_{i=1}^{m}\rho_i$ and $\mu(z'_1 \leftplus_{\sum_{j=1}^{n}\sigma_j} y, K) = \sum_{j=1}^{n}\sigma_j$ and from the definition of bisimulation: $\sum_{i=1}^{m}\rho_i = \sum_{j=1}^{n}\sigma_j$. (Actually, this is the probability by which z and u reaches the equivalence class K.) Let us denote this sum by α. So, we have that $u'_1 \leftplus_\alpha w \leftrightarrow z'_1 \leftplus_\alpha y$ and $u'_1 \leftrightarrow z'_1$. By Theorem 3.3.36 we obtain $u'_1 \leftplus_\alpha w \leftrightarrow u'_1 \leftplus_\alpha y$. Using Lemma 3.3.54 we have $w \leftrightarrow y$. Finally, since $y \leftrightarrow w$ and $\mathbf{w}$ and $\mathbf{y}$ have less probabilistic choice operators than $\mathbf{z}$ and $\mathbf{u}$, respectively, from the inductive hypothesis it follows that *pBPA* $\vdash \mathbf{y} = \mathbf{w}$. Having that *pBPA* $\vdash \mathbf{z'_1} = \mathbf{u'_1}$ we conclude *pBPA* $\vdash \mathbf{z} = \mathbf{u}$.

□

Lemma 3.3.59. If $\mathbf{x}$ and $\mathbf{y}$ are basic $\mathcal{B}_+(pBPA)$ terms then:

$$x + y \leftrightarrow y \Rightarrow pBPA \vdash \mathbf{x} + \mathbf{y} = \mathbf{y}.$$

Proof. The lemma is proved by induction on $op(\mathbf{x}) + op(\mathbf{y})$ and case distinction on the structure of $\mathbf{x}$.

Case $\mathbf{x} \equiv \boldsymbol{\delta}$. The result follows from axiom A6;

Case $\mathbf{x} \equiv \mathbf{a}, a \in A$. $\breve{x} \xrightarrow{a} \surd$ and also $\breve{x} + \breve{y} \xrightarrow{a} \surd$. By assumption $x + y \leftrightarrow y$ we have that $\breve{y} \xrightarrow{a} \surd$. Then by Proposition 3.3.55*i.* we have that *pBPA* $\vdash \mathbf{y} = \mathbf{a} + \mathbf{y}$ and also *pBPA* $\vdash \mathbf{x} + \mathbf{y} = \mathbf{a} + \mathbf{y} = \mathbf{y}$;

Case $\mathbf{x} \equiv \boldsymbol{\delta} \cdot \mathbf{t}$. By *pBPA* $\vdash \mathbf{x} + \mathbf{y} = \boldsymbol{\delta} \cdot \mathbf{t} + \mathbf{y} = \boldsymbol{\delta} + \mathbf{y} = \mathbf{y}$;

Case $\mathbf{x} \equiv \mathbf{a} \cdot \mathbf{t}$. Then $a \cdot t + y \leftrightarrow y$. Since $\breve{a} \cdot t \xrightarrow{a} t$ we obtain that $\breve{y} \xrightarrow{a} s$ and $t \leftrightarrow s$. (5)
Since $\mathbf{t}$ and $\mathbf{s}$ are basic terms with $op(\mathbf{t}) < op(\mathbf{x})$ and $op(\mathbf{s}) < op(\mathbf{y})$ we consider the following cases:

Subcase $\mathbf{t}, \mathbf{s} \in \mathcal{B}_+(pBPA)$. Then $op(\mathbf{t} + \mathbf{s}) < op(\mathbf{x} + \mathbf{y})$ and from (5) we obtain $t + s \leftrightarrow s$ and $t + s \leftrightarrow t$. By the inductive hypothesis *pBPA* $\vdash \mathbf{t} + \mathbf{s} = \mathbf{s}$ and *pBPA* $\vdash \mathbf{t} + \mathbf{s} = \mathbf{t}$ and also *pBPA* $\vdash \mathbf{t} = \mathbf{s}$; (6.1)

Subcase $\mathbf{t} \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$ *or* $\mathbf{s} \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$. Then we want to apply Lemma 3.3.58 on (5). To do so we need to show that the hypothesis of the lemma is fulfilled. Thus, if $\mathbf{u}$ and $\mathbf{z}$ are basic $\mathcal{B}_+(pBPA)$ terms such that $op(\mathbf{u}) + op(\mathbf{z}) < op(\mathbf{t}) + op(\mathbf{s})$, then $op(\mathbf{u}) + op(\mathbf{z}) < op(\mathbf{x}) + op(\mathbf{y})$ since $op(\mathbf{t}) < op(\mathbf{x})$ and $op(\mathbf{s}) < op(\mathbf{y})$. Then from the inductive hypothesis we obtain that the hypothesis in Lemma 3.3.58 is satisfied. Therefore, the result of the lemma can be applied on (5). Thus, we obtain *pBPA* $\vdash \mathbf{t} = \mathbf{s}$. (6.2)

In both cases, (6.1) and (6.2), we have *pBPA* $\vdash \mathbf{x} + \mathbf{y} = \mathbf{a} \cdot \mathbf{t} + \mathbf{y} = \mathbf{a} \cdot \mathbf{s} + \mathbf{y} = \mathbf{y}$;

Case $\mathbf{x} \equiv \mathbf{x_1} + \mathbf{x_2}$. from the assumption $x_1 + x_2 + y \leftrightarrow y$ using Proposition 3.3.57 we obtain $x_1 + y \leftrightarrow y$ and $x_2 + y \leftrightarrow y$. Then by the inductive hypothesis *pBPA* $\vdash \mathbf{x_1} + \mathbf{y} = \mathbf{y}$ and *pBPA* $\vdash \mathbf{x_2} + \mathbf{y} = \mathbf{y}$. Hence, *pBPA* $\vdash \mathbf{x} + \mathbf{y} = \mathbf{x_1} + \mathbf{x_2} + \mathbf{y} = \mathbf{x_1} + \mathbf{x_2} + \mathbf{y} + \mathbf{y} = \mathbf{y} + \mathbf{y} = \mathbf{y}$.

□

Theorem 3.3.60 (*Completeness theorem for pBPA*). If $\mathbf{z}$ and $\mathbf{u}$ are closed *pBPA* terms, then $z \leftrightarrow\!\!\!\!\!\!\underline{}\; u \Rightarrow$ *pBPA* $\vdash \mathbf{z} = \mathbf{u}$.

Proof. By the Elimination theorem and the Soundness theorem it is sufficient to prove that this result is valid for basic terms. Let us assume that $\mathbf{u}$ and $\mathbf{z}$ are basic *pBPA* terms and $z \leftrightarrow\!\!\!\!\!\!\underline{}\; u$.

Case $\mathbf{z}, \mathbf{u} \in \mathcal{B}_+(pBPA)$. From the assumption $z \leftrightarrow\!\!\!\!\!\!\underline{}\; u$ we derive that $z + u \leftrightarrow\!\!\!\!\!\!\underline{}\; z + z \leftrightarrow\!\!\!\!\!\!\underline{}\; z$ and $z + u \leftrightarrow\!\!\!\!\!\!\underline{}\; u + u \leftrightarrow\!\!\!\!\!\!\underline{}\; u$. By Lemma 3.3.59 we obtain *pBPA* $\vdash \mathbf{z} + \mathbf{u} = \mathbf{z}$ and *pBPA* $\vdash \mathbf{z} + \mathbf{u} = \mathbf{u}$. Therefore, *pBPA* $\vdash \mathbf{z} = \mathbf{u}$.

Case $\mathbf{u} \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$ *or* $\mathbf{z} \in \mathcal{B}(pBPA) \setminus \mathcal{B}_+(pBPA)$. From the previous case we have that $\forall \mathbf{x}, \mathbf{y} \in \mathcal{B}_+(pBPA) \;:\; x + y \leftrightarrow\!\!\!\!\!\!\underline{}\; y \Rightarrow$ *pBPA* $\vdash \mathbf{x} + \mathbf{y} = \mathbf{y}$. Since it is satisfied by all basic $\mathcal{B}_+(pBPA)$ terms, it is satisfied by all basic $\mathcal{B}_+(pBPA)$ terms $\mathbf{x}$ and $\mathbf{y}$ such that $op(\mathbf{x}) + op(\mathbf{y}) < op(\mathbf{z}) + op(\mathbf{u})$. Then, applying Lemma 3.3.58 on the assumption $z \leftrightarrow\!\!\!\!\!\!\underline{}\; u$ we obtain *pBPA* $\vdash \mathbf{z} = \mathbf{u}$.

□

Chapter 4

Parallel composition and communication

4.1 Introduction

In this section, we propose a variant of asynchronous probabilistic parallel composition which is defined algebraically by a set of axioms. Then, by adding it together with other auxiliary operators and the relevant axioms to the process algebra *pBPA* a probabilistic variant of *ACP*, denoted *pACP*$^+$, with asynchronous parallel composition is obtained.

With the intention to motivate the way parallel composition is defined let us look into the asynchronous parallel composition of standard *ACP*. In *ACP* (as well as in CCS) two parallel processes can perform any action independently, and also, they can synchronize if allowed (provided the communication between the two processes is defined). Thus, the parallel processes are not forced to synchronize (as opposed to the CSP parallel composition) but they can autonomously perform actions that could be synchronized. For example, if $x \equiv a + b$ and $y \equiv c + d$ merge and if a and c communicate into an e action, then one possible scenario is that x and y synchronize and e is performed, but x can also autonomously perform a which is then followed by y, or y can autonomously perform c followed by x. (There are other possible scenarios as result of merging x and y, four in total.) In other words, if x and y do not synchronize then each of them executes actions independently of the other one; x resolves the choice between a and b without any influence and independently of the choice between c and d in y. Algebraically this is expressed as $x \parallel y = e + a \lfloor\!\lfloor y + c \lfloor\!\lfloor x + \ldots$, where "$\ldots$" expresses that some other events can take place. Note that the choice between all possible sub-scenarios, e, $a \lfloor\!\lfloor y$ and $c \lfloor\!\lfloor x$, is non-deterministic. Once again we emphasize that the left merge operator was introduced in order to get a finite axiomatization of the merge operator.

Now, let us consider probabilistic processes $p \equiv a \leftthreetimes_{1/2} b$ and $q \equiv c \leftthreetimes_{1/3} d$ (in the probabilistic setting) and follow the same reasoning - *two processes either synchronize or perform actions autonomously*. Among four (see Figure 4.1), one possible scenario is that p performs a and q performs c. This scenario has probability $1/6$. We call it "a/c" scenario. Due to asynchronicity (the interleaving reasoning) besides synchronizing into a communication action $e(= a \mid c)$, each process can independently perform its own action, p performs a which is then followed by q or q performs c which is then followed by p. In fact, as soon as p has chosen to perform a, it may be executed regardless of whether or not q has resolved its probabilistic choice, so each of the actions c and d may be performed in accordance with the given probabilities. And the same holds for q, if it performs the first action. This means that the probabilistic choices are not expected to be resolved at the same time in both parallel processes.

Thus, in total there are three possible sub-scenarios enclosed into the "a/c" scenario and the choice which sub-scenario takes place is non-deterministic. The probability $1/6$ corresponds to the

probability that this scenario occurs, but the probability of a particular sub-scenario is *unknown*.

This way of combining probabilities and parallel composition with the interleaving reasoning is also considered in [49] where the authors use bundle probabilistic transition systems.

The chapter is organized as follows: first we introduce an extension of *pBPA* with probabilistic parallel composition as described above. Then we construct the bisimulation model of it obtaining only finite processes. Finally, we present another direction to extend *pBPA* with parallel composition and show that it does not capture our intuition about probabilistic parallel processes.

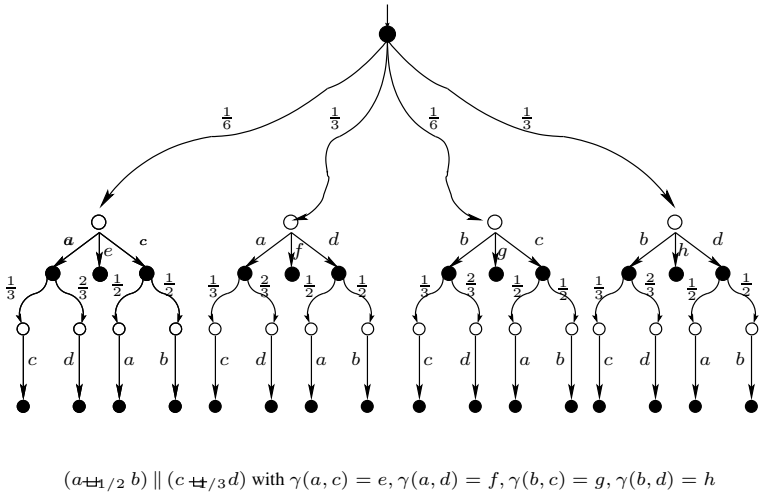


Figure 4.1: An example of parallel composition of probabilistic processes.

4.2 Probabilistic Process Algebra with parallel composition

Axiom system of *pACP*$^+$

Next we give an algebraic definition of the intuitively described parallel composition. First let us note that it can simply be axiomatized by the infinite set of conditional axioms shown in Table 4.1. The axioms show exactly what has been said in the introduction: if x_i is one possible outcome of the probabilistic choice of x which has probability π_i and y_j is the same for y with probability ρ_j, then "x_i/y_j" is one possible scenario of the parallel composition of x and y which has probability $\pi_i \cdot \rho_j$. This scenario consists of three alternatives, one of which is synchronization and the other two show asynchronous behaviour of the parallel composition $x \parallel y$ within the x_i/y_j scenario. Of course, here we assume that x_i and y_j do not have unresolved probabilistic choices. This assumption/requirement is expressed exactly by the condition of the axioms: $x_i = x_i + x_i$ and/or $y_j = y_j + y_j$. In other words, a term p satisfies the equation $p = p + p$ iff *pACP*$^+ \vdash p = p_b$ for a basic term $p_b \in \mathcal{B}_+$ (see also Lemma 4.3.17).

The next step is to give a finite axiomatization of the merge operator. For that purpose we introduce a new quaternary operator called "merge with memory" and denote it by $\between\!\!\between$. The finite set of axioms which define this operator and the merge operator as well is shown in Table 4.2.

The axiom $PrMM1$ expresses the relation between the merge operator and the new merge with memory operator. Namely, to expand the expression $x \parallel y$ in the first step it is necessary to "copy" and "memorize" the initial terms x and y. They will be needed in later steps of the derivation

for $n \geq 2, m \geq 2, x \equiv x_1 \leftplus_{\pi_1} x_2 \ldots \leftplus_{\pi_{n-1}} x_n, y \equiv y_1 \leftplus_{\rho_1} y_2 \ldots \leftplus_{\rho_{m-1}} y_m$
$x_i = x_i + x_i, y_j = y_j + y_j \Rightarrow \quad x \parallel y = \leftplus_{\pi_i \cdot \rho_j, 1 \leq i \leq n, 1 \leq j \leq m} (x_i \lfloor\!\lfloor y + y_j \lfloor\!\lfloor x + x_i \mid y_j)$

for $n \geq 2, x \equiv x_1 \leftplus_{\pi_1} x_2 \ldots \leftplus_{\pi_{n-1}} x_n$
$x_i = x_i + x_i, y = y + y \Rightarrow \quad x \parallel y = \leftplus_{\pi_i, 1 \leq i \leq n} (x_i \lfloor\!\lfloor y + y \lfloor\!\lfloor x + x_i \mid y)$

for $m \geq 2, y \equiv y_1 \leftplus_{\rho_1} y_2 \ldots \leftplus_{\rho_{m-1}} y_m$
$x = x + x, y_j = y_j + y_j \Rightarrow \quad x \parallel y = \leftplus_{\rho_j, 1 \leq j \leq m} (x \lfloor\!\lfloor y + y_j \lfloor\!\lfloor x + x \mid y_j)$

$x = x + x, y = y + y \Rightarrow \quad x \parallel y = x \lfloor\!\lfloor y + y \lfloor\!\lfloor x + x \mid y$

Table 4.1: Parallel composition defined by infinite set of axioms.

$$
\begin{array}{lcll}
x \parallel y & = & (x, x) \llbracket (y, y) & PrMM1 \\
(x \leftplus_\pi x', z) \llbracket (y, w) & = & (x, z) \llbracket (y, w) \leftplus_\pi (x', z) \llbracket (y, w) & PrMM2 \\
(x, z) \llbracket (y \leftplus_\pi y', w) & = & (x, z) \llbracket (y, w) \leftplus_\pi (x, z) \llbracket (y', w) & PrMM3 \\
\end{array}
$$

$$x = x + x, y = y + y \Rightarrow (x, z) \llbracket (y, w) = x \lfloor\!\lfloor w + y \lfloor\!\lfloor z + x \mid y \qquad PrMM4$$

Table 4.2: Axioms for the merge with memory operator.

when $PrMM4$ will be applied (see also the explanation below). If x (y) does still have an unresolved probabilistic choice, then before interleaving takes place it has to be resolved. The axiom $PrMM2$ ($PrMM3$) shows exactly the way this probabilistic choice is resolved. It expresses that the probability distribution (probabilistic choice) over sub-terms of x (y) induces a probability distribution over the set of all possible scenarios of the parallel composition $x \parallel y$. The axiom $PrMM4$ shows the "x/y" scenario of the parallel composition $z \parallel w$, under assumption that z and w are the initial parallel processes. (Note that the last axiom in Table 4.1 resembles this one.)

If we go back to the axioms in Table 4.1, we notice that x and y appear in the right-hand side of the axioms and x and y are exactly the terms which have started the parallel composition. Here, in the finite axiomatization, we also need to keep track of these terms as we have mentioned above, so they will be "recalled" when the interleaving of x and y takes place. For that reason the *merge with memory operator* has two arguments more, the second z and the fourth w argument used to store the initial parallel terms. (In the last axiom in Table 4.1 z is exactly x and w is y and in any of these axioms the initial terms are given explicitly.) Thus, these arguments stay unchanged during the derivation/transformation until the last step, in which $PrMM4$ is applied.

Let us summarize the definition of the probabilistic version of *ACP* called Algebra of Communicating Processes with probabilistic choice *pACP*$^+$, where $+$ stands for the extra merge operator added to this algebra. *pACP*$^+$ is parametrized by a set of atomic actions A and a communication function $\gamma : A_\delta \times A_\delta \to A_\delta$ which indicates atomic actions that communicate. This function is assumed to be commutative and associative, and satisfies the equation $\gamma(\delta, a) = \delta$ for all $a \in A_\delta$. It has a signature

consisting of a set of constants A and the constant δ and the operators of ***pBPA***, three binary operators: $\|$ (merge, parallel composition), $\lfloor\!\lfloor$ and $|$ (communication merge), a unary operator ∂_H with $H \subseteq A$ (encapsulation operator) and a quaternary operator $\rrbracket$ (merge with memory operator). The set of axioms consists of the axioms of ***pBPA*** in Table 3.1, 3.2 and 3.3 as well as the axioms given in Table 4.2 and 4.3 together with the conditional axioms given in Table 4.4.

The new axioms that do not appear in the axiomatization of ***ACP*** are: $PrCM1-5$ and $PrD5$. $PrCM1$ expresses that the left-merge operator left-distributes over probabilistic choice operator. $PrCM2$ and $PrCM3$ express that the communication merge distributes (left and right) over probabilistic choice operator. And the encapsulation operator also distributes over the probabilistic choice operator as axiom $PrD5$ shows.

$a \mid b$	=	$\gamma(a,b)$		CF
$a \lfloor\!\lfloor x$	=	$a \cdot x$		$CM2$
$a \cdot x \lfloor\!\lfloor y$	=	$a \cdot (x \parallel y)$		$CM3$
$(x+y) \lfloor\!\lfloor z$	=	$x \lfloor\!\lfloor z + y \lfloor\!\lfloor z$		$CM4$
$(x \leftthreetimes_\pi y) \lfloor\!\lfloor z$	=	$x \lfloor\!\lfloor z \leftthreetimes_\pi y \lfloor\!\lfloor z$		$PrCM1$
$a \mid b \cdot x$	=	$(a \mid b) \cdot x$		$CM5$
$a \cdot x \mid b$	=	$(a \mid b) \cdot x$		$CM6$
$a \cdot x \mid b \cdot y$	=	$(a \mid b) \cdot (x \parallel y)$		$CM7$
$(x \leftthreetimes_\pi y) \mid z$	=	$x \mid z \leftthreetimes_\pi y \mid z$		$PrCM2$
$x \mid (y \leftthreetimes_\pi z)$	=	$x \mid y \leftthreetimes_\pi x \mid z$		$PrCM3$
$\partial_H(a)$	=	a	if $a \notin H$	$D1$
$\partial_H(a)$	=	δ	if $a \in H$	$D2$
$\partial_H(x+y)$	=	$\partial_H(x) + \partial_H(y)$		$D3$
$\partial_H(x \cdot y)$	=	$\partial_H(x) \cdot \partial_H(y)$		$D4$
$\partial_H(x \leftthreetimes_\pi y)$	=	$\partial_H(x) \leftthreetimes_\pi \partial_H(y)$		$PrD5$

Table 4.3: Additional axioms for ***pACP***$^+$.

$z = z + z \Rightarrow (x+y) \mid z = x \mid z + y \mid z$	$PrCM4$
$z = z + z \Rightarrow z \mid (x+y) = z \mid x + z \mid y$	$PrCM5$

Table 4.4: Communication merge in ***pACP***$^+$.

Certainly, an interesting detail is the constrained version $PrCM4$ and $PrCM5$ of the ***ACP*** axioms $CM8$ and $CM9$, respectively. Again, the constraint has the form $p = p + p$ which means (as mentioned before) that the right-side equation of the conditional axiom can be applied only if the right arguments of the communication merge is a $\mathcal{D}(\textbf{\textit{pACP}}^+)$ term in the case of $PrCM4$ axiom. And similar for $PrCM5$ axiom. The process denoted by this term can perform only a trivial probabilistic transition. Let us support the need of this condition by the following example.

Example 4.2.1. Consider the two terms $(a+b) \mid (c \leftthreetimes_\pi d)$ and $a \mid (c \leftthreetimes_\pi d) + b \mid (c \leftthreetimes_\pi d)$.
The process represented by the first terms does the following: it chooses between c and d according to the given probabilities and then, the chosen action communicates with a or b. The latter choice is non-deterministic due to non-determinism between a and b. Actually, we can derive the following equations in *pACP*$^+$:

$(a+b) \mid (c \leftthreetimes_\pi d) = ((a+b) \mid c) \leftthreetimes_\pi ((a+b) \mid d) = (a \mid c + b \mid c) \leftthreetimes_\pi (a \mid d + b \mid d)$.

The second term $a \mid (c \leftthreetimes_\pi d) + b \mid (c \leftthreetimes_\pi d)$ contains two probabilistic choices. Thus, the process represented by this term first resolves the probabilistic choices (which are identical in this case but of course it does not mean the outcomes will be the same). Then, the outcome of the first choice communicates with a and the outcome of the second choice communicates with b. Each summand in the alternative composition offers two (probabilistic) options: $a \mid c$ and $a \mid d$ for the first one, and $b \mid c$ and $b \mid d$ for the second one.

The following equalities are provable in *pACP*$^+$:

$a \mid (c \leftthreetimes_\pi d) + b \mid (c \leftthreetimes_\pi d) = (a \mid c \leftthreetimes_\pi a \mid d) + (b \mid c \leftthreetimes_\pi b \mid d) =$
$(a \mid c + b \mid c) \leftthreetimes_{\pi^2} (a \mid d + b \mid c) \leftthreetimes_{\pi(1-\pi)} (a \mid c + b \mid d) \leftthreetimes_{\pi(1-\pi)} (a \mid d + b \mid d)$.

It is easy to conclude that these terms if interpreted in the model of *pBPA* represent two different process terms. The second one has $(a \mid d + b \mid c)$ as a sub-term with a positive assigned probability which is not the case with the first term. But, if we would have unrestricted distribution laws instead of $PrCM4$ and $PrCM5$ these terms would become equal. □

Example 4.2.2. Assuming that $\gamma(a,c) = e$, $\gamma(a,d) = f$, $\gamma(b,c) = g$ and $\gamma(b,d) = h$, the algebraic expansion in *pACP*$^+$ of the term $(a \leftthreetimes_{1/2} b) \parallel (c \leftthreetimes_{1/3} d)$ can be done in the following way:

$$
\begin{aligned}
& (a \leftthreetimes_{1/2} b) \parallel (c \leftthreetimes_{1/3} d) \\
\overset{PrMM1}{=}\ & (a \leftthreetimes_{1/2} b,\ a \leftthreetimes_{1/2} b) \between (c \leftthreetimes_{1/3} d,\ c \leftthreetimes_{1/3} d) \\
\overset{PrMM2}{=}\ & ((a,\ a \leftthreetimes_{1/2} b) \between (c \leftthreetimes_{1/3} d,\ c \leftthreetimes_{1/3} d)) \leftthreetimes_{1/2} ((b,\ a \leftthreetimes_{1/2} b) \between (c \leftthreetimes_{1/3} d,\ c \leftthreetimes_{1/3} d)) \\
\overset{2\times PrMM3}{=}\ & \big(((a,\ a \leftthreetimes_{1/2} b) \between (c,\ c \leftthreetimes_{1/3} d)) \leftthreetimes_{1/3} ((a,\ a \leftthreetimes_{1/2} b) \between (d,\ c \leftthreetimes_{1/3} d))\big) \leftthreetimes_{1/2} \\
& \quad \big(((b,\ a \leftthreetimes_{1/2} b) \between (c,\ c \leftthreetimes_{1/3} d)) \leftthreetimes_{1/3} ((b,\ a \leftthreetimes_{1/2} b) \between (d,\ c \leftthreetimes_{1/3} d))\big) \\
=\ & ((a,\ a \leftthreetimes_{1/2} b) \between (c,\ c \leftthreetimes_{1/3} d)) \leftthreetimes_{1/6} ((a,\ a \leftthreetimes_{1/2} b) \between (d,\ c \leftthreetimes_{1/3} d)) \leftthreetimes_{1/3} \\
& \quad ((b,\ a \leftthreetimes_{1/2} b) \between (c,\ c \leftthreetimes_{1/3} d)) \leftthreetimes_{1/6} ((b,\ a \leftthreetimes_{1/2} b) \between (d,\ c \leftthreetimes_{1/3} d)) \\
\overset{4\times PrMM4}{=}\ & \big(a \lfloor\!\lfloor (c \leftthreetimes_{1/3} d) + c \lfloor\!\lfloor (a \leftthreetimes_{1/2} b) + (a \mid c)\big) \leftthreetimes_{1/6} \\
& \quad \big(a \lfloor\!\lfloor (c \leftthreetimes_{1/3} d) + d \lfloor\!\lfloor (a \leftthreetimes_{1/2} b) + (a \mid d)\big) \leftthreetimes_{1/3} \\
& \quad \big(b \lfloor\!\lfloor (c \leftthreetimes_{1/3} d) + c \lfloor\!\lfloor (a \leftthreetimes_{1/2} b) + (b \mid c)\big) \leftthreetimes_{1/6} \\
& \quad \big(b \lfloor\!\lfloor (c \leftthreetimes_{1/3} d) + d \lfloor\!\lfloor (a \leftthreetimes_{1/2} b) + (b \mid d)\big) \\
=\ & \big(a \cdot (c \leftthreetimes_{1/3} d) + c \cdot (a \leftthreetimes_{1/2} b) + e\big) \leftthreetimes_{1/6} \big(a \cdot (c \leftthreetimes_{1/3} d) + d \cdot (a \leftthreetimes_{1/2} b) + f\big) \leftthreetimes_{1/3} \\
& \quad \big(b \cdot (c \leftthreetimes_{1/3} d) + c \cdot (a \leftthreetimes_{1/2} b) + g\big) \leftthreetimes_{1/6} \big(b \cdot (c \leftthreetimes_{1/3} d) + d \cdot (a \leftthreetimes_{1/2} b) + h\big).
\end{aligned}
$$

□

Even though axiom $CM1$ in Table 2.4 is omitted in this axiomatization we are still able in *pACP*$^+$ to derive all equations provable in *ACP*. One can observe that axioms $PrMM2$ and $PrMM3$ can never be applied on an *ACP* term taken as a *pACP*$^+$ term. Furthermore, the condition of axiom $PrMM4$ is fulfilled for all such terms. Thus, for every two terms u and v from the subset of *pACP*$^+$ terms that form the set of *ACP* terms we easily derive: $u \parallel v = (u,u) \between (v,v) = u \lfloor\!\lfloor v + v \lfloor\!\lfloor u + u \mid v$ from which we obtain $u \parallel v = u \lfloor\!\lfloor v + v \lfloor\!\lfloor u + u \mid v$. And this is exactly the $CM1$ axiom. Even more, for these terms axioms $PrCM4$ and $PrCM5$ become exactly axioms $CM8$ and $CM9$ respectively. Finally, if we omit all axioms in Table 4.3 that regard the probabilistic choice operator we end up with the axiom system of *ACP*. Moreover, the removed axioms can never be applied to *ACP* terms since they do not contain a probabilistic choice. So, we can conclude that every equation provable in *ACP*

is provable in *pACP*$^+$ as well and no new equalities between *ACP* terms can be proved in *pACP*$^+$. Consequently, *pACP*$^+$ is an *equational conservative extension* of *ACP*.

The set of basic terms of *pACP*$^+$ is defined in the same way as the set of the basic terms in *pBPA* (Definition 3.2.19). In order to show completeness of *pACP*$^+$ for the bisimulation model defined in the next section, first we need to prove that the operators added in the signature of *pACP*$^+$ can be eliminated in favour of the basic operators of *pBPA*. Namely, for every closed term in *pACP*$^+$ there is a basic term in *pBPA* that can be proved equal using the axioms. From now on by $\mathcal{SP}(pACP^+)$ we denote the set of all closed terms over the signature Σ_{pACP^+}.

Lemma 4.2.3. Let p and q be basic terms. Then there are closed *pBPA* terms r, s, t and u such that *pACP*$^+ \vdash p \between q = r$, *pACP*$^+ \vdash p \mid q = s$, *pACP*$^+ \vdash p \parallel q = t$ and *pACP*$^+ \vdash \partial_H(p) = u$ for some $H \subseteq A$. (Note: for the $\between$ operator see Lemma 4.2.4.)

Proof. The proof is given by double induction on the structure on p and q proving all four statements in parallel. First we treat cases when p and q are basic $\mathcal{B}_+$ terms. The nonessential symmetric cases of the given ones are not considered; the result about the $\between$ operator depends only on the left argument; the result about the $\parallel$ and $\mid$ does not depend on the order of the arguments. The part for the encapsulation operator is given by induction on the structure of p only.

Case $p \equiv a, a \in A_\delta$ *and* $q \equiv b \in A_\delta$. *pACP*$^+ \vdash p \between q = a \cdot b$; *pACP*$^+ \vdash p \mid q = \gamma(a,b)$ and *pACP*$^+ \vdash p \parallel q = a \cdot b + b \cdot a + \gamma(a,b)$. All three obtained term on the right-hand sides are closed *pBPA* terms. Moreover, if $a \notin H$ then *pACP*$^+ \vdash \partial_H(p) = a$, otherwise *pACP*$^+ \vdash \partial_H(p) = \delta$. In both cases a closed *pBPA* term is obtained;

Case $p \equiv a, a \in A_\delta$ *and* $q \equiv b \cdot q_1$. *pACP*$^+ \vdash p \between q = a \cdot b \cdot q_1$ which is a closed *pBPA* term; *pACP*$^+ \vdash p \mid q = \gamma(a,b) \cdot q_1$ which is a closed *pBPA* term; *pACP*$^+ \vdash p \parallel q = a \cdot b \cdot q_1 + b \cdot (a \parallel q_1) + \gamma(a,b) \cdot q_1$. Then by the inductive hypothesis there is a closed *pBPA* term t_1 such that *pACP*$^+ \vdash a \parallel q_1 = t_1$. Thus, *pACP*$^+ \vdash p \parallel q = a \cdot b \cdot q_1 + b \cdot t_1 + \gamma(a,b) \cdot q_1$ which is a closed *pBPA* term;

Case $p \equiv a \cdot p_1, a \in A_\delta$ *and* $q \equiv b \cdot q_1$. *pACP*$^+ \vdash p \between q = a \cdot (p_1 \parallel b \cdot q_1)$. By the inductive hypothesis there is a closed *pBPA* term r_1 such that *pACP*$^+ \vdash p_1 \parallel b \cdot q_1 = r_1$. Therefore, *pACP*$^+ \vdash p \between q = a \cdot r_1$ and $a \cdot r_1$ is a closed *pBPA* term;

pACP$^+ \vdash p \mid q = \gamma(a,b) \cdot (p_1 \parallel q_1)$. By the inductive hypothesis there is a closed *pBPA* term s_1 such that *pACP*$^+ \vdash p_1 \parallel q_1 = s_1$. Therefore, *pACP*$^+ \vdash p \mid q = \gamma(a,b) \cdot s_1$ and it is a closed *pBPA* term;

pACP$^+ \vdash p \parallel q = a \cdot (p_1 \parallel b \cdot q_1) + b \cdot (a \cdot p_1 \parallel q_1) + \gamma(a,b) \cdot (p_1 \parallel q_1)$. By the inductive hypothesis there are closed *pBPA* terms t_1, t_2 and t_3 such that *pACP*$^+ \vdash p_1 \parallel b \cdot q_1 = t_1$, *pACP*$^+ \vdash a \cdot p_1 \parallel q_1 = t_2$ and *pACP*$^+ \vdash p_1 \parallel q_1 = t_3$. Then *pACP*$^+ \vdash p \parallel q = a \cdot t_1 + b \cdot t_2 + \gamma(a,b) \cdot t_3$ and we obtain a closed *pBPA* term;

pACP$^+ \vdash \partial_H(p) = \delta \cdot \partial_H(p_1) = \delta$ if $a \in H$. Otherwise, *pACP*$^+ \vdash \partial_H(p) = a \cdot \partial_H(p_1)$. By the inductive hypothesis there is a closed *pBPA* term u_1 such that *pACP*$^+ \vdash \partial(p_1) = u_1$. Then, *pACP*$^+ \vdash \partial_H(p) = a \cdot u_1$ which is a closed *pBPA* term;

Case $p \equiv a, a \in A_\delta$ *and* $q \equiv q_1 + q_2$. *pACP*$^+ \vdash p \between q = a \cdot q$ which is a closed *pBPA* term;

pACP$^+ \vdash p \mid q = (a \mid q_1) + (a \mid q_2)$. By the inductive hypothesis there are closed *pBPA* terms s_1 and s_2 such that *pACP*$^+ \vdash a \mid q_1 = s_1$ and *pACP*$^+ \vdash a \mid q_2 = s_2$. Then *pACP*$^+ \vdash p \mid q = s_1 + s_2$ which is a closed *pBPA* term;

pACP$^+ \vdash p \parallel q = a \cdot q + q_1 \mathbin{\lfloor\!\lfloor} a + q_2 \mathbin{\lfloor\!\lfloor} a + a \mid q_1 + a \mid q_2$. By the inductive hypothesis there are closed *pBPA* terms t_1, t_2, t_3 and t_4 such that *pACP*$^+ \vdash q_1 \mathbin{\lfloor\!\lfloor} a = t_1$, *pACP*$^+ \vdash q_2 \mathbin{\lfloor\!\lfloor} a = t_2$, *pACP*$^+ \vdash a \mid q_1 = t_3$ and *pACP*$^+ \vdash a \mid q_2 = t_4$. Then *pACP*$^+ \vdash p \parallel q = a \cdot q + t_1 + t_2 + t_3 + t_4$ which is a closed *pBPA* term;

Case $p \equiv a \cdot p_1, a \in A_\delta$ *and* $q \equiv q_1 + q_2$. *pACP*$^+ \vdash p \mathbin{\lfloor\!\lfloor} q = a \cdot (p_1 \parallel q)$. By the inductive hypothesis there is a closed *pBPA* term r_1 such that *pACP*$^+ \vdash p_1 \parallel q = r_1$. Hence, *pACP*$^+ \vdash p \mathbin{\lfloor\!\lfloor} q = a \cdot r_1$ which is a closed *pBPA* term;

pACP$^+ \vdash p \mid q = (a \cdot p_1 \mid q_1) + (a \cdot p_1 \mid q_2)$. By the inductive hypothesis there are closed *pBPA* terms s_1 and s_2 such that *pACP*$^+ \vdash a \cdot p_1 \mid q_1 = s_1$ and *pACP*$^+ \vdash a \cdot p_1 \mid q_2 = s_2$. Then *pACP*$^+ \vdash p \mid q = s_1 + s_2$ which is a closed *pBPA* term;

pACP$^+ \vdash p \parallel q = a \cdot (p_1 \parallel q) + q_1 \mathbin{\lfloor\!\lfloor} p + q_2 \mathbin{\lfloor\!\lfloor} p + a \cdot p_1 \mid q_1 + a \cdot p_1 \mid q_2$. By the inductive hypothesis there are closed *pBPA* terms t_1, t_2, t_3, t_4 and t_5 such that *pACP*$^+ \vdash p_1 \parallel q = t_1$, *pACP*$^+ \vdash q_1 \parallel p = t_2$, *pACP*$^+ \vdash q_2 \mathbin{\lfloor\!\lfloor} p = t_3$, *pACP*$^+ \vdash a \cdot p_1 \mid q_1 = t_4$ and *pACP*$^+ \vdash a \cdot p_1 \mid q_2 = t_5$. Then *pACP*$^+ \vdash p \mid q = a \cdot t_1 + t_2 + t_3 + t_4 + t_5$ which is a closed *pBPA* term;

Case $p \equiv p_1 + p_2$ *and* $q \equiv q_1 + q_2$. *pACP*$^+ \vdash p \mathbin{\lfloor\!\lfloor} q = (p_1 \mathbin{\lfloor\!\lfloor} q) + (p_2 \mathbin{\lfloor\!\lfloor} q)$. By the inductive hypothesis there are closed *pBPA* terms r_1 and r_2 such that *pACP*$^+ \vdash p_1 \mathbin{\lfloor\!\lfloor} q = r_1$ and *pACP*$^+ \vdash p_2 \mathbin{\lfloor\!\lfloor} q = r_2$. Then, *pACP*$^+ \vdash p \mathbin{\lfloor\!\lfloor} q = r_1 + r_2$ which is a closed *pBPA* term;

pACP$^+ \vdash p \mid q = (p_1 \mid q_1) + (p_1 \mid q_2) + (p_2 \mid q_1) + (p_2 \mid q_2)$. By the inductive hypothesis there are closed *pBPA* terms s_1, s_2, s_3 and s_4 such that *pACP*$^+ \vdash p_1 \mid q_1 = s_1$, *pACP*$^+ \vdash p_1 \mid q_2 = s_2$, *pACP*$^+ \vdash p_2 \mid q_1 = s_3$ and *pACP*$^+ \vdash p_2 \mid q_2 = s_4$. Then *pACP*$^+ \vdash p \mid q = s_1 + s_2 + s_3 + s_4$ which is a closed *pBPA* term;

pACP$^+ \vdash p \parallel q = (p_1 \mathbin{\lfloor\!\lfloor} q) + (p_2 \mathbin{\lfloor\!\lfloor} q) + (q_1 \mathbin{\lfloor\!\lfloor} p) + (q_2 \mathbin{\lfloor\!\lfloor} p) + (p_1 \mid q_1) + (p_1 \mid q_2) + (p_2 \mid q_1) + (p_2 \mid q_2)$. By the inductive hypothesis there are closed *pBPA* terms $t_1, t_2, \ldots, t_8$ such that *pACP*$^+ \vdash p_1 \mathbin{\lfloor\!\lfloor} q = t_1$, *pACP*$^+ \vdash p_2 \mathbin{\lfloor\!\lfloor} q = t_2$, *pACP*$^+ \vdash q_1 \mathbin{\lfloor\!\lfloor} p = t_3$, *pACP*$^+ \vdash q_2 \mathbin{\lfloor\!\lfloor} p = t_4$, *pACP*$^+ \vdash p_1 \mid q_1 = t_5$, *pACP*$^+ \vdash p_1 \mid q_2 = t_6$, *pACP*$^+ \vdash p_2 \mid q_1 = t_7$ and *pACP*$^+ \vdash p_2 \mid q_2 = t_8$. Then *pACP*$^+ \vdash p \mid q = t_1 + t_2 + t_3 + t_4 + t_5 + t_6 + t_7 + t_8$ which is a closed *pBPA* term;

pACP$^+ \vdash \partial_H(p) = \partial_H(p_1) + \partial_H(p_2)$. By the inductive hypothesis there are closed *pBPA* terms u_1 and u_2 such that *pACP*$^+ \vdash \partial_H(p_1) = u_1$ and *pACP*$^+ \vdash \partial_H(p_2) = u_2$. Thus, *pACP*$^+ \vdash \partial_H(p) = u_1 + u_2$ which is a closed *pBPA* term;

By this all possibilities for basic $\mathcal{B}_+$ terms are exhausted. Still we need to investigate the cases when p or q are $\mathcal{B} \setminus \mathcal{B}_+$ basic terms.

Case $p \in \mathcal{B}_+$ *and* $q \in \mathcal{B} \setminus \mathcal{B}_+$. For some $m \in \mathbb{N}, m \geq 2$, $q_i \in \mathcal{B}_+$ and $\rho_i \in \langle 0, 1 \rangle$ for $1 \leq i \leq m$, $q \equiv q_1 \leftplus_{\rho_1} q_2 \leftplus_{\rho_2} \ldots q_{m-1} \leftplus_{\rho_{m-1}} q_m$. If we look at the proofs about the left merge operator in the previous cases we can observe that the equations used there do not depend on the left argument q. Therefore, since p is a basic $\mathcal{B}_+$ term the previous cases apply here as well (for the left merge only). So we conclude that there is a closed *pBPA* term r such that *pACP*$^+ \vdash p \mathbin{\lfloor\!\lfloor} q = r$;

pACP$^+ \vdash p \mid q = (p \mid q_1) \leftplus_{\rho_1} (p \mid q_2) \leftplus_{\rho_2} \ldots (p \mid q_{m-1}) \leftplus_{\rho_{m-1}} (p \mid q_m)$ and the result follows from the inductive hypothesis if applied on every term $p \mid q_i$;

pACP$^+ \vdash p \parallel q = (p \mathbin{\lfloor\!\lfloor} q + q_1 \mathbin{\lfloor\!\lfloor} p + p \mid q_1) \leftplus_{\rho_1} (p \mathbin{\lfloor\!\lfloor} q + q_2 \mathbin{\lfloor\!\lfloor} p + p \mid q_2) \leftplus_{\rho_2} \ldots \leftplus_{\rho_{m-1}} (p \mathbin{\lfloor\!\lfloor} q + q_m \mathbin{\lfloor\!\lfloor} p + p \mid q_m)$ and the result follows from the inductive hypothesis which is applicable on every summand in any bracket on the right-hand side of this equation;

Case $p \in \mathcal{B} \setminus \mathcal{B}_+$ *and* $q \in \mathcal{B}_+$. For some $n \in \mathbb{N}, n \geq 2$, $p_i \in \mathcal{B}_+$ and $\pi_i \in \langle 0,1 \rangle$ for $1 \leq i \leq n$ and $p \equiv p_1 \leftplus_{\pi_1} p_2 \leftplus_{\pi_2} \ldots p_{n-1} \leftplus_{\pi_{n-1}} p_n$. The only difference with the previous case is the left merge. So, for it we have $pACP^+ \vdash p \lfloor\!\lfloor q = (p_1 \lfloor\!\lfloor q) \leftplus_{\pi_1} (p_2 \lfloor\!\lfloor q) \leftplus_{\pi_2} \ldots (p_{n-1} \lfloor\!\lfloor q) \leftplus_{\pi_{n-1}} (p_n \lfloor\!\lfloor q)$ and the result follows from the inductive hypothesis when it is applied on each term $p_i \lfloor\!\lfloor q$;

For the encapsulation operator we have:
$pACP^+ \vdash \partial_H(p) = \partial_H(p_1) \leftplus_{\pi_1} \partial_H(p_2) \leftplus_{\pi_2} \ldots \partial_H(p_{n-1}) \leftplus_{\pi_{n-1}} \partial_H(p_n)$
and the result follows from the inductive hypothesis when it is applied on each $\partial_H(p_i)$;

Case $p, q \in \mathcal{B} \setminus \mathcal{B}_+$. for some $n \in \mathbb{N}, n \geq 2$, $p_i \in \mathcal{B}_+$ and $\pi_i \in \langle 0,1 \rangle$ for $1 \leq i \leq n$, $p \equiv p_1 \leftplus_{\pi_1} p_2 \leftplus_{\pi_2} \ldots p_{n-1} \leftplus_{\pi_{n-1}} p_n$ and also for some $m \in \mathbb{N}, m \geq 2$, $q_j \in \mathcal{B}_+$ and $\rho_j \in \langle 0,1 \rangle$ for $1 \leq j \leq m$, $q \equiv q_1 \leftplus_{\rho_1} q_2 \leftplus_{\rho_2} \ldots q_{m-1} \leftplus_{\rho_{m-1}} q_m$. Then the case about the left merge is the same as in the previous case.

$$pACP^+ \vdash p \mid q = \big(p_1 \leftplus_{\pi_1} p_2 \leftplus_{\pi_2} \ldots p_{n-1} \leftplus_{\pi_{n-1}} p_n\big) \mid \big(q_1 \leftplus_{\rho_1} q_2 \leftplus_{\rho_2} \ldots q_{m-1} \leftplus_{\rho_{m-1}} q_m\big) \underset{PrCM4(n\times),PrCM5(n\cdot m\times)}{=} \leftplus_{\pi_i \cdot \rho_j : 1 \leq i \leq n, 1 \leq j \leq m} (p_i \mid q_j).$$

By the inductive hypothesis there are closed *pBPA* terms s_{ij} for $1 \leq i \leq n$ and $1 \leq j \leq m$ such that $pACP^+ \vdash p_i \mid q_j = s_{ij}$. Then the result follows from the inductive hypothesis. For the case $p \parallel q$ we will obtain basically an expression which is an alternative composition of the previous two cases (the case for the $\lfloor\!\lfloor$ and $\mid$ operators) which is easy to derive using the $PrMM2-4$ axioms. Again the result follows directly from the inductive hypothesis.

□

Lemma 4.2.4. If p, q, z and w are basic terms, then there is a closed *pBPA* term r such that $pACP^+ \vdash (p,z) \between (q,w) = r$.

Proof. We prove the claim using induction on the structure on p and q.

Case $p, q \in \mathcal{B}_+$. $pACP^+ \vdash (p,z) \between (q,w) = p \lfloor\!\lfloor w + q \lfloor\!\lfloor w + p \mid q$ and the result follows from Lemma 4.2.3.

Case $p \in \mathcal{B}_+$ *and* $q \in \mathcal{B} \setminus \mathcal{B}_+$. For some $m \in \mathbb{N}, m \geq 2$, $q_i \in \mathcal{B}_+$ and $\rho_i \in \langle 0,1 \rangle$ for $1 \leq i \leq m$, $q \equiv q_1 \leftplus_{\rho_1} q_2 \leftplus_{\rho_2} \ldots q_{m-1} \leftplus_{\rho_{m-1}} q_m$. Then
$pACP^+ \vdash (p,z) \between (q,w) = (p,z) \between (q_1,w) \leftplus_{\rho_1} (p,z) \between (q_2,w) \leftplus_{\rho_2} \ldots \leftplus_{\rho_{m-1}} (p,z) \between (q_m,w)$ and the result follows from the inductive hypothesis;

Case $p, q \in \mathcal{B} \setminus \mathcal{B}_+$. For some $n \in \mathbb{N}, n \geq 2$, $p_i \in \mathcal{B}_+$ and $\pi_i \in \langle 0,1 \rangle$ for $1 \leq i \leq n$, $p \equiv p_1 \leftplus_{\pi_1} p_2 \leftplus_{\pi_2} \ldots p_{n-1} \leftplus_{\pi_{n-1}} p_n$ and also for some $m \in \mathbb{N}, m \geq 2$, $q_j \in \mathcal{B}_+$ and $\rho_j \in \langle 0,1 \rangle$ for $1 \leq j \leq m$, $q \equiv q_1 \leftplus_{\rho_1} q_2 \leftplus_{\rho_2} \ldots q_{m-1} \leftplus_{\rho_{m-1}} q_m$. Then $pACP^+ \vdash (p,z) \between (q,w) = \leftplus_{\pi_i \cdot \rho_j : 1 \leq i \leq n, 1 \leq j \leq m} (p_i,z) \between (q_j,w)$ and by the inductive hypothesis there are closed *pBPA* terms s_{ij} for $1 \leq i \leq n$ and $1 \leq j \leq m$ such that $pACP^+ \vdash (p_i,z) \between (q_j,w) = s_{ij}$. The result follows straightforwardly.

□

Theorem 4.2.5 (*Elimination theorem of* $pACP^+$). Let p be a closed $pACP^+$ term. Then there is a closed *pBPA* term q such that $pACP^+ \vdash p = q$.

Proof. Let p be a closed $pACP^+$ term. The theorem is proved by case distinction on the structure of p.

Case $p \equiv a, a \in A_\delta$. p is a closed *pBPA* term;

Case $p \equiv p_1 \cdot p_2$. p_1 and p_2 are closed *pACP*$^+$ terms and the inductive hypothesis is applicable on them. Thus, there exist closed *pBPA* terms q_1 and q_2 such that *pACP*$^+ \vdash p_1 = q_1$ and *pACP*$^+ \vdash p_2 = q_2$. Then *pACP*$^+ \vdash p = p_1 \cdot p_2 = q_1 \cdot q_2$ and $q_1 \cdot q_2$ is a closed *pBPA* term;

Case $p \equiv p_1 + p_2$ *or* $p \equiv p_1 \leftplus_\pi p_2$. These cases are treated analogously as the previous case;

Case $p \equiv p_1 \between p_2$. p_1 and p_2 are closed *pACP*$^+$ terms. By the induction there are closed *pBPA* terms q_1 and q_2 such that *pACP*$^+ \vdash p_1 = q_1$ and *pACP*$^+ \vdash p_2 = q_2$. By Theorem 3.2.23 there are basic terms r_1 and r_2 such that *pBPA* $\vdash q_1 = r_1$ and *pBPA* $\vdash q_2 = r_2$. But then also, *pACP*$^+ \vdash p_1 = r_1$ and *pACP*$^+ \vdash p_2 = r_2$ and *pACP*$^+ \vdash p_1 \between p_2 = r_1 \between r_2$ as well. From Lemma 4.2.3 follows that there is a closed *pBPA* term s such that *pACP*$^+ \vdash r_1 \between r_2 = s$;

Case $p \equiv p_1 \mid p_2$. It can be proved in a similar way like the previous case;

Case $p \equiv (p_1, z_1) \between (p_2, z_2)$. It can be proved in a similar way like the case where $p \equiv p_1 \between p_2$, just instead of Lemma 4.2.3, Lemma 4.2.4 is applied;

Case $p \equiv p_1 \parallel p_2$. *pACP*$^+ \vdash p = p_1 \parallel p_2 = (p_1, p_1) \between (p_2, p_2)$ and the result follows from the previous case;

Case $p \equiv \partial_H(p_1)$. p_1 is a closed *pACP*$^+$ term. By the induction there is a closed *pBPA* term q_1 such that *pACP*$^+ \vdash p_1 = q_1$. By Theorem 3.2.23 there is a basic term r_1 such that *pBPA* $\vdash q_1 = r_1$. Thus, *pACP*$^+ \vdash p_1 = r_1$ and *pACP*$^+ \vdash \partial_H(p_1) = \partial_H(r_1)$ as well. From Lemma 4.2.3 follows that there is a closed *pBPA* term s such that *pACP*$^+ \vdash \partial_H(r_1) = s$ which concludes the proof. □

4.3 Structured operational semantics of *pACP*$^+$

In this section, we construct the bisimulation model of *pACP*$^+$, $\mathcal{M}_{pACP^+}$. We follow the schema and refer to definitions given in Section 3.3.1. We do not deal with the recursive specification and projection in *pACP*$^+$, so we only present the model of finite processes. Adding recursive specifications in *pACP*$^+$ and solutions of them (and thus making a model with infinite processes), can be done in a similar way as in Chapter 3.

4.3.1 Model of *pACP*$^+$ and properties of the model

The operational semantics of *pACP*$^+$ is given by the term-deduction system $\mathbf{T}_{pACP^+} = (\breve{\Sigma}_{pACP^+}, \mathbf{DR}_{pACP^+})$ with $\breve{\Sigma}_{pACP^+} = (A_\delta \cup \breve{A}_\delta, +, \cdot, \leftplus_\pi, \parallel, \between, \mid, \between, \partial_H)$ and with the deduction rules shown in Table 3.8 (on pg. 55) and 3.10 (on pg. 56) (the deduction rules of *pBPA*), the rules in Table 4.5 (rules for probabilistic transitions for the new operators) as well as the deduction rules for atomic transitions in Table 4.6 (basically the deduction rules of *ACP*). With PRA replaced by *pACP*$^+$, the items 1, 3-5 in Definition 3.3.2 (on pg. 49) together with the added ones in Definition 4.3.1 (according to the 7th item in Definition 3.3.2) define the set of static processes $\mathbb{SP}(pACP^+)$; the items 1-3 in Definition 3.3.3 (on pg. 49) together with 5.1-5.3 in Definition 4.3.2 define the set of trivial static processes $\mathbb{D}(pACP^+)$; the items 1-3 in Definition 3.3.4 (on pg. 50) together with 5.1-5.3 in Definition 4.3.3 define the set of dynamic processes, $\mathbb{DP}(pACP^+)$; the PDF function μ on $\mathbb{PT}(pACP^+)$ is defined by

Definition 4.3.4 and the probabilistic bisimulation relation on $\mathbb{PT}(pACP^+)$ is defined by Definition 3.3.11 (on pg. 53) with PRA is replaced by $pACP^+$.

Definition 4.3.1. (Continuation of Definition 3.3.2)

7.1. if $s, t \in \mathbb{SP}(pACP^+)$, then $s \between t, s \mid t, s \parallel t \in \mathbb{SP}(pACP^+)$;

7.2. if $s, t, z, w \in \mathbb{SP}(pACP^+)$, then $(s, z) \between (t, w) \in \mathbb{SP}(pACP^+)$;

7.3. if $s \in \mathbb{SP}(pACP^+)$, then $\partial_H(s) \in \mathbb{SP}(pACP^+)$.

Definition 4.3.2. (Continuation of Definition 3.3.3)

5.1. if $s, t \in \mathbb{D}(pACP^+)$, then $s \mid t \in \mathbb{D}(pACP^+)$;

5.2. if $s \in \mathbb{D}(pACP^+), t \in \mathbb{SP}(pACP^+)$, then $s \between t \in \mathbb{D}(pACP^+)$;

5.3. if $s \in \mathbb{D}(pACP^+)$, then $\partial_H(s) \in \mathbb{D}(pACP^+)$.

Definition 4.3.3. (Continuation of Definition 3.3.4)

5.1. $\varphi(s \between t) = \varphi(s) \between t$;

5.2. $\varphi(s \mid t) = \varphi(s) \mid \varphi(t)$;

5.3. $\varphi(\partial_H(s)) = \partial_H(\varphi(s))$.

$$\frac{x \rightsquigarrow x', y \rightsquigarrow y'}{x \parallel y \rightsquigarrow x' \between y + y' \between x + x' \mid y'} \qquad \frac{x \rightsquigarrow x', y \rightsquigarrow y'}{(x, z) \between (y, w) \rightsquigarrow x' \between w + y' \between z + x' \mid y'}$$

$$\frac{x \rightsquigarrow x'}{x \between y \rightsquigarrow x' \between y} \qquad \frac{x \rightsquigarrow x', y \rightsquigarrow y'}{x \mid y \rightsquigarrow x' \mid y'} \qquad \frac{x \rightsquigarrow x'}{\partial_H(x) \rightsquigarrow \partial_H(x')}$$

Table 4.5: Probabilistic transitions of additional operators of $pACP^+$.

Definition 4.3.4. (PDF for $pACP^+$) A probability distribution function on $\mathbb{PT}(pACP^+)$ is defined by the equalities in Table 3.6, 3.7 and 4.7.

Observe that the deduction rules for action transitions of the parallel composition operator are not involved in this term-deduction system. As it will be proved later (Proposition 4.3.8) static process can perform a probabilistic step and it reaches a dynamic process which can proceed by an atomic transition. Therefore, a static process can be a parallel composition of two other static processes. After performing a probabilistic transition the dynamic process reached is no longer a parallel composition. If we look at all the rules for probabilistic transitions we can observe that a dynamic process that is a parallel composition of two processes can never be obtained.

$$\frac{x \xrightarrow{a} x'}{x \between y \xrightarrow{a} x' \parallel y} \qquad \frac{x \xrightarrow{a} \surd}{x \between y \xrightarrow{a} y} \qquad \frac{x \xrightarrow{a} x', y \xrightarrow{b} y', \gamma(a,b) = c}{x \mid y \xrightarrow{c} x' \parallel y'}$$

$$\frac{x \xrightarrow{a} x', y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \mid y \xrightarrow{c} x', y \mid x \xrightarrow{c} x'} \qquad \frac{x \xrightarrow{a} \surd, y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \mid y \xrightarrow{c} \surd}$$

$$\frac{x \xrightarrow{a} x', a \notin H}{\partial_H(x) \xrightarrow{a} \partial_H(x')} \qquad \frac{x \xrightarrow{a} \surd, a \notin H}{\partial_H(x) \xrightarrow{a} \surd}$$

Table 4.6: Action transitions of *pACP*$^+$.

$\mu(x \parallel y, x' \between y + y' \between x + x' \mid y')$	$=$	$\mu(x,x') \cdot \mu(y,y')$	
$\mu(x \between y, x' \between y)$	$=$	$\mu(x,x')$	
$\mu(x \mid y, x' \mid y')$	$=$	$\mu(x,x') \cdot \mu(y,y')$	
$\mu((x,z) \between (y,w), x' \between w + y' \between q + x' \mid y')$	$=$	$\mu(x,x') \cdot \mu(y,y')$	
$\mu(\partial_H(x), \partial_H(x'))$	$=$	$\mu(x,x')$	
$\mu(x,u)$	$=$	0	$otherwise$

Table 4.7: Equalities that define PDFs for *pACP*$^+$ (part 3 - parallel composition)

Many properties given and proved valid in *pBPA* need to be extended in *pACP*$^+$. In their proofs in Chapter 3, the axioms of *pBPA* and the deduction rules of $\mathbf{T}_{pBPA}$ were used. Since no axiom or deduction rule for the operators of *pBPA* is added to *pACP*$^+$ and $\mathbf{T}_{pACP^+}$, it is clear that these proofs remain valid in *pACP*$^+$ and $\mathbf{T}_{pACP^+}$, respectively. If the proof of one property given in Chapter 3 is inductive, then it is sufficient to continue the induction for the added operators in *pACP*$^+$.

Proposition 4.3.5. μ is well-defined on $\mathbb{PT}$(*pACP*$^+$).

Proof. We give the continuation of the proof of Proposition 3.3.18.

Case $\mathbb{SP}$(*pACP*$^+$) *processes.* Assume that $t \in \mathbb{SP}$(*pACP*$^+$).

Case $t \equiv s \between r$. $\mu(s \between r, u) = \begin{cases} \mu(s,v), & if\ u \equiv v \between r \\ 0, & otherwise \end{cases}$. By inductive hypothesis $\mu(s,v)$ is defined and so, $\mu(s \between r, u)$ is defined as well.

Case $t \equiv s \mid r$. $\mu(s \mid r, u) = \begin{cases} \mu(s,v) \cdot \mu(r,w), & if\ u \equiv v \mid w \\ 0, & otherwise \end{cases}$. $\mu(s,v)$ and $\mu(r,w)$ are defined by the inductive hypothesis. Hence, so $\mu(s \mid r, u)$ is defined as well.

Case $t \equiv s \parallel r$. $\mu(s \parallel r, u) = \begin{cases} \mu(s,v) \cdot \mu(r,w), & if\ u \equiv v \between r + w \between s + v \mid w \\ 0, & otherwise \end{cases}$. $\mu(s,v)$ and $\mu(r,w)$ are defined by the inductive hypothesis. Therefore, $\mu(s \parallel r, u)$ is defined as well.

Case $t \equiv (s,z) \between (r,w)$. $\mu((s,z) \between (r,w), u) = \begin{cases} \mu(s,x) \cdot \mu(r,y), if\ u \equiv x \between w + y \between z + x \mid y \\ 0, otherwise \end{cases}$

$\mu(s,x)$ and $\mu(r,y)$ are defined by the inductive hypothesis, so $\mu((s,z) \between (r,w), u)$ is defined as well.

Case $t \equiv \partial_H(s)$. $\mu(\partial_H(s), u) = \begin{cases} \mu(s,v), & if\ u \equiv \partial_H(v) \\ 0, & otherwise \end{cases}$. $\mu(s,v)$ is defined by the inductive hypothesis, so $\mu(\partial_H(s), u)$ is defined as well.

Case $\mathbb{DP}(pACP^+)$ *processes.* Assume that $t \in \mathbb{DP}(pACP^+)$. We will prove that $\mu(t,u) = 0$.

Case $t \equiv s \between r$. $\mu(s \between r, u) = \begin{cases} \mu(s,v), & if\ u \equiv v \between r \\ 0, & otherwise \end{cases}$. $\mu(s,v) = 0$ by the inductive hypothesis and $\mu(s \between r, u) = 0$ as well.

Case $t \equiv s \mid r$. $\mu(s \mid r, u) = \begin{cases} \mu(s,v) \cdot \mu(r,w), & if\ u \equiv v \mid w \\ 0, & otherwise \end{cases}$. By the inductive hypothesis $\mu(s,v) = 0$ and $\mu(r,w) = 0$. Then, $\mu(s \mid r, u) = 0$ as well.

Case $t \equiv \partial_H(s)$. $\mu(\partial_H(s), u) = \begin{cases} \mu(s,v), & if\ u \equiv \partial_H(v) \\ 0, & otherwise \end{cases}$. By the inductive hypothesis $\mu(s,v) = 0$. Then $\mu(\partial_H(s), u) = 0$ as well.

□

Proposition 4.3.6. The cPDF μ^* is well-defined on $\mathbb{PT}(pACP^+)$.

Proof. Continuation of the proof of Proposition 3.3.20.

Case $t \equiv s \between r$.

$$\begin{aligned} \mu(s \between r, M) &= \sum_{x \in M} \mu(s \between r, x) = \sum_{x : x \in M \,\&\, \exists x' : x \equiv x' \between r} \mu(s \between r, x) = \sum_{x' : x' \between r \in M} \mu(s, x') \\ &= \mu(s, \{x' \,:\, x' \between r \in M\}) \in [0,1] \text{ by the inductive hypothesis.} \end{aligned}$$

Case $t \equiv s \mid r$.

$$\begin{aligned} \mu(s \mid r, M) &= \sum_{x \in M} \mu(s \mid r, x) = \sum_{x : x \in M \,\&\, \exists x', x'' : x \equiv x' \mid x''} \mu(s \mid r, x) \\ &= \sum_{x', x'' : x' \mid x'' \in M} \mu(s, x') \cdot \mu(r, x'') \\ &\leq \mu(s, \{x' : \exists x'' : x' \mid x'' \in M\}) \cdot \mu(r, \{x'' : \exists x' : x' \mid x'' \in M\}) \in [0,1] \end{aligned}$$

by the inductive hypothesis.

Case $t \equiv s \parallel r$.

$$\begin{aligned} \mu(s \parallel r, M) &= \sum_{x \in M} \mu(s \parallel r, x) = \sum_{x : x \in M \,\&\, \exists x', x'' : x \equiv x' \between r + x'' \between s + x' \mid x''} \mu(s \parallel r, x) \\ &= \sum_{x', x'' : x' \between r + x'' \between s + x' \mid x'' \in M} \mu(s, x') \cdot \mu(r, x'') \\ &\leq \mu(s, \{x' : \exists x'' : x' \between r + x'' \between s + x' \mid x'' \in M\}) \\ &\qquad \cdot \mu(r, \{x'' : \exists x' : x' \between r + x'' \between s + x' \mid x'' \in M\}) \in [0,1] \end{aligned}$$

by the inductive hypothesis.

Case $t \equiv (s,z) \between (r,w)$.

$$\begin{aligned}\mu((s,z) \between (r,w), M) &= \sum_{x \in M} \mu((s,z) \between (r,w), x) \\ &= \sum_{x:x\in M \& \exists x',x'':x \equiv x' \between w+x'' \between z+x' \,|\, x''} \mu((s,z) \between (r,w), x) \\ &= \sum_{x',x'':x' \between w+x'' \between z+x' \,|\, x'' \in M} \mu(s,x') \cdot \mu(r,x'') \\ &\leq \mu(s, \{x' : \exists x'' : x' \between w + x'' \between z + x' \,|\, x'' \in M\}) \\ &\quad \cdot \mu(r, \{x'' : \exists x' : x' \between w + x'' \between z + x' \,|\, x'' \in M\}) \in [0,1]\end{aligned}$$

by the inductive hypothesis.

Case $t \equiv \partial_H(s)$.

$$\begin{aligned}\mu(\partial_H(s), M) &= \sum_{x \in M} \mu(\partial_H(s), x) = \sum_{x:x\in M \& \exists x':x \equiv \partial_H(x')} \mu(\partial_H(s), x) \\ &= \sum_{x':\partial_H(x') \in M} \mu(s,x') = \mu(s, \{x' \,:\, \partial_H(x') \in M\}) \in [0,1]\end{aligned}$$

by the inductive hypothesis.

□

Proposition 4.3.7. Let be $p,q,z,w \in \mathbb{SP}(pACP^+)$ and $K,L,P,Q \subseteq \mathbb{PT}(pACP^+)$. We denote: $K \,{}^P\!\parallel^Q\, L = \{k \between q + l \between p + k \,|\, l \,:\, k \in K,\ l \in L,\ p \in P,\ q \in Q\}$ and if P or Q are singletons we omit the brackets. Then:

i. The equalities given in Proposition 3.3.21 are valid when *pBPA* $+ PR$ is replaced by *pACP*$^+$;

ii. $\mu(p \parallel q, K \,{}^p\!\parallel^q\, L) = \mu(p,K) \cdot \mu(q,L)$;

iii. $\mu((p,z) \between (q,w), K \,{}^z\!\parallel^w\, L) = \mu(p,K) \cdot \mu(q,L)$;

iv. $\mu(p \between q, K \between L) = \mu(p,K)$ if $q \in L$, and $\mu(p \between q, K \between L) = 0$ otherwise.

v. $\mu(p \,|\, q, K \,|\, L) = \mu(p,K) \cdot \mu(q,L)$;

vi. $\mu(\partial_H(p), \partial_H(K)) = \mu(p,K)$.

Proof.

ii. $\mu(p \parallel q, K \,{}^p\!\parallel^q\, L) = \mu(p \parallel q, \bigcup_{k\in K} \bigcup_{l \in L} \{k \between q + l \between p + k \,|\, l\}) = \sum_{k\in K} \sum_{l\in L} \mu(p \parallel q, k \between q + l \between p + k \,|\, l)$

$$= \sum_{k\in K} \sum_{l\in L} \mu(p,k) \cdot \mu(q,l) = \Big(\sum_{k\in K} \mu(p,k)\Big)\Big(\sum_{l\in L} \mu(q,l)\Big) = \mu(p,K) \cdot \mu(q,L).$$

iii. In a similar way as in the case *ii.*

iv. If $q \in L$ then $\mu(p \between q, K \between L) = \mu(p \between q, \bigcup_{k\in K} \{k \between q\}) = \sum_{k\in K} \mu(p \between q, k \between q) = \sum_{k\in K} \mu(p,k) = \mu(p,K)$.

v. $\mu(p \,|\, q, K \,|\, L) = \mu(p \,|\, q, \bigcup_{k\in K} \bigcup_{l\in L} \{k \,|\, l\}) = \sum_{k\in K} \sum_{l\in L} \mu(p \,|\, q, k \,|\, l) = \sum_{k\in K} \sum_{l\in L} \mu(p,k) \cdot \mu(q,l)$

$$= \Big(\sum_{k\in K} \mu(p,k)\Big)\Big(\sum_{l\in L} \mu(q,l)\Big) = \mu(p,K) \cdot \mu(q,L).$$

vi. $\mu(\partial_H(p), \partial_H(K)) = \mu(\partial_H(p), \bigcup_{k\in K}\{\partial_H(k)\}) = \sum_{k\in K}\mu(\partial_H(p), \partial_H(k))$
$= \sum_{k\in K}\mu(p,k) = \mu(p,K).$ □

Alternation of probabilistic transitions and action transitions in the model of *pACP*$^+$ is confirmed by Proposition 4.3.8 and Proposition 4.3.9 given below.

Proposition 4.3.8. If $p \in \mathbb{SP}(pACP^+)$ and $p \rightsquigarrow u$, then $u \in \mathbb{DP}(pACP^+)$.

Proof. The proof is a continuation of the inductive proof of Proposition 3.3.22. Let us assume that $p \rightsquigarrow u$.

Case $p \equiv q \between r$. From the assumption it follows that $q \rightsquigarrow v$ and $u \equiv v \between r$. From the inductive hypothesis $v \in \mathbb{DP}(pACP^+)$ and $u \in \mathbb{DP}(pACP^+)$ as well;

Case $p \equiv q \mid r$. There are v and w such that t$q \rightsquigarrow v$, $r \rightsquigarrow w$ and $u \equiv v \mid w$. From the inductive hypothesis $v \in \mathbb{DP}(pACP^+)$ and $w \in \mathbb{DP}(pACP^+)$ from which $u \in \mathbb{DP}(pACP^+)$;

Case $p \equiv q \between r$. There are v and w such that $q \rightsquigarrow v$, $r \rightsquigarrow w$ and $u \equiv v \between r + w \between r + v \mid w$. From the inductive hypothesis $v \in \mathbb{DP}(pACP^+)$ and $w \in \mathbb{DP}(pACP^+)$ and also $v \between r, w \between q, v \mid w \in \mathbb{DP}(pACP^+)$. Hence, $u \in \mathbb{DP}(pACP^+)$;

Case $p \equiv (q,z) \between (r,s)$. From the assumption we have that $q \rightsquigarrow v$, $r \rightsquigarrow w$ and $u \equiv v \between s + w \between z + v \mid w$. From the inductive hypothesis $v \in \mathbb{DP}(pACP^+)$ and $w \in \mathbb{DP}(pACP^+)$. Therefore, $u \in \mathbb{DP}(pACP^+)$ as well;

Case $p \equiv \partial_H(q)$. Thus, $q \rightsquigarrow v$ and $u \equiv \partial_H(v)$. From the inductive hypothesis $v \in \mathbb{DP}(pACP^+)$ and $u \in \mathbb{DP}(pACP^+)$ as well.

□

Proposition 4.3.9. If x is a $\mathbb{D}(pACP^+)$ process and $x \xrightarrow{a} p$ for some $a \in A$, then $p \in \mathbb{SP}(pACP^+)$.

Proof. It is easy to prove by induction on the structure of $\mathbb{DP}(pACP^+)$ processes. □

We can prove that the alternative definition of probabilistic bisimulation given on page 63 is equivalent to probabilistic bisimulation (Definition 3.3.11) on $\mathbb{PT}(pACP^+)$ by proving that Proposition 3.3.28 is valid for $\mathbb{PT}(pACP^+)$ processes. Then, this can be used in the proofs of the Congruence and Soundness theorem. For these reasons we give several prerequisites and obtain the result straightforwardly (Corollary 4.3.14).

Proposition 4.3.10. If u is a $\mathbb{D}(pACP^+)$ process, then the only possible probabilistic transition of u is $u \rightsquigarrow \breve{u}$.

Proof. We give a continuation of the inductive proof of Proposition 3.3.24.

Case $u \equiv v \between t$. By the inductive hypothesis $v \rightsquigarrow \breve{v}$ is the only possible probabilistic transition of v. Then $u \rightsquigarrow \breve{v} \between t$ and this is the only possible probabilistic transition of u;

Case $u \equiv v \mid w$. By the inductive hypothesis $v \rightsquigarrow \breve{v}$ and $w \rightsquigarrow \breve{w}$ are the only possible probabilistic transitions of v and w, respectively. Therefore, $u \rightsquigarrow \breve{v} \mid \breve{w}$ and this is the only possible probabilistic transition of u;

Case $u \equiv \partial_H(v)$. From the inductive hypothesis $v \rightsquigarrow \breve{v}$ is the only possible probabilistic transition of v. Then $u \rightsquigarrow \partial_H(\breve{v})$ and this is the only possible probabilistic transition of u.

□

Proposition 4.3.11. If u is a $\mathbb{D}(pACP^+)$ process, then $\mu(u, \breve{u}) = 1$. □

Proposition 4.3.12. Let be $p \in \mathbb{PT}(pACP^+)$. Then $\mu(p, x) > 0$ iff $p \rightsquigarrow x$.

Proof. We give only the part of the proof concerning the $\|$ operator. The inductive proof for the other operators can easily be derived.

Assume that $p \in \mathbb{PT}(pACP^+)$ and $p \equiv q \,\|\, r$.

($\Rightarrow$) Let be $\mu(p, x) > 0$. From the definition of the probability distribution function and from the assumption $\mu(p, x) > 0$ it follows that $x \equiv v \between r + w \between q + v \,|\, w$ and $\mu(q, v) \cdot \mu(q, w) = \mu(p, x) > 0$. This implies $\mu(q, v) > 0$ and $\mu(r, w) > 0$. From the inductive hypothesis it follows that $q \rightsquigarrow v$ and $r \rightsquigarrow w$. Finally, from the deduction rules we conclude that $p \rightsquigarrow x$.

($\Leftarrow$) Let be $p \rightsquigarrow x$. From the assumption $p \equiv q \,\|\, r$ we obtain that $q \rightsquigarrow v$ and $r \rightsquigarrow w$ and $x \equiv v \between r + \between q + v \,|\, w$. From the inductive hypothesis it follows that $\mu(q, v) > 0$ and $\mu(r, w) > 0$. Since $\mu(p, x) = \mu(q, v) \cdot \mu(r, w)$, $\mu(p, x) > 0$ as well. □

Proposition 4.3.13. If $p \in \mathbb{SP}(pACP^+)$ then $\mu(p, \mathbb{PT}(pACP^+)) = 1$.

Proof. We just give the continuation of the inductive proof of Proposition 3.3.30.

Case $p \equiv q \between r$. From Proposition 4.3.7*iv.* and the inductive hypothesis we obtain:

$$\begin{aligned} \mu(p, \mathbb{DP}(pACP^+)) &= \mu(q \between r, \mathbb{DP}(pACP^+)) = \mu(q \between r, \mathbb{DP}(pACP^+) \between r) \\ &= \mu(q, \mathbb{DP}(pACP^+)) = 1; \end{aligned}$$

Case $p \equiv q \,|\, r$. From Proposition 4.3.7*v.* and the inductive hypothesis we obtain:

$$\begin{aligned} \mu(p, \mathbb{DP}(pACP^+)) &= \mu(q \,|\, r, \mathbb{DP}(pACP^+)) = \mu(q \,|\, r, \mathbb{DP}(pACP^+) \,|\, \mathbb{DP}(pACP^+)) \\ &= \mu(q, \mathbb{DP}(pACP^+)) \cdot \mu(r, \mathbb{DP}(pACP^+)) = 1 \cdot 1 = 1; \end{aligned}$$

Case $p \equiv q \,\|\, r$. Using Proposition 4.3.7*ii.* and the inductive hypothesis we obtain

$$\begin{aligned} \mu(p, \mathbb{DP}(pACP^+)) &= \mu(q \,\|\, r, \mathbb{DP}(pACP^+)) = \mu(q \,\|\, r, \mathbb{DP}(pACP^+)^q \,\|\, {}^r\mathbb{DP}(pACP^+)) \\ &= \mu(q, \mathbb{DP}(pACP^+)) \cdot \mu(r, \mathbb{DP}(pACP^+)) = 1 \cdot 1 = 1; \end{aligned}$$

Case $p \equiv (q, z) \between\!\between (r, w)$. Using Proposition 4.3.7*iii.* and the inductive hypothesis we obtain

$$\begin{aligned} \mu(p, \mathbb{DP}(pACP^+)) &= \mu((q, z) \between\!\between (r, w), \mathbb{DP}(pACP^+)) \\ &= \mu((q, z) \between\!\between (r, w), \mathbb{DP}(pACP^+)^z \,\|\, {}^w\mathbb{DP}(pACP^+)) \\ &= \mu(q, \mathbb{DP}(pACP^+)) \cdot \mu(r, \mathbb{DP}(pACP^+)) = 1 \cdot 1 = 1; \end{aligned}$$

Case $p \equiv \partial_H(q)$. Applying Proposition 4.3.7*vi.* and the inductive hypothesis we obtain

$$\mu(p, \mathbb{DP}(pACP^+)) = \mu(\partial_H(q), \partial_H(\mathbb{DP}(pACP^+)) = \mu(q, \mathbb{DP}(pACP^+)) = 1.$$

□

Corollary 4.3.14.

i. Let $p \in \mathbb{PT}(pACP^+)$ and $M \subseteq \mathbb{PT}(pACP^+)$. Then $\mu(p, M) > 0$ iff $\exists x \in M : p \rightsquigarrow x$;

ii. Proposition 3.3.32 is valid in $\mathbb{PT}(pACP^+)$

□

Theorem 4.3.15 (*Congruence theorem of pACP$^+$*). $\leftrightarrow$ is a congruence relation on $\mathbb{PT}(pACP^+)$ with respect to the $+, \cdot, \leftthreetimes_\pi, \between, |, \|, \between$ and ∂_H operators.

Proof. The part of the proof for the operators of *pBPA* is the same as the proof of the Congruence theorem of *pBPA* (Theorem 3.3.36) if *pBPA* is replaced by *pACP*$^+$. Here we give the rest of the proof which concerns the operators: $\|, \between, |, \between$ and ∂_H.

Parallel composition. Let x, y, z and w be $\mathbb{PT}(pACP^+)$ processes such that $x \leftrightarrow y$ and $z \leftrightarrow w$. So, there exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. We define a relation R in the following way:

$$R = Eq\big(\alpha \cup \beta \cup R_1 \cup R_2\big),$$

where

$$\begin{aligned}\alpha = \{&(p \,\|\, q, s \,\|\, t) \;:\; p, q, s, t \in \mathbb{SP}(pACP^+), (p, s) \in R_1, (q, t) \in R_2\},\\ \beta = \{&(u \between q + v \between p + u \,|\, v, l \between t + k \between s + l \,|\, k) \;:\; p, q, s, t \in \mathbb{SP}(pACP^+),\\ &\qquad u, v, l, k \in \mathbb{DP}(pACP^+),\\ &\qquad (p, s),\ (u, l) \in R_1, (q, t),\ (v, k) \in R_2\}.\end{aligned}$$

We can make the following observations:

M1: α and β are equivalence relations; α, R_1 and R_2 contain pairs of static processes relevant to R. β equivalence classes of $\mathbb{SP}(pACP^+)$ processes are singletons;

M2: if $(p \,\|\, q, s \,\|\, t) \in \alpha$ and $K \in \mathbb{DP}(pACP^+)/\beta$, then $p \,\|\, q \rightsquigarrow K$ iff $s \,\|\, t \rightsquigarrow K$;

M3: if $p \,\|\, q \rightsquigarrow K$ for $K \in \mathbb{DP}(pACP^+)/\beta$, then $K = [u \between q + v \between p + u \,|\, v]_\beta$ for some u, v such that $p \rightsquigarrow u$ and $q \rightsquigarrow v$. Moreover, from the definition of β we have that $K = [u]_{R_1}{}^{[p]_{R_1}} \,\|\, {}^{[q]_{R_2}}[v]_{R_2}$;

M4: since R_1, R_2 and β are all subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(pACP^+)/R$, then $M = \bigcup_{i_1 \in I_1} M^1_{i_1}$, $M = \bigcup_{i_2 \in I_2} M^2_{i_2}$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I_1, I_2 and J and for some equivalence classes $M^1_{i_1}$ $(i_1 \in I_1)$, $M^2_{i_2}$ $(i_2 \in I_2)$ and K_j $(j \in J)$ of R_1, R_2 and β, respectively.

Now suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}(pACP^+)$ and $M \in \mathbb{DP}(pACP^+)/R$. Then

1. If $(r, r_1) \in R_k, k = 1, 2$, then the result can be proved easily by use of **M4** and Proposition 3.3.9 *ii.* (see the proof of Theorem 3.3.36 pg. 63);

2. If $(r, r_1) \in \alpha$, then $r \equiv p \,\|\, q$ and $r_1 \equiv s \,\|\, t$ for some $p, q, s, t \in \mathbb{SP}(pACP^+)$ such that $(p, s) \in R_1$ and $(q, t) \in R_2$. According to **M3** and **M4**, $K_j = [u_j]_{R_1}{}^{[p]_{R_1}} \,\|\, {}^{[q]_{R_2}}[v_j]_{R_2}$ and $p \rightsquigarrow u_j$ and $q \rightsquigarrow v_j$. From Proposition 4.3.7*ii.* it follows that

$$\begin{aligned}\mu(p \,\|\, q, K_j) &= \mu(p \,\|\, q, [u_j]_{R_1}{}^{[p]_{R_1}} \,\|\, {}^{[q]_{R_2}}[v_j]_{R_2}) = \mu(p, [u_j]_{R_1}) \cdot \mu(q, [v_j]_{R_2})\\ &= \mu(s, [u_j]_{R_1}) \cdot \mu(t, [v_j]_{R_2}) = \mu(s \,\|\, t, [u_j]_{R_1}{}^{[p]_{R_1}} \,\|\, {}^{[q]_{R_2}}[v_j]_{R_2}) = \mu(s \,\|\, t, K_j).\end{aligned}$$

Using Proposition 3.3.9 *ii.* we can easily prove that $\mu(p \,\|\, q, M) = \mu(s \,\|\, t, M)$.

Merge with memory. Let $x_1, x_2, x_3, x_4, y_1, y_2, y_3$ and y_4 be $\mathbb{PT}(pACP^+)$ processes such that $x_i \leftrightarrow y_i$, $i = 1, 2, 3, 4$. So, there exist probabilistic bisimulations R_1, R_2, R_3 and R_4 such that $(x_i, y_i) \in R_i$, for $i = 1, 2, 3, 4$. We define a relation R in the following way:

$$R = Eq\big(\alpha \cup \beta \cup R_{14} \cup R_{23} \cup R_{12} \cup R_1 \cup R_2 \cup R_3 \cup R_4\big),$$

where

$$\alpha = \{((p_1, z_1) \between (q_1, w_1), (p_2, z_2) \between (q_2, w_2)) \ : \ p_1, q_1, z_1, w_1, p_2, q_2, z_2, w_2 \in \mathbb{SP}(\textit{pACP}^+), \\ (p_1, p_2) \in R_1, (q_1, q_2) \in R_2, \\ (z_1, z_2) \in R_3, (w_1, w_2) \in R_4\},$$

$$\beta = \{(u_1 \between w_1 + v_1 \between z_1 + u_1 \,|\, v_1, u_2 \between w_2 + v_2 \between z_2 + u_2 \,|\, v_2) \ : \ z_1, z_2, w_1, w_2 \in \mathbb{SP}(\textit{pACP}^+), \\ u_1, v_1, u_2, v_2 \in \mathbb{DP}(\textit{pACP}^+), \\ (u_1, u_2) \in R_1, \ (v_1, v_2) \ \in R_2, \\ (z_1, z_2) \in R_3, \ (w_1, w_2) \in R_4\},$$

R_{14}, R_{12} and R_{23} are defined in the same way like the relation R in the proof for parallel composition, except that the relation R_1 and R_2 occurring there are replaced by: R_1 and R_4 for R_{14}, R_1 and R_2 for R_{12} and R_2 and R_3 for R_{23}, respectively.
Let us note that:

MM1: α, β, R_{14}, R_{12} and R_{23} are equivalence relations; α, R_{14}, R_{12} and R_{23} contain pairs of static processes relevant to R;

MM2: If $((p_1, z_1) \between (q_1, w_1), (p_2, z_2) \between (q_2, w_2)) \in \alpha$ and $K \in \mathbb{DP}(\textit{pACP}^+)/\beta$, then $(p_1, z_1) \between (q_1, w_1) \rightsquigarrow K$ iff $(p_2, z_2) \between (q_2, w_2) \rightsquigarrow K$;

MM3: If $(p_1, z_1) \between (q_1, w_1) \rightsquigarrow K$ for $K \in \mathbb{DP}(\textit{pACP}^+)/\beta$, then $K = [u \between w_1 + v \between z_1 + u \,|\, v]_\beta$ for some u, v such that $p \rightsquigarrow u$ and $q \rightsquigarrow v$. Moreover, from the definition of β we have that $K = [u]_{R_1} {}^{[z_1]_{R_3}} \between {}^{[w_1]_{R_4}} [v]_{R_2}$;

MM4: since R_{14}, R_{12}, R_{23} and β are all subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(\textit{pACP}^+)/R$, then $M = \bigcup_{i \in I} M_i^1$, $M = \bigcup_{n \in N} M_n^2$, $M = \bigcup_{l \in L} M_l^3$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I, N, L and J and for some equivalence classes M_i^1 $(i \in I)$, M_n^2 $(n \in N)$, M_l^3 $(l \in L)$ and K_j $(j \in J)$ of R_{14}, R_{12}, R_{23} and β, respectively.

Now suppose that $(r_1, r_2) \in R$ for some $r_1, r_2 \in \mathbb{SP}(\textit{pACP}^+)$ and $M \in \mathbb{DP}(\textit{pACP}^+)/R$. Then

1. If $(r_1, r_2) \in R_{14}$ or $(r_1, r_2) \in R_{12}$ or $(r_1, r_2) \in R_{23}$ then the result follows from **MM4** and Proposition 3.3.9*ii.*;

2. If $(r_1, r_2) \in \alpha$ then $r \equiv (p_1, z_1) \between (q_1, w_1)$ and $r_1 \equiv (p_2, z_2) \between (q_2, w_2)$ for some $p_1, p_2, q_1, q_2, z_1, z_2, w_1, w_2 \in \mathbb{SP}(\textit{pACP}^+)$ such that $(p_1, p_2) \in R_1$, $(q_1, q_2) \in R_2$, $(z_1, z_2) \in R_3$ and $(w_1, w_2) \in R_4$. According to **MM3** and **MM4**, $K_j = [u_j]_{R_1} {}^{[z_1]_{R_3}} \between {}^{[w_1]_{R_4}} [v_j]_{R_2}$ and $p_1 \rightsquigarrow u_j$ and $q_1 \rightsquigarrow v_j$. Then from Proposition 4.3.7 *iii.* we obtain that

$$\begin{aligned} \mu((p_1, z_1) \between (q_1, w_1), K_j) &= \mu((p_1, z_1) \between (q_1, w_1), [u_j]_{R_1} {}^{[z_1]_{R_3}} \between {}^{[w_1]_{R_4}} [v_j]_{R_2}) \\ &= \mu(p_1, [u_j]_{R_1}) \cdot \mu(q_1, [v_j]_{R_2}) \\ &= \mu(p_2, [u_j]_{R_1}) \cdot \mu(q_2, [v_j]_{R_2}) \\ &= \mu((p_2, z_2) \between (q_2, w_2), [u_j]_{R_1} {}^{[z_1]_{R_3}} \between {}^{[w_1]_{R_4}} [v_j]_{R_2}) \\ &= \mu((p_2, z_2) \between (q_2, w_2), K_j). \end{aligned}$$

From Proposition 3.3.9 *ii.* we can easily prove that $\mu((p_1, z_1) \between (q_1, w_1), M) = \mu((p_2, z_2) \between (q_2, w_2), M)$.

Left merge. Let x, y, z and w be $\mathbb{PT}(\textit{pACP}^+)$ processes such that $x \leftrightarrows y$ and $z \leftrightarrows w$. So, there exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. We define a relation R in the following way:

$$R = Eq(\alpha' \cup \beta' \cup \alpha \cup \beta \cup R_1 \cup R_2),$$

where
$\alpha' = \{(p \between q, s \between t) \ : \ p,q,s,t \in \mathbb{SP}(\textit{pACP}^+), (p,s) \in R_1, (q,t) \in R_2\}$,
$\beta' = \{(u \between q, v \between t) \ : \ q,t \in \mathbb{SP}(\textit{pACP}^+), \ u,v \in \mathbb{DP}(\textit{pACP}^+), \ (u,v) \in R_1, (q,t) \in R_2\}$,
and α and β are the relations defined in the proof of parallel composition.

From the definitions of the relations we can observe that:

LM1: α' and β' are equivalence relations; α', α, R_1 and R_2 contain pairs of static processes relevant to R;

LM2: if $(p \between q, s \between t) \in \alpha'$ and $K \in \mathbb{DP}(\textit{pACP}^+)/\beta'$, then $p \between q \rightsquigarrow K$ iff $s \between t \rightsquigarrow K$;

LM3: if $p \between q \rightsquigarrow K$ for $K \in \mathbb{DP}(\textit{pACP}^+)/\beta'$, then $K = [u \between q]_{\beta'}$ for some u such that $p \rightsquigarrow u$. Moreover, from the definition of β' we have that $K = [u]_{R_1} \between [q]_{R_2}$;

LM4: since R_1, R_2, β and β' are all subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(\textit{pACP}^+)/R$, then $M = \bigcup_{i_1 \in I_1} M^1_{i_1}$, $M = \bigcup_{i_2 \in I_2} M^2_{i_2}$, $M = \bigcup_{j \in J} K_j$ and $M = \bigcup_{n \in N} M_n$ for some non-empty index sets I_1, I_2, J and N and for some equivalence classes $M^1_{i_1}$ $(i_1 \in I_1)$, $M^2_{i_2}$ $(i_2 \in I_2)$, K_j $(j \in J)$ and M_n $(n \in N)$ of R_1, R_2 β' and β, respectively.

Now suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}(\textit{pACP}^+)$ and $M \in \mathbb{DP}(\textit{pACP}^+)/R$. Then

1. If $(r, r_1) \in R_k, k = 1, 2$ then the result follows from **LM4** and Proposition 3.3.9*ii.*;
2. If $(r, r_1) \in \alpha$ the proof is given in the part for the $\between$ operator;
3. If $(r, r_1) \in \alpha'$ then $r \equiv p \between q$ and $r_1 \equiv s \between t$ for some $p, q, s, t \in \mathbb{SP}(\textit{pACP}^+)$ such that $(p, s) \in R_1$ and $(q, t) \in R_2$. According to **LM3** and **LM4**, $K_j = [u_j]_{R_1} \between [q]_{R_2}$ and $p \rightsquigarrow u_j$. Then from Proposition 4.3.7 *iv.* we obtain that
$$\begin{aligned} \mu(p \between q, K_j) &= \mu(p \between q, [u_j]_{R_1} \between [q]_{R_2}) = \mu(p, [u_j]_{R_1}) = \mu(s, [u_j]_{R_1})) \\ &= \mu(s \between t, [u_j]_{R_1} \between [q]_{R_2}) = \mu(s \between t, K_j). \end{aligned}$$
From Proposition 3.3.9 *ii.* we can easily prove that $\mu(p \between q, M) = \mu(s \between t, M)$.

Communication merge. Let x, y, z and w be $\mathbb{PT}(\textit{pACP}^+)$ processes such that $x \leftrightarrow y$ and $z \leftrightarrow w$. So, there exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. We define a relation R in the following way:

$$R = Eq(\alpha' \cup \beta' \cup \alpha \cup \beta \cup R_1 \cup R_2),$$

where
$\alpha' = \{(p \mid q, s \mid t) \ : \ p,q,s,t \in \mathbb{SP}(\textit{pACP}^+), (p,s) \in R_1, (q,t) \in R_2\}$,
$\beta' = \{(u \mid v, l \mid k) \ : \ u,v,l,k \in \mathbb{DP}(\textit{pACP}^+), \ (u,l) \in R_1, (v,k) \in R_2\}$,
and α and β are the relations defined in the proof of parallel composition operator.

Observe that:

CM1: α' and β' are equivalence relations; α', α, R_1 and R_2 contain pairs of static processes relevant to R;

CM2: if $(p \mid q, s \mid t) \in \alpha'$ and $K \in \mathbb{DP}(\textit{pACP}^+)/\beta'$, then $p \mid q \rightsquigarrow K$ iff $s \mid t \rightsquigarrow K$;

CM3: if $p \mid q \rightsquigarrow K$ for $K \in \mathbb{DP}(\textit{pACP}^+)/\beta'$, then $K = [u \mid v]_{\beta'}$ for some u, v such that $p \rightsquigarrow u$ and $q \rightsquigarrow v$. Moreover, from the definition of β' we have that $K = [u]_{R_1} \mid [v]_{R_2}$;

CM4: since R_1, R_2, β and β' are all subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(pACP^+)/R$, then $M = \bigcup_{i_1 \in I_1} M^1_{i_1}$, $M = \bigcup_{i_2 \in I_2} M^2_{i_2}$, $M = \bigcup_{j \in J} K_j$ and $M = \bigcup_{n \in N} M_n$ for some non-empty index sets I_1, I_2, J and N and for some equivalence classes $M^1_{i_1}$ $(i_1 \in I_1)$, $M^2_{i_2}$ $(i_2 \in I_2)$, K_j $(j \in J)$ and M_n $(n \in N)$ of R_1, R_2, β' and β, respectively.

Now suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}(pACP^+)$ and $M \in \mathbb{DP}(pACP^+)/R$. Then

1. If $(r, r_1) \in R_k, k = 1, 2$ then the result follows from **CM4** and Proposition 3.3.9*ii.*;
2. If $(r, r_1) \in \alpha$ the proof is given in the part for the $\|$ operator;
3. If $(r, r_1) \in \alpha'$ then $r \equiv p \,|\, q$ and $r_1 \equiv s \,|\, t$ for some $p, q, s, t \in \mathbb{SP}(pACP^+)$ such that $(p, s) \in R_1$ and $(q, t) \in R_2$. According to **CM3** and **CM4**, $K_j = [u_j]_{R_1} \,|\, [v_j]_{R_2}$ and $p \rightsquigarrow u_j$ and $q \rightsquigarrow v_j$. Then from Proposition 4.3.7 *v.* we obtain that
$$\begin{aligned} \mu(p \,|\, q, K_j) &= \mu(p \,|\, q, [u_j]_{R_1} \,|\, [v_j]_{R_2}) = \mu(p, [u_j]_{R_1}) \cdot \mu(q, [v_j]_{R_2}) \\ &= \mu(s, [u_j]_{R_1}) \cdot \mu(t, [v_j]_{R_2}) = \mu(s \,|\, t, [u_j]_{R_1} \,|\, [v_j]_{R_2}) = \mu(s \,|\, t, K_j). \end{aligned}$$
From Proposition 3.3.9 *v.* we can easily prove that $\mu(p \,|\, q, M) = \mu(s \,|\, t, M)$.

Encapsulation. Let x and y be $\mathbb{PT}(pACP^+)$ processes such that $x \leftrightarrows y$. So, there exists a probabilistic bisimulation R_1 such that $(x, y) \in R_1$. We define a relation R in the following way:

$$R = Eq(\alpha \cup \beta \cup R_1),$$

where
$\alpha = \{(\partial_H(p), \partial_H(q)) \,:\, p, q \in \mathbb{SP}(pACP^+), (p, q) \in R_1\}$,
$\beta = \{(\partial_H(u), \partial_H(v)) \,:\, u, v \in \mathbb{DP}(pACP^+),\ (u, v) \in R_1\}$.
Let us note that:

E1: α and β are equivalence relations; α and R_1 contain pairs of static processes relevant to R;

E2: if $(\partial_H(p), \partial_H(q)) \in \alpha$ and $K \in \mathbb{DP}(pACP^+)/\beta$, then $\partial_H(p) \rightsquigarrow K$ iff $\partial_H(q) \rightsquigarrow K$;

E3: if $\partial_H(p) \rightsquigarrow K$ for $K \in \mathbb{DP}(pACP^+)/\beta$, then $K = [\partial_H(u)]_\beta$ for some u such that $p \rightsquigarrow u$. Moreover, from the definition of β we have that $K = \partial_H([u]_{R_1})$;

E4: since R_1 and β are all subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(pACP^+)/R$, then $M = \bigcup_{i \in I} M_i$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I and J and for some equivalence classes M_i $(i \in I)$ and K_j $(j \in J)$ of R_1 and β, respectively.

Now suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}(pACP^+)$ and $M \in \mathbb{DP}(pACP^+)/R$. Then

1. If $(r, r_1) \in R_1$ then the result follows from **E4** and Proposition 3.3.9*ii.*;
2. If $(r, r_1) \in \alpha$ then $r \equiv \partial_H(p)$ and $r_1 \equiv \partial_H(q)$ for some $p, q \in \mathbb{SP}(pACP^+)$ such that $(p, q) \in R_1$. According to **E3** and **E4**, $K_j = \partial_H([u_j]_{R_1})$ and $p \rightsquigarrow u_j$. Then from Proposition 4.3.7*vi.* we obtain that
$$\begin{aligned} \mu(\partial_H(p), K_j) &= \mu(\partial_H(p), \partial_H([u_j]_{R_1})) = \mu(p, [u_j]_{R_1}) = \mu(q, [u_j]_{R_1}) \\ &= \mu(\partial_H(q), \partial_H([u_j]_{R_1})) = \mu(\partial_H(q), K_j). \end{aligned}$$
From Proposition 3.3.9*ii.* it follows that $\mu(\partial_H(p), M) = \mu(\partial_H(q), M)$.

□

The most tricky part in the proof of the Soundness theorem is the part about the conditional axioms: $PrMM4$, $PrCM4$ and $PrCM5$. First of all we should analyze the condition(s) of these axioms which in all cases has the form $p = p + p$. And we also need to find a way to use it as an assumption to prove soundness of the equation occurring on the right-hand side of the conditional axiom. Recall that $p \leftrightarrow p + p$ means that process p can reach only a single equivalence class doing probabilistic transitions. In that sense it behaves like a $\mathbb{D}(pACP^+)$ process. On the syntactic level we have proved the idempotency law for $\mathbb{D}(pACP^+)$ terms (see Proposition 3.2.17 on pg. 43 which can easily be extended for $pACP^+$). It is very easy to prove this property on the semantical level (Lemma 4.3.16). The main prerequisite for the soundness proof is stated in Lemma 4.3.17. It expresses exactly what we have claimed about a process that satisfy relation $p \leftrightarrow p+p$ - by every probabilistic transition it reaches bisimilar processes.

Lemma 4.3.16.

i. If $x \in \mathbb{D}(pACP^+)$ then $x \leftrightarrow x + x$.

ii. If $x, y, z \in \mathbb{D}(pACP^+)$ then $z \leftrightarrow x + y$ implies $z \leftrightarrow x + z$ (See Lemma 3.3.57). □

Lemma 4.3.17. (Towards Soundness of $pACP^+$)

i. Let x be an $\mathbb{SP}(pACP^+)$ process such that $x \rightsquigarrow x_1, x \rightsquigarrow x_2, \ldots, x \rightsquigarrow x_n$, $n \geq 1$, are all possible probabilistic transitions of x and for each i, j, $1 \leq i \leq n, 1 \leq j \leq n$, if $i \neq j$ then $x_i \not\leftrightarrow x_j$. Then there exists an $m, 1 \leq m \leq n$, such that $x + x \rightsquigarrow x_m + x_m$ is the only possible probabilistic transition of $x + x$ to the equivalence class $[x_m + x_m]_{\leftrightarrow}$.

ii. Let x be an $\mathbb{SP}(pACP^+)$ process such that $x \leftrightarrow x + x$. Then if $x \rightsquigarrow x'$ and $x \rightsquigarrow x''$ for some $x', x'' \in \mathbb{DP}(pACP^+)$, then $x' \leftrightarrow x''$.

Proof.

i. By the assumption $x \rightsquigarrow x_1, x \rightsquigarrow x_2, \ldots, x \rightsquigarrow x_n$ are all possible probabilistic transitions of x. It implies that $x + x \rightsquigarrow x_i + x_j$ for $i, j \in \{1, \ldots, n\}$ are all possible probabilistic transitions of $x + x$. We need to prove that

$$\exists m : \forall i, j : i \neq m \vee j \neq m \Rightarrow x_i + x_j \not\leftrightarrow x_m + x_m.$$

On the set $\{x_1, \ldots, x_n\}$ we define the following partial order:

$$x_i \leftarrow x_k \Leftrightarrow \exists x_j : x_i + x_j \leftrightarrow x_k + x_k.$$

Having that $\forall k : x_k + x_k \leftrightarrow x_k$ (Lemma 4.3.16 *i.*) we can reformulate the previous definition into:

$$x_i \leftarrow x_k \Leftrightarrow \exists x_j : x_i + x_j \leftrightarrow x_k. \tag{4.1}$$

$\leftarrow$ is a partial order because it is:

reflexive $x_k \leftarrow x_k$ since $x_k + x_k \leftrightarrow x_k$;

asymmetric Let be $x_i \leftarrow x_k$ and $x_k \leftarrow x_i$. From the definition of $\leftarrow$ we have that there are i_j, k_j such that $x_i + x_{i_j} \leftrightarrow x_k$ and $x_k + x_{k_j} \leftrightarrow x_i$. Then from Lemma 4.3.16*ii.* we obtain $x_i + x_k \leftrightarrow x_k$ and $x_k + x_i \leftrightarrow x_i$ and also $x_i \leftrightarrow x_k$. From the assumption that if $j \neq l$ then $x_j \not\leftrightarrow x_l$ we obtain $x_i \equiv x_k$;

transitive Let be $x_i \underline{\leftarrow} x_j$ and $x_j \underline{\leftarrow} x_k$. From the definition of $\underline{\leftarrow}$ we have that there are i_j, j_k such that $x_i + x_{i_j} \underline{\leftrightarrow} x_j$ and $x_j + x_{j_k} \underline{\leftrightarrow} x_k$. It implies that $x_i + x_{i_j} + x_{j_k} \underline{\leftrightarrow} x_j + x_{j_k} \underline{\leftrightarrow} x_k$. From Lemma 4.3.16*ii.* it follows that $x_i + x_k \underline{\leftrightarrow} x_k$ and also $x_i \underline{\leftarrow} x_k$.

Thus we have that $\underline{\leftarrow}$ is a partial order on the finite set $\{x_1, \ldots, x_n\}$. Then, there is a minimal element, that is:

$$\exists x_m : \forall x_i : x_i \underline{\leftarrow} x_m \Rightarrow x_m \equiv x_i.$$

Moreover if there is a j such that $x_m + x_j \underline{\leftrightarrow} x_m$, then we obtain $x_j \underline{\leftarrow} x_m$ (from the definition of $\underline{\leftarrow}$) and also $x_j \equiv x_m$ (since x_m is a minimal element). Thus we have obtained that

$$\exists x_m : \forall x_i, x_j : x_i \not\equiv x_m \vee x_j \not\equiv x_m \Rightarrow x_i + x_j \underline{\not\leftrightarrow} x_m$$

which says that the only possible process in $\{x_i + x_j : i, j \in \{1, \ldots, n\}\}$ bisimilar to x_m is $x_m + x_m$. This leads to the result that $x + x \rightsquigarrow x_m + x_m$ is the only possible probabilistic transition of $x + x$ to equivalence class $[x_m + x_m]_{\underline{\leftrightarrow}}$.

ii. Without loss of generality we can suppose that x is a process such that x does at most one probabilistic transition to an equivalence class. From *i.* it follows that exists a process y such that $x \rightsquigarrow y$, and $x + x \rightsquigarrow y + y$ is the only possible probabilistic transition of $x + x$ to equivalence class $[y + y]_{\underline{\leftrightarrow}}$. Thus it is sufficient to prove that $\mu(x, y) = 1$. The assumption $x \underline{\leftrightarrow} x + x$ implies $\mu(x, [y]_{\underline{\leftrightarrow}}) = \mu(x + x, [y]_{\underline{\leftrightarrow}})$. Having that $\mu(x, [y]_{\underline{\leftrightarrow}}) = \mu(x, y)$, $\mu(x + x, [y + y]_{\underline{\leftrightarrow}}) = \mu(x + x, y + y) = \mu(x, y)^2$ and $[y]_{\underline{\leftrightarrow}} = [y + y]_{\underline{\leftrightarrow}}$, we obtain $\mu(x, y) = \mu(x, y)^2$ for $\mu(x, y) \in [0, 1]$. It follows that $\mu(x, y) = 1$. By this we proved that x makes only one probabilistic transition exactly to the equivalence class of y. □

Theorem 4.3.18 (*Soundness of pACP$^+$*). Let $\mathbf{p}$ and $\mathbf{q}$ be closed *pACP$^+$* terms. If *pACP$^+$* $\vdash \mathbf{p} = \mathbf{q}$, then $p \underline{\leftrightarrow} q$.

Proof. We only treat the axioms which are added to *pBPA* to obtain *pACP$^+$*. The proof of soundness of the axioms of *pBPA* remains valid in *pACP$^+$* as well. For the axioms: CF, CM2, CM3, CM5, CM6, CM7, D1 and D2 we only give an equivalence relation that relates the left-hand side and the right-hand side of the considered axiom. Observe that the non-trivial pairs of related processes by these relations are $\mathbb{D}$(*pACP$^+$*) and $\mathbb{DP}$(*pACP$^+$*) processes. As we know $\mathbb{DP}$(*pACP$^+$*) processes can perform only action transitions. Thus, the part of the soundness proof regarding the action transitions (including action termination) for these pairs is very similar to the soundness proof of the corresponding *ACP* axiom with only difference in the used notation. For the $\mathbb{D}$(*pACP$^+$*) processes we use Proposition 4.3.10. By combining Proposition 4.3.11, 4.3.12 and 4.3.13 it is easy to conclude that the proposed equivalence relations for these axioms are bisimulation.

Axiom CF. Relation R is defined in the following way:

$$R = Eq\Big(\{(c, a \,|\, b), (\breve{c}, \breve{a} \,|\, \breve{b}) \ : \ \gamma(a, b) = c\}\Big).$$

Axiom CM2. Relation R is defined in the following way:

$$R = Eq\Big(\{(a \between p, a \cdot p) \ : \ p \in \mathbb{SP}(\textit{pACP}^+)\} \cup \{(\breve{a} \between p, \breve{a} \cdot p) \ : \ p \in \mathbb{SP}(\textit{pACP}^+)\}\Big).$$

Axiom CM3. Relation R is defined in the following way:

$$\begin{aligned} R &= Eq\Big(\{(a\cdot p\between q, a\cdot(p\parallel q)) \,:\, p,q\in\mathbb{SP}(\textit{pACP}^+)\} \\ &\qquad \cup\{(\breve{a}\cdot p\between q, \breve{a}\cdot(p\parallel q)) \,:\, p,q\in\mathbb{SP}(\textit{pACP}^+)\}\Big). \end{aligned}$$

Axiom CM4. We define a relation R in the following way:

$$\begin{aligned} R &= Eq\Big(\{((p+q)\between s, p\between s+q\between s) \,:\, p,q,s\in\mathbb{SP}(\textit{pACP}^+)\} \\ &\qquad \cup\{((u+v)\between s, u\between s+v\between s) \,:\, u,v\in\mathbb{DP}(\textit{pACP}^+), s\in\mathbb{SP}(\textit{pACP}^+)\}\Big). \end{aligned}$$

Suppose $\Big(((p+q)\between s),(p\between s+q\between s)\Big)\in R$ for some $p,q,s\in\mathbb{SP}(\textit{pACP}^+)$ and $M\in\mathbb{DP}(\textit{pACP}^+)/R$. Then

$$\begin{aligned} \mu((p+q)\between s,(u+v)\between s) &= \mu(p+q,u+v)=\mu(p,u)\cdot\mu(q,v) \\ &= \mu(p\between s,u\between s)\cdot\mu(q\between s,v\between s)=\mu(p\between s+q\between s,u\between s+v\between s). \end{aligned}$$

If $(u+v)\between s\in M$ then also $u\between s+v\between s\in M$ and the result $\mu((p+q)\between s,M)=\mu(p\between s+q\between s,M)$ follows from Proposition 3.3.10. Otherwise, $\mu((p+q)\between s,M)=\mu(p\between s+q\between s,M)=0$.

Axiom PrCM1. We define a relation R in the following way:

$$R=Eq\Big(\{((p\leftplus_\pi q)\between s, p\between s\leftplus_\pi q\between s) \,:\, p,q,s\in\mathbb{SP}(\textit{pACP}^+)\}\Big).$$

Suppose $\Big((p\leftplus_\pi q)\between s, p\between s\leftplus_\pi q\between s\Big)\in R$ for some $p,q,s\in\mathbb{SP}(\textit{pACP}^+)$ and $M\in\mathbb{DP}(\textit{pACP}^+)/R$. Then,

$$\begin{aligned} \mu((p\leftplus_\pi q)\between s,v\between s) &= \mu(p\leftplus_\pi q,v)=\pi\cdot\mu(p,v)+(1-\pi)\cdot\mu(q,v) \\ &= \pi\cdot\mu(p\between s,v\between s)+(1-\pi)\cdot\mu(q\between s,v\between s)=\mu(p\between s\leftplus_\pi q\between s,v\between s). \end{aligned}$$

If $v\between s\in M$ then the result $\mu((p\leftplus_\pi q)\between s,M)=\mu(p\between s\leftplus_\pi q\between s,M)$ follows from Proposition 3.3.10. Otherwise, $\mu((p\leftplus_\pi q)\between s,M)=\mu(p\between s\leftplus_\pi q\between s,M)=0$.

Axiom CM5. We define a relation R in the following way:

$$R=Eq\Big(\{(a\cdot p\mid b,c\cdot p),\ (\breve{a}\cdot p\mid\breve{b},\breve{c}\cdot p) \,:\, p\in\mathbb{SP}(\textit{pACP}^+),\gamma(a,b)=c\}\Big).$$

Axiom CM6. Relation R is defined in the following way:

$$R=Eq\Big(\{(a\mid b\cdot p,c\cdot p),\ (\breve{a}\mid\breve{b}\cdot p,\breve{c}\cdot p) \,:\, p\in\mathbb{SP}(\textit{pACP}^+),\gamma(a,b)=c\}\Big).$$

Axiom CM7. Relation R is defined in the following way:

$$R=Eq\Big(\{(a\cdot p\mid b\cdot q,c\cdot(p\parallel q)),\ (\breve{a}\cdot p\mid\breve{b}\cdot q,\breve{c}\cdot(p\parallel q)) \,:p,q\in\mathbb{SP}(\textit{pACP}^+),\gamma(a,b)=c\}\Big).$$

Axiom PrCM2. We define a relation R in the following way:

$$R = Eq\Big(\{((p \leftplus_\pi q) \mid s, p \mid s \leftplus_\pi q \mid s) \ : \ p, q, s \in \mathbb{SP}(\mathit{pACP}^+)\}\Big).$$

Suppose $\Big((p \leftplus_\pi q) \mid s, p \mid s \leftplus_\pi q \mid s\Big) \in R$ for some $p, q, s \in \mathbb{SP}(\mathit{pACP}^+)$ and $M \in \mathbb{DP}(\mathit{pACP}^+)/R$. Then

$$\begin{array}{rcl} \mu((p \leftplus_\pi q) \mid s, v \mid w) & = & \mu(p \leftplus_\pi q, v) \cdot \mu(s, w) = (\pi \cdot \mu(p, v) + (1 - \pi) \cdot \mu(q, v)) \cdot \mu(s, w) \\ & = & \pi \cdot \mu(p, v) \cdot \mu(s, w) + (1 - \pi) \cdot \mu(q, v) \cdot \mu(s, w) \\ & = & \mu(p \mid s \leftplus_\pi q \mid s, v \mid w). \end{array}$$

If $v \mid w \in M$ then $\mu((p \leftplus_\pi q) \mid s, M) = \mu(p \mid s \leftplus_\pi q \mid s, M)$ by use of Proposition 3.3.10. Otherwise, $\mu((p \leftplus_\pi q) \mid s, M) = \mu(p \mid s \leftplus_\pi q \mid s, M) = 0$.

Axiom PrCM3. Relation R is defined as:

$$R = Eq\Big(\{(p \mid (q \leftplus_\pi s), p \mid s \leftplus_\pi p \mid s) \ : \ p, q, s \in \mathbb{SP}(\mathit{pACP}^+)\}\Big).$$

and the proof is similar to the proof of PrCM2.

Axiom PrMM1. We define a relation R in the following way:

$$R = Eq\Big(\{(p \parallel q, (p, p) \between (q, q)) \ : \ p, q \in \mathbb{SP}(\mathit{pACP}^+)\}\Big).$$

Suppose that $\Big(p \parallel q, (p, p) \between (q, q)\Big) \in R$ for some $p, q \in \mathbb{SP}(\mathit{pACP}^+)$ and $M \in \mathbb{DP}(\mathit{pACP}^+)/R$. Then u is reachable from $p \parallel q$ and also from $(p, p) \between (q, q)$ if and only if $u \equiv v \between q + w \between p + v \mid w$ for some $v, w \in \mathbb{DP}(\mathit{pACP}^+)$ such that $p \rightsquigarrow v$ and $q \rightsquigarrow w$. From the definition of the PDF we have that

$$\mu(p \parallel q, u) = \mu(p, v) \cdot \mu(q, w) = \mu((p, p) \between (q, q), u).$$

Using Proposition 3.3.10 we obtain $\mu(p \parallel q, M) = \mu((p, p) \between (q, q), M)$ in case $u \in M$. In any other case $\mu(p \parallel q, M) = \mu((p, p) \between (q, q), M) = 0$.

Axiom PrMM2. We define a relation R in the following way:

$$R = Eq\Big(\{((p_1 \leftplus_\pi p_2, z) \between (q, w), (p_1, z) \between (q, w) \leftplus_\pi (p_2, z) \between (q, w)) : p_1, p_2, q, z, w \in \mathbb{SP}(\mathit{pACP}^+)\}\Big).$$

Suppose $\Big((p_1 \leftplus_\pi p_2, z) \between (q, w), (p_1, z) \between (q, w) \leftplus_\pi (p_2, z) \between (q, w)\Big) \in R$ for some p_1,p_2, q, z, $w \in \mathbb{SP}(\mathit{pACP}^+)$ and $M \in \mathbb{DP}(\mathit{pACP}^+)/R$. u is reachable from $(p_1 \leftplus_\pi p_2, z) \between (q, w)$ iff $(p_1, z) \between (q, w) \leftplus_\pi (p_2, z) \between (q, w)$. Then, $u \equiv x \between w + y \between z + x \mid y$ for some $x, y \in \mathbb{DP}(\mathit{pACP}^+)$ such that $p \rightsquigarrow x$ and $q \rightsquigarrow y$. From the definition of the PDF we have that

$$\mu((p_1 \leftplus_\pi p_2, z) \between (q, w), u) = \mu(p_1 \leftplus_\pi p_2, x) \cdot \mu(q, y) = (\pi \cdot \mu(p_1, x) + (1 - \pi) \cdot \mu(p_2, x)) \cdot \mu(q, y)$$

and

$$\begin{aligned}\mu((p_1,z)\between(q,w)\leftplus_\pi(p_2,z)\between(q,w),u) &= \pi\cdot\mu((p_1,z)\between(q,w),u)\\ &\quad+(1-\pi)\cdot\mu((p_2,z)\between(q,w),u)\\ &=\pi\cdot\mu(p_1,x)\cdot\mu(q,y)+(1-\pi)\cdot\mu(p_2,x)\cdot\mu(q,y).\end{aligned}$$

If $u\in M$, then we conclude that
$\mu((p_1\leftplus_\pi p_2,z)\between(q,w),M) = \mu((p_1,z)\between(q,w)\leftplus_\pi(p_2,z)\between(q,w),M)$ by use of Proposition 3.3.10. Otherwise
$\mu((p_1\leftplus_\pi p_2,z)\between(q,w),M)=\mu((p_1,z)\between(q,w)\leftplus_\pi(p_2,z)\between(q,w),M)=0$.

Axiom PrMM3. We define a relation R in the following way:

$$R=Eq\Big(\{((p,z)\between(q_1\leftplus_\pi q_2,w),(p,z)\between(q_1,w)\leftplus_\pi(p,z)\between(q_2,w)):\ p,q_1,q_2,z,w\in\mathbb{SP}(\mathit{pACP}^+)\}\Big).$$

The proof is similar to the previous one.

Axiom D1. Relation R is defined in the following way:

$$R=Eq\Big(\{(\partial_H(a),a),(\partial_H(\breve{a}),\breve{a})\ :\ a\notin H\}\Big)$$

Axiom D2. Relation R is defined in the following way:

$$R=Eq\Big(\{(\partial_H(a),\delta),(\partial_H(\breve{a}),\breve{\delta})\ :\ a\in H\}\Big)$$

Axiom D3. We define a relation R in the following way:

$$\begin{aligned}R\ =\ Eq\Big(&\{(\partial_H(p+q),\partial_H(p)+\partial_H(q))\ :\ p,q\in\mathbb{SP}(\mathit{pACP}^+)\}\\ &\cup\{(\partial_H(u+v),\partial_H(u)+\partial_H(v))\ :\ u,v\in\mathbb{DP}(\mathit{pACP}^+)\}\Big).\end{aligned}$$

Suppose that $(\partial_H(p+q),\partial_H(p)+\partial_H(q))\in R$ for some $p,q\in\mathbb{SP}(\mathit{pACP}^+)$ and $M\in\mathbb{DP}(\mathit{pACP}^+)/R$. Then,

$$\mu(\partial_H(p+q),\partial_H(u+v))=\mu(p+q,u+v)=\mu(p,u)\cdot\mu(q,v)$$

and

$$\mu(\partial_H(p)+\partial_H(q),\partial_H(u)+\partial_H(v))=\mu(p+q,u+v)=\mu(p,u)\cdot\mu(q,v).$$

If $\partial_H(u+v)\in M$ then also $\partial_H(u)+\partial_H(v)\in M$ and the result $\mu(\partial_H(p+q),M)=\mu(\partial_H(p)+\partial_H(q),M)$ follows from Proposition 3.3.10. Otherwise, $\mu(\partial_H(p+q),M)=\mu(\partial_H(p)+\partial_H(q),M)=0$.

Axiom D4. We define a relation R in the following way:

$$\begin{aligned}R\ =\ Eq\Big(&\{(\partial_H(p\cdot q),\partial_H(p)\cdot\partial_H(q))\ :\ p,q\in\mathbb{SP}(\mathit{pACP}^+)\}\\ &\{(\partial_H(u\cdot q),\partial_H(u)\cdot\partial_H(q))\ :\ u\in\mathbb{DP}(\mathit{pACP}^+),\ q\in\mathbb{SP}(\mathit{pACP}^+)\}\Big).\end{aligned}$$

Suppose that $(\partial_H(p\cdot q),\partial_H(p)\cdot\partial_H(q))\in R$ for some $p,q\in\mathbb{SP}(\mathit{pACP}^+)$ and $M\in\mathbb{DP}(\mathit{pACP}^+)/R$. Then, $\mu(\partial_H(p\cdot q),\partial_H(u\cdot q))=\mu(p\cdot q,u\cdot q)=\mu(p,u)=\mu(\partial_H(p),\partial_H(u))=\mu(\partial_H(p)\cdot\partial_H(q),\partial_H(u)\cdot\partial_H(q))$. The result follows from Proposition 3.3.10 since $\partial_H(u\cdot q)\in M$ iff $\partial_H(u)\cdot\partial_H(q)\in M$.

Axiom PrD5. We define a relation R in the following way:

$$R = Eq\Big(\{(\partial_H(p \leftthreetimes_\pi q), \partial_H(p) \leftthreetimes_\pi \partial_H(q)) \ : \ p, q \in \mathbb{SP}(\textit{pACP}^+)\}\Big).$$

Suppose $(\partial_H(p \leftthreetimes_\pi q), \partial_H(p) \leftthreetimes_\pi \partial_H(q)) \in R$ for some $p, q \in \mathbb{SP}(\textit{pACP}^+)$ and $M \in \mathbb{DP}(\textit{pACP}^+)/R$. Then,

$$\begin{aligned}\mu(\partial_H(p \leftthreetimes_\pi q), \partial_H(u)) &= \mu(p \leftthreetimes_\pi q, u) = \pi \cdot \mu(p, u) + (1-\pi) \cdot \mu(q, u) \\ &= \pi \cdot \mu(\partial_H(p), \partial_H(u)) + (1-\pi) \cdot \mu(\partial_H(q), \partial_H(u)) \\ &= \mu(\partial_H(p) \leftthreetimes_\pi \partial_H(q), \partial_H(u)).\end{aligned}$$

From Proposition 3.3.10 follows that $\mu(\partial_H(p \leftthreetimes_\pi q), M) = \mu(\partial_H(p) \leftthreetimes_\pi \partial_H(q), M)$ if $\partial_H(u) \in M$. Otherwise, $\mu(\partial_H(p \leftthreetimes_\pi q), M) = \mu(\partial_H(p) \leftthreetimes_\pi \partial_H(q), M) = 0$.

Axiom PrMM4. Let us suppose that $p, q, z, w \in \mathbb{SP}(\textit{pACP}^+)$ and $p \leftrightarrows p + p$ and $q \leftrightarrows q + q$ and let $\mathcal{RP}(p) = \{u : p \rightsquigarrow u\}$ and $\mathcal{RP}(q) = \{v : q \rightsquigarrow v\}$. From Lemma 4.3.17 *ii.* it follows that

for all $u_1, u_2 \in \mathcal{RP}(p)$, $u_1 \leftrightarrows u_2$ and $\mu(p, [u_1]_{\leftrightarrows}) = \mu(p, \mathcal{RP}(p)) = 1$ and

for all $v_1, v_2 \in \mathcal{RP}(q)$, $v_1 \leftrightarrows v_2$ and $\mu(q, [v_1]_{\leftrightarrows}) = \mu(q, \mathcal{RP}(q)) = 1$. (1)

We will prove that $(p, z) \between (q, w) \leftrightarrows p \between w + q \between z + p \,|\, q$.

Probabilistic transitions. Assume that $(p, z) \between (q, w) \rightsquigarrow x$. Then $x \equiv u \between w + v \between z + u \,|\, v$ for some $u \in \mathcal{RP}(p)$ and $v \in \mathcal{RP}(q)$. It follows directly that $p \between w + q \between z + p \,|\, q \rightsquigarrow u \between w + v \between z + u \,|\, v$. And $x \leftrightarrows x$.

Now assume that $p \between w + q \between z + p \,|\, q \rightsquigarrow x$. Then, $x \equiv u_1 \between w + v_1 \between z + u_2 \,|\, v_2$ and $u_1, u_2 \in \mathcal{RP}(p), v_1, v_2 \in \mathcal{RP}(q)$. We obtain that $(p, z) \between (q, w) \rightsquigarrow u_1 \between w + v_1 \between z + u_1 \,|\, v_1$. Moreover, since $u_1 \leftrightarrows u_2$ and $v_1 \leftrightarrows v_2$ according to the Congruence theorem (Theorem 4.3.15) we obtain $u_1 \between w + v_1 \between z + u_2 \,|\, v_2 \leftrightarrows u_1 \between w + v_1 \between z + u_1 \,|\, v_1$. (2)

Note that in both cases we obtained that the reachable dynamic processes are bisimilar - in the first case both processes reach the same process x, in the second case it is obtained due to the Congruence theorem. Therefore, no investigation on action transitions or action termination are necessary.

PDF. From the previous discussion about probabilistic transitions of $(p, z) \between (q, w)$ we have that the set of all reachable processes from this process is $N = \{u \between w + v \between z + u \,|\, v : u \in \mathcal{RP}(p), v \in \mathcal{RP}(q)\} = \mathcal{RP}(p)^z \parallel {}^w\mathcal{RP}(q)$. Moreover, if $n_1, n_2 \in N$ then $n_1 \leftrightarrows n_2$ (from (1)). And also, if $u \between w + v \between z + u \,|\, v \in N$ then $N \subseteq [u \between w + v \between z + u \,|\, v]_{\leftrightarrows}$. Finally, we obtain:

$$\begin{aligned}&\mu((p, z) \between (q, w), [u \between w + v \between z + u \,|\, v]_{\leftrightarrows}) \\ &\qquad = \mu((p, z) \between (q, w), N) = \mu((p, z) \between (q, w), \mathcal{RP}(p)^z \parallel {}^w\mathcal{RP}(q)) \\ &\qquad = \mu(p, \mathcal{RP}(p)) \cdot \mu(q, \mathcal{RP}(q)) = 1.\end{aligned}$$

Therefore, $\mu((p, z) \between (q, w), [u \between w + v \between z + u \,|\, v]_{\leftrightarrows}) = 1$ and for any other equivalence class $M \in \mathbb{DP}(\textit{pACP}^+)/\leftrightarrows$ we have that $\mu((p, z) \between (q, w), M) = 0$.

Now we discuss the set of reachable processes from $p \between w + q \between z + p \,|\, q$. Let this set be denoted by K. From the discussion about the probabilistic transitions of this process we conclude that $K = \{u \between w + v \between z + u_1 \,|\, v_1 : u, u_1 \in \mathcal{RP}(p), v, v_1 \in \mathcal{RP}(q)\}$. Moreover,

if $k_1, k_2 \in K$, then $k_1 \leftrightarrows k_2$. And also, if $u \between w + v \between z + u_1 \,|\, v_1 \in K$ then $K \subseteq [u \between w + v \between z + u_1 \,|\, v_1]_{\leftrightarrows}$. Therefore,

$$\begin{aligned}
&\mu(p \between w + q \between z + p \,|\, q, [u \between w + v \between z + u_1 \,|\, v_1]_{\leftrightarrows}) \\
&\quad = \mu(p \between w + q \between z + p \,|\, q, K) \\
&\quad = \mu(p \between w + q \between z + p \,|\, q, \bigcup_{u' \in \mathcal{RP}(p)} \bigcup_{v' \in \mathcal{RP}(q)} \bigcup_{u'_1 \in \mathcal{RP}(p)} \bigcup_{v'_1 \in \mathcal{RP}(q)} \{u' \between w + v' \between z + u'_1 \,|\, v'_1\}) \\
&\quad = \sum_{u' \in \mathcal{RP}(p)} \sum_{v' \in \mathcal{RP}(q)} \sum_{u'_1 \in \mathcal{RP}(p)} \sum_{v'_1 \in \mathcal{RP}(q)} \mu(p, u') \cdot \mu(q, v') \cdot \mu(p, u'_1) \cdot \mu(q, v'_1) \\
&\quad = \Big(\sum_{u' \in \mathcal{RP}(p)} \mu(p, u') \Big) \cdot \Big(\sum_{v' \in \mathcal{RP}(q)} \mu(p, v') \Big) \cdot \Big(\sum_{u'_1 \in \mathcal{RP}(p)} \mu(p, u'_1) \Big) \cdot \Big(\sum_{v'_1 \in \mathcal{RP}(q)} \mu(q, v'_1) \Big) \\
&\quad = 1.
\end{aligned}$$

Thus, $\mu(p \between w + q \between z + p \,|\, q, [u \between w + v \between z + u_1 \,|\, v_1]_{\leftrightarrows}) = 1$. For any other equivalence class $M \in \mathbb{DP}(\textit{pACP}^+)/\leftrightarrows$ we have that $\mu(p \between w + q \between z + p \,|\, q, M) = 0$.
Finally, from (2) it follows that $[u \between w + v \between z + u \,|\, v]_{\leftrightarrows} = [u \between w + v \between z + u_1 \,|\, v_1]_{\leftrightarrows}$. Hence,

$$\mu((p,z) \between (q,w), [u \between w + v \between z + u \,|\, v]_{\leftrightarrows}) = \mu(p \between w + q \between z + p \,|\, q, [u \between w + v \between z + u \,|\, v]_{\leftrightarrows}) = 1.$$

And, $\mu((p,z) \between (q,w), M) = \mu(p \between w + q \between z + p \,|\, q, M) = 0$ for all other $M \in \mathbb{DP}(\textit{pACP}^+)/\leftrightarrows$.

Axiom PrCM4. Let $s \in \mathbb{SP}(\textit{pACP}^+)$ such that $s \leftrightarrows s + s$ and $\mathcal{RP}(s) = \{w : s \rightsquigarrow w\}$. By Lemma 4.3.17*ii.* we have that for every $w_1, w_2 \in \mathcal{RP}(s)$, $w_1 \leftrightarrows w_2$ and $\mu(s, \mathcal{RP}(s)) = 1$. We will prove that for arbitrary $p, q \in \mathbb{SP}(\textit{pACP}^+)$, $(p + q) \,|\, s \leftrightarrows p \,|\, s + q \,|\, s$.

Probabilistic transitions. Suppose that $(p + q) \,|\, s \rightsquigarrow u$. We obtain that $u \equiv (v_1 + v_2) \,|\, w_1$ and $p \rightsquigarrow v_1, q \rightsquigarrow v_2, w_1 \in \mathcal{RP}(s)$. Then also $p \,|\, s + q \,|\, s \rightsquigarrow v_1 \,|\, w_1 + v_2 \,|\, w_1$. According to the definition of bisimulation relation we need to prove that
$(v_1 + v_2) \,|\, w_1 \leftrightarrows v_1 \,|\, w_1 + v_2 \,|\, w_1$. (3)
If $p \,|\, s + q \,|\, s \rightsquigarrow u$, then $u \equiv v_1 \,|\, w_1 + v_2 \,|\, w_2$ and $p \rightsquigarrow v_1, q \rightsquigarrow v_2, w_1, w_2 \in \mathcal{RP}(s)$. Then $(p + q) \,|\, s \rightsquigarrow (v_1 + v_2) \,|\, w_1$. Therefore, we need to prove that
$(v_1 + v_2) \,|\, w_1 \leftrightarrows v_1 \,|\, w_1 + v_2 \,|\, w_2$. (4)

Action transitions. One can see that (3) is a special case of (4), therefore it is sufficient to prove the case (4).

Suppose that $(v_1 + v_2) \,|\, w_1 \xrightarrow{a} p$ for some $a \in A$. Then for some $b, c \in A$ such that $\gamma(b, c) = a$ one of the following cases occurs: (1.) ((a.) $v_1 \xrightarrow{b} p_1$ or (b.) $v_2 \xrightarrow{b} p_1$) and $w_1 \xrightarrow{c} p_2$ and $p \equiv p_1 \between p_2$, or (2.) ((a.) $v_1 \xrightarrow{b} p$ or (b.) $v_2 \xrightarrow{b} p$) and $w_1 \xrightarrow{c} \surd$, or (3.) ((a.) $v_1 \xrightarrow{b} \surd$ or (b.) $v_2 \xrightarrow{b} \surd$) and $w_1 \xrightarrow{c} p$. Whenever $v_1 \,|\, w_1 \xrightarrow{a} p$ (cases 1.a., 2.a., 3.a.) it follows directly that $v_1 \,|\, w_1 + v_2 \,|\, w_2 \xrightarrow{a} p$ as well. In the other cases since $w_1 \leftrightarrows w_2$, we have that (1.b.) $w_2 \xrightarrow{c} p'_2$ and $p_2 \leftrightarrows p'_2$ and therefore $v_1 \,|\, w_1 + v_2 \,|\, w_2 \xrightarrow{a} p_1 \between p'_2$; moreover $p_1 \between p_2 \leftrightarrows p_1 \between p'_2$ according to the Congruence theorem; (2.b.) $w_2 \xrightarrow{c} p'$ and $p \leftrightarrows p'$ and $v_1 \,|\, p_1 + v_2 \,|\, w_2 \xrightarrow{a} p'$ and $p \leftrightarrows p'$; (3.b.) $w_2 \xrightarrow{c} \surd$ and $v_1 \,|\, w_1 + v_2 \,|\, w_2 \xrightarrow{a} p$.
Suppose that $v_1 \,|\, w_1 + v_2 \,|\, w_2 \xrightarrow{a} p$ for some $a \in A$. Then, for some $b, c \in A$ such that $\gamma(b, c) = a$ one of the following cases occurs: (1.) ((a.) $v_1 \xrightarrow{b} p_1$ and $w_1 \xrightarrow{c} p_2$ and $p \equiv p_1 \between p_2$ or (b.) $v_1 \xrightarrow{b} \surd$ and $w_1 \xrightarrow{c} p$ or (c.) $v_1 \xrightarrow{b} p$ and $w_1 \xrightarrow{c} \surd$) or (2.) ((a.)

$v_2 \xrightarrow{b} p_1$ and $w_2 \xrightarrow{c} p_2$ and $p \equiv p_1 \parallel p_2$ or (b.) $v_2 \xrightarrow{b} \surd$ and $w_2 \xrightarrow{c} p$ or (c.) $v_2 \xrightarrow{b} p$ and $w_2 \xrightarrow{c} \surd$). In the cases 1.a., 1.b. and 1.c. it follows directly that $(v_1 + v_2) \mid w_1 \xrightarrow{a} p$. For the other cases since $w_1 \leftrightarrow w_2$ it follows that (2.a.) $w_1 \xrightarrow{c} p_2'$ and $p_2 \leftrightarrow p_2'$ from which $(v_1 + v_2) \mid w_1 \xrightarrow{a} p_1 \parallel p_2'$ and $p_1 \parallel p_2 \leftrightarrow p_1 \parallel p_2'$; (2.b.) $w_1 \xrightarrow{c} p'$ and $p \leftrightarrow p'$; therefore $(v_1 + v_2) \mid w_1 \xrightarrow{a} p'$ and $p \leftrightarrow p'$; (2.c.) $w_1 \xrightarrow{c} \surd$ and $(v_1 + v_2) \mid w_1 \xrightarrow{a} p$.

Action termination. Suppose that $(v_1 + v_2) \mid w_1 \xrightarrow{a} \surd$ for some $a \in A$. Then for some $b, c \in A$ such that $\gamma(b, c) = a$ one of the following cases occurs: (1.) $v_1 \xrightarrow{b} \surd$ and $w_1 \xrightarrow{c} \surd$, or (2.) $v_2 \xrightarrow{b} \surd$ and $w_1 \xrightarrow{c} \surd$. In the first case it follows that $v_1 \mid w_1 \xrightarrow{a} \surd$ and therefore $v_1 \mid w_1 + v_2 \mid w_2 \xrightarrow{a} \surd$ as well. In the second case since $w_1 \leftrightarrow w_2$, we have that $w_2 \xrightarrow{c} \surd$. Then, $v_2 \mid w_2 \xrightarrow{a} \surd$ and also $v_1 \mid w_1 + v_2 \mid w_2 \xrightarrow{a} \surd$.

Suppose that $v_1 \mid w_1 + v_2 \mid w_2 \xrightarrow{a} \surd$ for some $a \in A$. Then, for some $b, c \in A$ such that $\gamma(b, c) = a$ one of the following cases occurs: (1.) $v_1 \xrightarrow{b} \surd$ and $w_1 \xrightarrow{c} \surd$ or (2.) $v_2 \xrightarrow{b} \surd$ and $w_2 \xrightarrow{c} \surd$. In the first case it follows directly that $v_1 + v_2 \xrightarrow{b} \surd$ and also $(v_1 + v_2) \mid w_1 \xrightarrow{a} \surd$. In the second case, since $w_1 \leftrightarrow w_2$ it follows that $w_1 \xrightarrow{c} \surd$. Since $v_1 + v_2 \xrightarrow{b} \surd$ we obtain that $(v_1 + v_2) \mid w_1 \xrightarrow{a} \surd$.

Herewith we proved (3) and (4) valid.

PDF. Now, let us suppose that $M \in \mathbb{DP}(pACP^+)/\leftrightarrow$. From (4) follows that $(v_1+v_2) \mid w_1 \in M$ iff $v_1 \mid w_1 + v_2 \mid w_2 \in M$ for some $w_1, w_2 \in \mathcal{RP}(s)$ and for some v_1 and v_2 such that $p \rightsquigarrow v_1$ and $q \rightsquigarrow v_2$. Moreover, the subset of M reachable from $(p + q) \mid s$ is contained in the set $K = ([v_1]_{\leftrightarrow} + [v_2]_{\leftrightarrow}) \mid \mathcal{RP}(s) \subset M$. And the subset of M reachable from $p \mid s + q \mid s$ is contained in the set $N = [v_1]_{\leftrightarrow} \mid \mathcal{RP}(s) + [v_2]_{\leftrightarrow} \mid \mathcal{RP}(s) \subset M$. Having that $\mu(s, \mathcal{RP}(s)) = 1$ we obtain:
$\mu((p + q) \mid s, M) = \mu((p + q) \mid s, K) = \mu(p, [v_1]_{\leftrightarrow}) \cdot \mu(q, [v_2]_{\leftrightarrow}) \cdot \mu(s, \mathcal{RP}(s))$
$= \mu(p, [v_1]_{\leftrightarrow}) \cdot \mu(q, [v_2]_{\leftrightarrow})$. And

$$\begin{aligned} \mu(p \mid s + q \mid s, M) &= \mu(p \mid s + q \mid s, N) \\ &= \mu(p, [v_1]_{\leftrightarrow}) \cdot \mu(s, \mathcal{RP}(s)) \cdot \mu(q, [v_2]_{\leftrightarrow}) \cdot \mu(s, \mathcal{RP}(s)) \\ &= \mu(p, [v_1]_{\leftrightarrow}) \cdot \mu(q, [v_2]_{\leftrightarrow}). \end{aligned}$$

Thus, for a reachable class M we obtain that $\mu((p + q) \mid s, M) = \mu(p \mid s + q \mid s, M)$. If M is not reachable from $(p+q) \mid s$ and $p \mid s+q \mid s$, then $\mu((p+q) \mid s, M) = \mu(p \mid s+q \mid s) = 0$.

Axiom PrCM5. In a similar way like the proof of PrCM4.

□

Completeness theorem

In order to prove the completeness property of $pACP^+$ with respect to the bisimulation model we use Verhoef's method as described in Section 2.3.

Lemma 4.3.19. (Conservativity of $\mathbf{T}_{pACP^+}$ with respect to $\mathbf{T}_{pBPA}$) The term-deduction system $\mathbf{T}_{pACP^+}$ is an operationally conservative extension of the term-deduction system $\mathbf{T}_{pBPA}$. □

Proof. In order to prove conservativity it is sufficient to verify the following condition:

- $\mathbf{T}_{pBPA}$ is pure , well-founded term-deduction system in path format;

- $\mathbf{T}_{pACP^+}$ is a term-deduction system in path format;

- $\mathbf{T}_{pBPA} \oplus \mathbf{T}_{pACP^+}$ is defined;

- There are no conclusions $s \xrightarrow{a} t$ or $s \xrightarrow{a} \surd$ of a rule in $\mathbf{T}_(pACP^+)$ such that $s = x$ or $s = f(x_1, \ldots, x_n)$ for some operator f of *pBPA*.

That all these properties hold can be trivially checked from the relevant definitions. □

Lemma 4.3.20. The term-deduction system $\mathbf{T}_{pACP^+}$ is an operationally conservative extension up to the probabilistic bisimulation of the term-deduction system $\mathbf{T}_{pBPA}$.

Proof. In order to prove that $\mathbf{T}_{pACP^+}$ is an operationally conservative extension up to the probabilistic bisimulation with respect to $\mathbf{T}_{pBPA}$ we need to check that the probabilistic bisimulation equivalence is defined in terms of predicate and relation symbols. Apart from the fourth clause in Definition 3.3.11, probabilistic bisimulation is defined in terms of predicate and relation symbols. Hence, from the previous result for operationally conservative extension (Lemma 4.3.19) we obtain that for each closed *pBPA* term s, its term-relation-predicate diagrams in both $\mathbf{T}_{pBPA}$ and $\mathbf{T}_{pACP^+}$ are the same. Moreover, for these terms the probability distribution function is defined in the same way in both $\mathbf{T}_{pBPA}$ and $\mathbf{T}_{pACP^+}$ (Definition 3.3.14 and Definition 4.3.4), which provides us with a conclusion that the fourth clause in Definition 3.3.11 does not disturb the notion of the probabilistic bisimulation defined only in terms of predicate and relation symbols. □

Lemma 4.3.21. (Conservativity of *pACP*$^+$ with respect to *pBPA*) *pACP*$^+$ is an equationally conservative extension of *pBPA*, that is, if t and s are closed *pBPA* terms, then *pBPA* $\vdash t = s \Leftrightarrow$ *pACP*$^+ \vdash t = s$.

Proof. According to the used method the conclusion follows from the facts that:

- $\mathbf{T}_{pACP^+}$ is an operationally conservative extension of $\mathbf{T}_{pBPA}$ up to probabilistic bisimulation (see Lemma 4.3.21);

- *pBPA* is a complete axiomatization with respect to the bisimulation model (see Theorem 3.3.60);

- $\mathbf{T}_{pACP^+}$ with respect to the probabilistic bisimulation equivalence induces a model of *pACP*$^+$ (see Theorem 4.3.18).

□

Theorem 4.3.22 (*Completeness theorem for pACP*$^+$). If t and s are closed *pACP*$^+$ terms, then $\mathcal{M}_{pACP^+} \vdash t \underline{\leftrightarrow} s \Rightarrow$ *pACP*$^+ \vdash t = s$.

Proof. Completeness follows immediately from the following results:

- *pACP*$^+$ has the elimination property for *pBPA* (see Theorem 4.2.5);

- *pACP*$^+$ is an equationally conservative extension of *pBPA* (see Lemma 4.3.21).

□

4.4 Alternative definition of parallel composition

Here we give an axiom system that can be considered as equivalent to *pACP*$^+$ in the sense that a equation of terms that do not contain $\between$, $\mid$ and $\blacktriangleleft$ operators holds in one theory if and only if it holds in the other theory. The main idea for proposing a new axiom system is to find an appropriate theory which does not have any extra operators. As it has been already mentioned, in order to obtain a finite axiomatization of the parallel composition operator in the previous section we introduced the merge with memory operator $\blacktriangleleft$.

We denote the new process algebra by *pACP*. The signature of *pACP* consists of the operators of *pBPA*, three binary operators: $\parallel$, $\between$ and $\mid$ and an unary operator ∂_H with $H \subseteq A$. The axioms about the merge operator (without the auxiliary operator $\blacktriangleleft$) are given in Table 4.8. The axioms for the other operators are the same as in *pACP*$^+$ except that the axioms $PrCM1$, $PrCM2$ and $PrCM3$ are not included. The distributive laws of $\between$ and $\mid$ with respect to $\dot{+}_\pi$ are not needed anymore (this is exactly what these axioms express), because they are integrated in the axioms of the merge operator. Of course as a result of this, if we consider *pACP* as an extension of *pBPA* then it does not have the elimination property for *pBPA* because $\between$ and $\mid$ cannot be eliminated.

$x \parallel y$	=	$x \between y + y \between x + x \mid y$
$(x \dot{+}_\pi x') \between z + y \between w + (x \dot{+}_\pi x') \mid y$	=	$(x \between z + y \between w + x \mid y) \dot{+}_\pi (x' \between z + y \between w + x' \mid y)$
$x \between z + (y \dot{+}_\pi y') \between w + x \mid (y \dot{+}_\pi y')$	=	$(x \between z + y \between w + x \mid y) \dot{+}_\pi (x \between z + y' \between w + x \mid y')$

Table 4.8: Additional axioms for *pACP*.

Without proving it, we claim that equations $p \parallel q = s$, for some *pBPA* closed terms p, q and s, is derivable in *pACP*$^+$ if and only if the same equation is derivable in *pACP*.

4.5 Another viewpoint to parallel composition

It is quite common when a new feature is added to a standard process algebra (whatever type it is: *ACP*, CCS, CSP, $LOTOS$ etc.) one tries to stay as close as possible to the underlying axiomatization and operational semantics. Especially in the framework of *ACP* it is an important issue to keep the key axiom of parallel composition expressing the interleaving reasoning. The process algebra *pACP*$^+$ presented in the previous section does *not* contain this axiom, but we can see that $PrMM4$ is a restricted variant of it. Now we will present a process algebra with a parallel composition, denoted *ACP*$_\pi$, which is an extension of *pBPA* (so it has a notion of probability) and has the axiom

$$x \parallel y = x \between y + y \between x + x \mid y \qquad CM1$$

in the unrestricted form. (The detailed work on this axiomatization can be found in [8].) But we will show by means of an example that our attempt to have a simple axiom that is very close to *ACP* leads to contraintuitive results.

Let us repeat again that we want to construct a probabilistic process algebra which has the axiom $x \parallel y = x \between y + y \between x + x \mid y$ without any restriction. Thus, we define *ACP*$_\pi$ in the following way: the signature of *ACP*$_\pi$ consists of the operators of *pBPA*, the three merge operators: $\parallel$, $\between$ and $\mid$ and the encapsulation operator ∂_H with $H \subseteq A$. *ACP*$_\pi$ is parametrized by a communication function $\gamma : A_\delta \times A_\delta \to A_\delta$. The set of axioms of *ACP*$_\pi$ consists of the axioms of *pBPA* and axiom $CM1$

given above and the axioms given in Table 4.3 and 4.4. Therefore, ACP_π does not have any additional operator. The axiom system is quite simple and close to *ACP*. For the same reason as explained in Section 4.2, the distribution laws of $\mid$ with respect to $+$ are in a restricted form. Note that ACP_π has the elimination property for *pBPA*, if the set of basic terms is defined by Definition 3.2.19 [8].

Operational semantics of ACP_π Next, we present the operational semantics of ACP_π which induces the bisimulation model of the process algebra. We give only the deduction rules, and the full construction of the model can be found in [8]. The operational semantics of ACP_π is given by the term-deduction system $\mathbf{T}_{ACP_\pi} = (\breve{\Sigma}_{ACP_\pi}, \mathbf{DR}_{ACP_\pi})$ with $\breve{\Sigma}_{ACP_\pi} = (A_\delta \cup \breve{A}_\delta, +, \cdot, \leftthreetimes_\pi, \parallel, \lfloor\!\lfloor, \mid, \partial_H)$ and with the deduction rules for *pBPA* (defined on page 77), the rule for the merge operator in Table 4.9, the deduction rules for probabilistic transitions of the left merge, the communication merge and the encapsulation operator in Table 4.5 and the rules for action transitions in Table 4.6. The definition of $\mathbb{SP}(ACP_\pi)$ and $\mathbb{DP}(ACP_\pi)$ can easily be obtained following the pattern in Section 3.3.1. The PDF function μ on $\mathbb{PT}(ACP_\pi)$ is defined by Definition 4.5.1 and the probabilistic bisimulation relation on $\mathbb{PT}(ACP_\pi)$ is defined by Definition 3.3.11 when PA is replaced by ACP_π.

$$\frac{x \rightsquigarrow x', y \rightsquigarrow y', x \rightsquigarrow x'', y \rightsquigarrow y''}{x \parallel y \rightsquigarrow x' \lfloor\!\lfloor y + y' \lfloor\!\lfloor x + x'' \mid y''}$$

Table 4.9: Rules for the merge operator in ACP_π.

Definition 4.5.1. (PDF for ACP_π) A probability distribution function on $\mathbb{PT}(ACP_\pi)$ is defined by the equalities in Table 3.6, 3.7 and 4.10.

$\mu(x \parallel y, x' \lfloor\!\lfloor y + y' \lfloor\!\lfloor x + x'' \mid y'')$	$=$	$\mu(x,x') \cdot \mu(y,y') \cdot \mu(x,x'') \cdot \mu(y,y'')$	
$\mu(x \lfloor\!\lfloor y, x' \lfloor\!\lfloor y)$	$=$	$\mu(x,x')$	
$\mu(x \mid y, x' \mid y')$	$=$	$\mu(x,x') \cdot \mu(y,y')$	
$\mu(\partial_H(x), \partial_H(x'))$	$=$	$\mu(x,x')$	
$\mu(x,u)$	$=$	0	$otherwise$

Table 4.10: Equalities that defined PDF's for ACP_π (part 3 - parallel composition)

Differences with *pACP*$^+$ Thus, now we have two extensions of *pBPA*, both with a notion of probabilistic choice and parallel composition. The main differences between the two process algebras appear in the axioms and the deduction rules of the $\parallel$ operator. The axioms and the deduction rules for the other operators are common for both systems. So, *pACP*$^+$ has a more complex axiom system than ACP_π, but it has a simple and intuitively clear operational semantics. In both systems the interleaving approach to parallel composition is followed and the choice of the process which executes the next action is considered to be non-deterministic. But the "moment" when two parallel processes may interleave makes these systems different. Intuitively, in *pACP*$^+$ the interleaving between two parallel processes can take place only if they do not have unresolved probabilistic choice (in our terminology, they are trivial probabilistic processes). In order to have a finite axiomatization, we introduced an

auxiliary operator $]\![$. In ACP_π the interleaving of two parallel processes can take place "immediately", which is expressed by the unrestricted axiom: $x \parallel y = x \between y + y \between x + x \mid y$. But by applying this axiom, informally speaking, we produce copies of x (y) and each of them may contain an unresolved probabilistic choice. In other words, on the right-hand side of the axioms the two occurrences of x, one in $x \between y$ and the second in $x \mid y$, become independent processes which resolve their internal probabilistic choice (if any) independently. This means that the outcomes of the two probabilistic choices may differ (see also the deduction rule of the $\parallel$ operator and the definition of the PDF function). But the component x on the left-hand side of the axiom cannot have two different outcomes of its probabilistic choice[1]. Thus, this scenario has to be prevented from appearing. The solution we proposed is actually *pACP*$^+$.

Why it does not work! The approach used in ACP_π does not give the anticipated results for some concurrent probabilistic processes. This is illustrate by the following example.

Consider the processes $P \equiv send_1$ and $Q \equiv read_1 \leftarrow\!\!\!\!\!\!+_\pi fail$. Process P executes the action $send_1$ which may be treated as "send a datum at port 1". Process Q executes the action $read_1$ with probability π, that is, with probability π it reads a datum at port 1, or it fails with probability $1 - \pi$ and no further communications with process P are possible. We remark that this situation is real if communication is carried out via an unreliable transmission channel. Communication of P and Q is defined by a communication action $comm_1 = send_1 \mid read_1$. Intuitively, we expect that the behaviour of the whole system $\partial_H(P \parallel Q)$, for $H = \{send_1, read_1\}$, is expressed by the term $comm_1 \leftarrow\!\!\!\!\!\!+_\pi fail \cdot \delta$. But in ACP_π we obtain the following expression:

$$ACP_\pi \vdash \partial_H(P \parallel Q) = \partial_H(P \between Q + Q \between P + P \mid Q) = \delta + (\delta \leftarrow\!\!\!\!\!\!+_\pi fail \cdot \delta) + (comm_1 \leftarrow\!\!\!\!\!\!+_\pi \delta)$$
$$= comm_1 \leftarrow\!\!\!\!\!\!+_{\pi^2} fail \cdot \delta \leftarrow\!\!\!\!\!\!+_{(1-\pi)^2} (fail \cdot \delta + comm_1) \leftarrow\!\!\!\!\!\!+_{(1-\pi)\pi} \delta.$$

There is a scenario in which non-deterministic choice between the probabilistically dependent processes $fail$ and $comm_1$ arises. Moreover, there is a non-zero probability with which deadlock may occur. It is obvious that this process does not meet our intuition about the behaviour of the given parallel system.

[1] This is very similar to the situation with the idempotency law $A3$, whose restricted version $AA3$ is taken in *pBPA*.

Chapter 5

Probabilistic process algebra with discrete time

5.1 Introduction

The need to model timing aspects and to involve timed behaviour in the specification and the verification of concurrent systems has been widely accepted and explored in the framework of formal methods. Simultaneously introducing time and probability provides a new aspect to the specification and verification of concurrent systems. It allows more accurate modelling of timing behaviour and unreliability which in standard methods usually are encoded by alternative composition. Since one of the main issues in probabilistic methods is resolving non-determinism, combining time and probability can lead to a desired specification of a system which is free of non-determinism (see the example in Chapter 7).

In this chapter, we propose an extension of the probabilistic process algebras introduced in Chapter 3 and 4 with time features, which can be used to model both probabilistic and timing behaviour of systems. We consider a *discrete-time extension*, namely, time is introduced by cutting it up into a countably infinite number of time slices. Timing of actions is done with respect to the time slice in which they are executed. Furthermore, we do not assume that an absolute clock exists, but the moment when an action occurs is measured with respect to the previous action. This gives the relative aspect of timing. Thus, we end up with a discrete relative time version of probabilistic process algebra. In this chapter, we actually present three different process algebras built up in a modular way. First, we extend *pBPA* with constants that denote undelayable actions, actions that can be executed only in the time slice they are initialized in. To make the passage of time explicit, the time unit delay operator is introduced. In order to cope with more complex systems it is necessary to extend this algebra by constants that represent processes which can be initialized in the current or any future time slice. Thus, we end up with another timing extension of *pBPA* (Section 5.2.2).

Next, to the process algebra from Section 5.2.2 a notion of parallel composition and communication is added, following the same approach taken in Chapter 4. However, in order to obtain a finite axiomatization and clear deduction rules in the proposed time extension of $pACP^+$ we add an extra operator whose role will be explained later.

5.2 Basic Probabilistic Process Algebra with discrete relative time

In the next section, we present two basic probabilistic process algebras with discrete relative time. The first process algebra, $pBPA^{-}_{drt}$ does not have a notion of delayable actions. It means that processes presented by the terms of this algebra are either undelayable, their execution starts within the current time slice, or delayable but only for a finite (determined) number of time slices. The second process algebra, $pBPA_{drt}$, is an extension of $pBPA^{-}_{drt}$ and it is obtained by adding new constants denoting delayable actions and axioms that define equalities between delayable processes.

5.2.1 Probabilistic process algebra with undelayable actions

Basic Probabilistic Process Algebra with discrete relative time, $pBPA^{-}_{drt}$, for a certain set of atomic actions A has the signature that consists of: constants $\underline{\underline{a}}$ for $a \in A$ and $\underline{\underline{\delta}}$ for $\delta \notin A$, the operators of *pBPA*: $+$, $\cdot$ and $\leftthreetimes_\pi$ for $\pi \in \langle 0, 1\rangle$ and the unary (time) operators: σ_{rel} *one unit delay operator* and ν_{rel} *"now" operator*. The axioms of $pBPA^{-}_{drt}$ are shown in Table 3.1+5.1+5.2.

$x + y$	=	$y + x$	$A1$
$(x + y) + z$	=	$x + (y + z)$	$A2$
$\underline{\underline{a}} + \underline{\underline{a}}$	=	$\underline{\underline{a}}$	$DRTAA3$
$(x + y) \cdot z$	=	$x \cdot z + y \cdot z$	$A4$
$(x \leftthreetimes_\pi y) + z$	=	$(x + z) \leftthreetimes_\pi (y + z)$	$PrAC5$
$\sigma_{rel}(x) + \sigma_{rel}(y)$	=	$\sigma_{rel}(x + y)$	$DRT1$
$\sigma_{rel}(x) \cdot y$	=	$\sigma_{rel}(x \cdot y)$	$DRT2$
$\nu_{rel}(\underline{\underline{a}})$	=	$\underline{\underline{a}}$	$DCS1$
$\nu_{rel}(x + y)$	=	$\nu_{rel}(x) + \nu_{rel}(y)$	$DCS2$
$\nu_{rel}(x \cdot y)$	=	$\nu_{rel}(x) \cdot y$	$DCS3$
$\nu_{rel}(\sigma_{rel}(x))$	=	$\underline{\underline{\delta}}$	$DCS4$
$x + \underline{\underline{\delta}}$	=	x	$DRT3$
$\underline{\underline{\delta}} \cdot x$	=	$\underline{\underline{\delta}}$	$DRT4$

Table 5.1: Axioms of $pBPA^{-}_{drt}$ - part 1.

$\sigma_{rel}(x \leftthreetimes_\pi y)$	=	$\sigma_{rel}(x) \leftthreetimes_\pi \sigma_{rel}(y)$	$PrDRT1$
$\nu_{rel}(x \leftthreetimes_\pi y)$	=	$\nu_{rel}(x) \leftthreetimes_\pi \nu_{rel}(y)$	$PrDCS1$

Table 5.2: Probabilities and time operators.

For a given set of atomic actions A, a constant $\underline{\underline{a}}$ (for $a \in A$) denotes a process that with probability 1 executes action a within the current time slice and then terminates. $\underline{\underline{\delta}}$ denotes a process, called

undelayable deadlock, that with probability 1 deadlocks in the current time slice. The "time" operator $\sigma_{rel}(p)$ represents a process which behaves exactly like p but its initialization is postponed for one time slice. In that way, this operator makes the passage of time explicit. The other time operator ν_{rel} is used to expand the concept of "undelayable" activities from the set of atomic action over the set of processes in general. Namely, term $\nu_{rel}(p)$ represents a process that has to start its activities before the next time slice starts (if there are some) and at the same time the operator blocks all activities which p can perform but which are executable from the next time slice on (axiom $DCS4$). We shortly denote $\underline{\underline{A}}_\delta = \{\underline{\underline{a}} : a \in A_\delta\}$ and $\underline{\underline{A}} = \{\underline{\underline{a}} : a \in A\}$.

Axiom $PrDRT1$ needs some explanation. For probabilistic choice as well as for non-deterministic choice we use the concept of weak time factorization which says that *time passing does not determine a choice* (otherwise we deal with stochastic processes which is not an issue in this thesis). If both processes in probabilistic choice can idle to the next time slice then the moment when the choice is made does not affect the outcome of the choice. Let us consider the following processes: $\sigma_{rel}(\underline{\underline{a}}) \leftplus_\pi \sigma_{rel}(\underline{\underline{b}})$ and $\sigma_{rel}(\underline{\underline{a}} \leftplus_\pi \underline{\underline{b}})$. In the first process the probabilistic choice is resolved within the current time slice. After that a time tick occurs and then, in the second time slice, action a is executed with probability π and action b is executed with probability $1 - \pi$. The second process idles one time slice and then the probabilistic choice is resolved. Again, in the second time slice action a appears with probability π and action b with probability $1 - \pi$. To conclude, from the observational point of view these processes behave in the same way, in the next time slice both of them execute a with probability π and b with probability $1 - \pi$.

$DRT2$ and $DCS3$ express the relative timing approach. The time slice in which a certain action is performed is relative to the time at which the preceding action is performed. In the discrete-time setting with absolute timing these axioms are not valid [24].

5.2.2 Probabilistic process algebra with delayable actions

$pBPA^-_{drt}$ contains atomic actions that must be executed in the current time slice. If communication between such atomic actions does not occur in the current time slice the system ends in deadlock, provided there is no other alternative of course. Obviously, using the σ_{rel} operator the execution of a process may be delayed but only for a finite and fixed number of time slices. In specification of parallel systems usually communication is initiated by one of two processes that communicate and the other process is supposed to be ready at any moment to complete the communication. For example, in a communicating system Sender - Receiver, the Receiver should be always ready to accept a job sent by the Sender. Thus the communication is controlled and initiated by the Sender and this process can clearly be specified by undelayable atomic actions. The Receiver cannot be specified in $pBPA^-_{drt}$ since no infinite sum is permitted. Therefore, we need more powerful syntax to handle these type of processes.

In this section, we extend the signature by new constants denoted by a, b, c, ... which mean intuitively "with probability 1 process a executes the atomic action a (or b or c) in an arbitrary time slice and terminates after the execution" (axiom $a = \underline{\underline{a}} + \sigma_{rel}(a)$). We call these atomic actions *delayable*. Correspondingly, we introduce the constant δ meaning delayable deadlock (livelock), the process which with probability 1 can idle indefinitely, but nothing else (axiom $\delta = \underline{\underline{\delta}} + \sigma_{rel}(\delta)$).

Thus, we obtain the Basic Probabilistic Process Algebra with discrete relative time and delayable actions, $pBPA_{drt}$, with the signature that contains the constants and operators of $pBPA^-_{drt}$ and the new constants: a for each $a \in A$ (delayable atomic actions) and a special constant $\delta, \delta \notin A$ (delayable deadlock). The axioms for the new constants are given in Table 5.3 ($a \in A_\delta$). Together with the axioms of $pBPA^-_{drt}$, they make the axiomatization of $pBPA_{drt}$ (Tables 3.1+5.1+5.2+5.3).

$a = \underline{\underline{a}} + \sigma_{rel}(a)$			$RSPDA1$
$y = \underline{\underline{a}} + \sigma_{rel}(y)$	$\Rightarrow$	$y = a$	$RSPDA2$
$y = \underline{\underline{a}} \cdot x + \sigma_{rel}(y)$	$\Rightarrow$	$y = a \cdot x$	$RSPDA3$
$z = z + z \;\&\; y = \underline{\underline{a}} + \nu_{rel}(z) + \sigma_{rel}(y) \;\&\; y_1 = \nu_{rel}(z) + \sigma_{rel}(y_1)$	$\Rightarrow$	$y = a + y_1$	$RSPDA4$
$z = z + z \;\&\; y = \underline{\underline{a}} \cdot x + \nu_{rel}(z) + \sigma_{rel}(y) \;\&\; y_1 = \nu_{rel}(z) + \sigma_{rel}(y_1)$	$\Rightarrow$	$y = a \cdot x + y_1$	$RSPDA5$

Table 5.3: Axioms for delayable actions and processes.

Among the axioms in Table 5.3 only one, $RSPDA1$, is given as an equality. It expresses that delayable a behaves like $\underline{\underline{a}}$ but it can also postpone its activities for an arbitrary number of time steps after which it has the same behaviour. The other conditional axioms for delayable processes in Table 5.3 enable the derivation of certain equalities that cannot be derived from the axioms of $pBPA^{-}_{drt}$+$RSPDA1$. Axioms $RSPDA2$ and $RSPDA3$ give the general form of the terms considered equal to a and $a \cdot t$ respectively. Axioms $RSPDA4$ and $RSPDA5$ are used to derive equalities between more complex terms as shown by the following example.

Example 5.2.1. By this example we show the need of axioms $RSPDA1 - RSPDA5$. First, we will prove that $pBPA_{drt} \vdash a+a = a$. $pBPA_{drt} \vdash a+a = (\underline{\underline{a}}+\sigma_{rel}(a))+(\underline{\underline{a}}+\sigma_{rel}(a)) = (\underline{\underline{a}}+\underline{\underline{a}})+\sigma_{rel}(a+a) = \underline{\underline{a}} + \sigma_{rel}(a+a)$ and from $RSPDA2$ we obtain $pBPA_{drt} \vdash a + a = a$;

Next, assume that z is a closed $pBPA_{drt}$ term such that $z = z + z$ and let x, y and w be defined as: $x = \underline{\underline{a}} + \nu_{rel}(z) + \sigma_{rel}(x)$, $y = \underline{\underline{b}} + \sigma_{rel}(y)$ and $w = \underline{\underline{a}} + \underline{\underline{b}} + \nu_{rel}(z) + \sigma_{rel}(w)$. Informally, x denotes a process that at any moment can behave like $\underline{\underline{a}}$ or $\nu_{rel}(z)$. y is a process that can execute b at any moment. w is process that at any time slice can either execute a, b or it behaves like z. Clearly, w should be equal to $x+y$. But using the axioms of $pBPA^{-}_{drt}$ we cannot prove that $w = x+y$. In $pBPA_{drt}$ we have: $w = \underline{\underline{a}}+\underline{\underline{b}}+\nu_{rel}(z)+\sigma_{rel}(w) \stackrel{A1}{=} \underline{\underline{b}}+\underline{\underline{a}}+\nu_{rel}(z)+\sigma_{rel}(w)$ and since $x = \underline{\underline{a}}+\nu_{rel}(z)+\sigma_{rel}(x)$ it follows from $RSPDA4$ that $w = b+x$. From $RSPDA1$ it follows that $y = b$ from which $w = x+y$. □

Compared with the previous work on ACP-like discrete-time process algebras [20, 108, 24] we have introduced here delayable atomic actions only, like in [19], but not additional operators meant to generalize the concept of delayable actions over more complex processes (for instance, the unbounded delayable time operator or the iterated delay operator used in the discrete time extensions of *ACP* mentioned above). Thus, while $pBPA^{-}_{drt}$ is an extension of $BPA^{-}_{drt} - ID$ in [108] with probabilities, $pBPA_{drt}$ does not make an extension of $BPA_{drt} - ID$[1] [108] although they both deal with delayable processes. The difference is the definition of delayable processes. While [108] besides delayable actions uses the unbounded delay operator to define delayable processes in a more general sense, here we have only delayable action and more complex delayable processes are defined by conditional axioms. We do so in order to obtain a simpler process algebra. Combining the probabilistic choice operator and the operator used in the cited literature leads to a much more complicated axiomatization[2].

[1]Here, we use a shorter notation, that is, we omit the extension $-ID$ since it does not have any meaning in our setting. In [108] a constant denoting a catastrophic (immediate) deadlock is introduced, and the extension $-ID$ denotes the absence of that constant in the considered algebra.

[2]For example one problem which appears is: how to apply this operator on $\underline{\underline{a}} \,\overline{\sqcup}_{\pi}\, \underline{\underline{b}}$ and what is the meaning of that process. In other words, we cannot introduce the unbounded delay operator in the signature because we do not have a clear interpretation of applying it to probabilistic processes. It brings us to a similar situation as the one described in Example 5.2.2

By the next example we clarify the reason of adding the condition $z = z + z$ in the conditional axioms.

Example 5.2.2. Let x be such that $x = (\underline{\underline{a}} \leftplus_\pi \underline{\underline{b}}) + \sigma_{rel}(x)$ holds. From this equation we can derive:
$x = (\underline{\underline{a}} \leftplus_\pi \underline{\underline{b}}) + \sigma_{rel}((\underline{\underline{a}} \leftplus_\pi \underline{\underline{b}}) + \sigma_{rel}(x)) = (\underline{\underline{a}} \leftplus_\pi \underline{\underline{b}}) + \sigma_{rel}(\underline{\underline{a}} \leftplus_\pi \underline{\underline{b}}) + \sigma^2_{rel}(x))$
$= \big((\underline{\underline{a}} + \sigma_{rel}(\underline{\underline{a}})) \leftplus_{\pi^2} (\underline{\underline{b}} + \sigma_{rel}(\underline{\underline{a}})) \leftplus_{(1-\pi)\cdot\pi} (\underline{\underline{a}} + \sigma_{rel}(\underline{\underline{b}})) \leftplus_{\pi\cdot(1-\pi)} (\underline{\underline{b}} + \sigma_{rel}(\underline{\underline{b}}))\big) + \sigma^2_{rel}(x) = \ldots$
and if we go further on by each step we get more summands for which $PrAC5$ can be applied. Since this procedure of "unwinding" x is infinite, by each step new summands are added to the alternative compositions inside the brackets. This leads to an infinite sum which we do not permit. But also it expresses that x is a process with probability distribution over an infinite set of processes which lies beyond our restrictions. □

5.2.3 Properties of *pBPA*$_{drt}$

In this section, we present several properties of *pBPA*$_{drt}$. First we define the set of basic terms of this algebra in a similar way as we did for *pBPA*. Then, we show that using the axioms every basic term can be rewritten into a term with a special form. These forms will be used in the proof of the elimination property. We remark that Proposition 3.2.14 and 3.2.15 remain valid in *pBPA*$_{drt}$.

Basic terms

Next we define the set of basic terms in *pBPA*$_{drt}$. Later we prove the elimination property which expresses that every closed term is equal to a basic term.

Definition 5.2.3. The set of basic terms of *pBPA*$_{drt}$, $\mathcal{B}$(*pBPA*$_{drt}$), is defined inductively, with the help of an intermediary set $\mathcal{B}_+$(*pBPA*$_{drt}$) $\subseteq \mathcal{B}$(*pBPA*$_{drt}$) in a similar way as was done in the definition of basic terms of *pBPA*.

1. $\underline{\underline{A}} \cup \{\underline{\underline{\delta}}\} \subseteq \mathcal{B}_+(pBPA_{drt}) \subset \mathcal{B}(pBPA_{drt})$;
2. $A \cup \{\delta\} \subseteq \mathcal{B}_+(pBPA_{drt}) \subset \mathcal{B}(pBPA_{drt})$;
3. $a \in A,\ t \in \mathcal{B}(pBPA_{drt}) \Rightarrow \underline{\underline{a}} \cdot t, a \cdot t \in \mathcal{B}_+(pBPA_{drt})$;
4. $t, s \in \mathcal{B}_+(pBPA_{drt}) \Rightarrow t + s \in \mathcal{B}_+(pBPA_{drt})$;
5. $t \in \mathcal{B}_+(pBPA_{drt}) \Rightarrow \sigma_{rel}(t) \in \mathcal{B}_+(pBPA_{drt})$;
6. $t, s \in \mathcal{B}(pBPA_{drt}) \Rightarrow t \leftplus_\pi s \in \mathcal{B}(pBPA_{drt})$ for every $\pi \in \langle 0, 1\rangle$.

Remark 5.2.4. If we consider terms that only differ in the order of the summands to be identical (i.e. we work modulo axioms $A1$, $A2$, $PrAC1$ and $PrAC2$) the basic terms are exactly the terms of the form:

$$x \in \mathcal{B}_+ \text{ and } x \equiv \sum_{j<l} \underline{\underline{a_j}} \cdot t_j + \sum_{k<m} \underline{\underline{b_k}} + \sum_{u<v} c_u \cdot r_u + \sum_{w<z} d_w + \sum_{o<p} \sigma_{rel}(s_o) \text{ or} \tag{5.1}$$

$$x \equiv x_1 \leftplus_{\pi_1} x_2 \leftplus_{\pi_2} x_3 \ldots x_{n-1} \leftplus_{\pi_{n-1}} x_n \text{ and } n > 1 \tag{5.2}$$

where $x_i \equiv \sum_{j<l_i} \underline{\underline{a_{ij}}} \cdot t_{ij} + \sum_{k<m_i} \underline{\underline{b_{ik}}} + \sum_{u<v_i} c_{iu} \cdot r_{iu} + \sum_{w<z_i} d_{iw} + \sum_{o<p_i} \sigma_{rel}(s_{io})$ for certain a_j, b_k, c_u, d_w, $a_{ij}, b_{ik}, c_{iu}, d_{iw} \in A_\delta$, $t_j, r_u, t_{ij}, r_{iu} \in \mathcal{B}(pBPA_{drt})$, $s_o, s_{io} \in \mathcal{B}_+(pBPA_{drt})$ and n, m, l, v, z, p, m_i, l_i, $v_i, z_i, p_i \in \mathbb{N}$.

For $pBPA_{drt}$ we define a set of special closed terms $\mathcal{D}(pBPA_{drt})$ that represent the trivial probabilistic processes.

Definition 5.2.5. $\mathcal{SP}(pBPA_{drt})$ will denote the set of all closed terms over the signature of $pBPA_{drt}$. An auxiliary set of closed terms $\mathcal{D}(pBPA_{drt}) \subset \mathcal{SP}(pBPA_{drt})$ is defined as follows:

1. $\underline{\underline{A}}_{\delta} \subseteq \mathcal{D}(pBPA_{drt})$;
2. $A_{\delta} \subseteq \mathcal{D}(pBPA_{drt})$;
3. $s \in \mathcal{D}(pBPA_{drt}), t \in \mathcal{SP}(pBPA_{drt}) \Rightarrow s \cdot t \in \mathcal{D}(pBPA_{drt})$;
4. $s, t \in \mathcal{D}(pBPA_{drt}) \Rightarrow s + t \in \mathcal{D}(pBPA_{drt})$;
5. $s \in \mathcal{D}(pBPA_{drt}) \Rightarrow \sigma_{rel}(s), \nu_{rel}(s) \in \mathcal{D}(pBPA_{drt})$.

Remark 5.2.6. The terms in $\mathcal{D}(pBPA_{drt})$ are of the form:
$\sum_{i<m} s_i \cdot t_i + \sum_{j<n} \underline{\underline{a_j}} + \sum_{k<p} b_k + \sum_{l<q} \sigma_{rel}(o_l) + \sum_{g<w} \nu_{rel}(r_g)$ for some $n, m, p, q, w \in \mathbb{N}$, $a_j, b_k \in A_{\delta}$, $\mathcal{D}(pBPA_{drt})$ terms s_i, o_l, r_g and $\mathcal{SP}(pBPA_{drt})$ terms t_i. Moreover, $\mathcal{B}_+(pBPA_{drt}) \subset \mathcal{D}(pBPA_{drt})$.

For the basic terms the following properties hold. They will be used later on in the proof of the Elimination theorem of $pACP^+_{drt}$ in Section 5.4.

Proposition 5.2.7. If $t \in \mathcal{B}_+(pBPA_{drt})$, then either $pBPA_{drt} \vdash t = \nu_{rel}(s) + \sigma_{rel}(r)$ or $pBPA_{drt} \vdash t = \nu_{rel}(s)$ for some $s, r \in \mathcal{B}_+(pBPA_{drt})$. (This property is more general, namely it may be proved valid for all $\mathcal{D}(pBPA_{drt})$ terms.)

Proof. It is easy to prove the claim using induction on the structure of basic $\mathcal{B}_+(pBPA_{drt})$ terms. □

Proposition 5.2.8. If $p \in \mathcal{B}(pBPA_{drt}) \setminus \mathcal{B}_+(pBPA_{drt})$, then

$$\begin{aligned}
pBPA_{drt} \vdash \quad p = \quad & \nu_{rel}(s_1 \leftthreetimes_{\pi_1} s_2 \leftthreetimes_{\pi_2} \dots s_{n-1} \leftthreetimes_{\pi_n} s_n) \leftthreetimes_{\rho} \\
& \Big((\nu_{rel}(r_1) + \sigma_{rel}(u_1)) \leftthreetimes_{\alpha_1} (\nu_{rel}(r_2) + \sigma_{rel}(u_2)) \leftthreetimes_{\alpha_2} \dots \\
& \qquad (\nu_{rel}(r_{m-1}) + \sigma_{rel}(u_{m-1})) \leftthreetimes_{\alpha_{m-1}} (\nu_{rel}(r_m) + \sigma_{rel}(u_m)) \Big), \text{ or} \\
pBPA_{drt} \vdash \quad p = \quad & \Big((\nu_{rel}(r_1) + \sigma_{rel}(u_1)) \leftthreetimes_{\alpha_1} (\nu_{rel}(r_2) + \sigma_{rel}(u_2)) \leftthreetimes_{\alpha_2} \dots \\
& \qquad (\nu_{rel}(r_{m-1}) + \sigma_{rel}(u_{m-1})) \leftthreetimes_{\alpha_{m-1}} (\nu_{rel}(r_m) + \sigma_{rel}(u_m)) \Big), \text{ or} \\
pBPA_{drt} \vdash \quad p = \quad & \nu_{rel}(s_1 \leftthreetimes_{\pi_1} s_2 \leftthreetimes_{\pi_2} \dots s_{n-1} \leftthreetimes_{\pi_n} s_n),
\end{aligned}$$

for some $n, m \in \mathbb{N}$ and some $s_i, r_j, u_j \in \mathcal{B}_+(pBPA_{drt})$, $\rho, \pi_i, \alpha_j \in \langle 0, 1 \rangle$, $1 \leq i \leq n, 1 \leq j \leq m$.

Proof. It can be easily proved using induction on the number of $\leftthreetimes_{\rho}$ operators in p and using Proposition 5.2.7. □

Proposition 5.2.9. $pBPA_{drt} \vdash s = s + s$, for $s \in \mathcal{D}(pBPA_{drt})$.

Proof. Part of the proof about the operators of *pBPA* is exactly the same as the proof of Proposition 3.2.17. The other inductive steps are trivial except the case $a = a + a$ which is considered in Example 5.2.1. □

Elimination property of *pBPA*$_{drt}$ The Elimination theorem expresses that every closed *pBPA*$_{drt}$ term is equal to a basic *pBPA*$_{drt}$ term. In order to prove this property we employ the method of lexicographic path ordering described in Section 2.3.

Lemma 5.2.10. The term rewrite system consisting of the rules in Table 3.5 without the rule $RA7$ and the rules shown in Table 5.4 ($\pi \in \langle 0, 1 \rangle$) is strongly normalizing.

$\underline{\underline{\delta}} \cdot x$	$\rightarrow$	$\underline{\underline{\delta}}$	$RDRT4$
$\sigma_{rel}(x) \cdot y$	$\rightarrow$	$\sigma_{rel}(x \cdot y)$	$RDRT2$
$\nu_{rel}(\underline{\underline{a}})$	$\rightarrow$	$\underline{\underline{a}}$	$RDCS1$
$\nu_{rel}(a)$	$\rightarrow$	$\underline{\underline{a}}$	$RDCS1'$
$\nu_{rel}(x + y)$	$\rightarrow$	$\nu_{rel}(x) + \nu_{rel}(y)$	$RDCS2$
$\nu_{rel}(x \cdot y)$	$\rightarrow$	$\nu_{rel}(x) \cdot y$	$RDCS3$
$\nu_{rel}(\sigma_{rel}(x))$	$\rightarrow$	$\underline{\underline{\delta}}$	$RDCS4$
$\sigma_{rel}(x \leftplus_\pi y)$	$\rightarrow$	$\sigma_{rel}(x) \leftplus_\pi \sigma_{rel}(y)$	$RPrDRT1$
$\nu_{rel}(x \leftplus_\pi y)$	$\rightarrow$	$\nu_{rel}(x) \leftplus_\pi \nu_{rel}(y)$	$RPrDCS1$

Table 5.4: Additional rules for the term rewrite system of *pBPA*$_{drt}$.

Proof. We use the method of the lexicographical path ordering with the following ordering on the signature of *pBPA*$^-_{drt}$: $\nu_{rel} > \cdot > + > \leftplus_\pi$ and $\cdot > \sigma_{rel}$ and we give the symbol $\cdot$ the lexicographical status for the first argument. Then for each rewrite rule $p \rightarrow q$ in Table 5.4 we can easily prove that $p >_{lpo} q$. From Theorem 2.3.4 we obtain that the given term rewrite system is strongly normalizing. □

Lemma 5.2.11. The normal forms of closed *pBPA*$_{drt}$ terms are basic *pBPA*$_{drt}$ terms.

Proof. Suppose that p is a normal form of some closed *pBPA*$_{drt}$ term and suppose that p is not a basic term. Let p' denotes the smallest sub-term of p which is not a basic term. Then we can prove that p is not a normal form. We use the fact that each sub-term of p' is a basic term. We distinguish all possible cases:

Case $p' \equiv \underline{\underline{a}}$ *or* $p' \equiv a$, $a \in A_\delta$. p' is a basic term, which is in a contradiction with the assumption. So this case does not occur.

Case $p' \equiv p_1 \cdot p_2$. By case analysis on the structure of basic term p_1 we have:

- *Subcase* $p_1 \equiv \underline{\underline{a}}$ *or* $p_1 \equiv a$, $a \in A_\delta$. In this case p' would be a basic term, which contradicts the assumption that p' is not a basic term;
- *Subcase* $p_1 \equiv \underline{\underline{a}} \cdot p_1'$ *or* $p_1 \equiv a \cdot p_1'$, $a \in A_\delta$. Rewriting rule $RA5$ can be applied. So, p is not a normal form;
- *Subcase* $p_1 \equiv p_1' + p_1''$. Rewriting rule $RA4$ can be applied. So, p is not a normal form;
- *Subcase* $p_1 \equiv p_1' \leftplus_\pi p_1''$. Rewriting rule $RPAC4$ can be applied. So, p is not a normal form;
- *Subcase* $p_1 \equiv \sigma_{rel}(p_1')$. Rewriting rule $RDRT2$ can be applied. So, p is not a normal form.

Case $p' \equiv p_1 + p_2$. By case analysis on the structure of both terms p_1 and p_2 we obtain:

Subcase both p_1 *and* p_2 *are basic terms from* $\mathcal{B}_+$. p' would be a basic term, which contradicts the assumption that p' is not a basic term;

Subcase $p_1 \equiv p_1' \leftthreetimes_\pi p_1''$ *or* $p_2 \equiv p_2' \leftthreetimes_\sigma p_2''$. Rewriting rule $RPAC5$ or $RPAC5'$ is applicable. So p is not a normal form.

Case $p' \equiv p_1 \leftthreetimes_\pi p_2$. p' would be a basic term which is in contradiction with the assumption that p' is not a basic term.

Case $p' \equiv \sigma_{rel}(p_1)$. The following subcases are possible:

Subcase $p_1 \in \mathcal{B}_+$. p' would be a basic term, which contradicts the assumption that p' is not a basic term;

Subcase $p_1 \equiv p_1' \leftthreetimes_\pi p_1''$. Rewriting rule $RPrDRT1$ can be applied and so, p is not a normal form;

Case $p' \equiv \nu_{rel}(p_1)$. By case analysis on the structure of basic term p_1 we have:

Subcase $p_1 \equiv \underline{\underline{a}}$, $a \in A_\delta$. rewriting rule $RDCS1$ can be applied. So, p is not a normal form;

Subcase $p_1 \equiv a$, $a \in A_\delta$. Rewriting rule $RDCS1$ can be applied. So, p is not a normal form;

Subcase $p_1 \equiv \underline{\underline{a}} \cdot p_1'$ *or* $p_1 \equiv a \cdot p_1'$, $a \in A$. Rewriting rule $RDCS3$ can be applied. So, p is not a normal form;

Subcase $p_1 \equiv p_1' + p_1''$. Rewriting rule $RDCS2$ can be applied. So, p is not a normal form;

Subcase $p_1 \equiv p_1' \leftthreetimes_\pi p_1''$. Rewriting rule $RPrDCS1$ can be applied. So, p is not a normal form;

Subcase $p_1 \equiv \sigma_{rel}(p_1')$. Rewriting rule $RDCS4$ can be applied. So, p is not a normal form.

□

As a corollary of the previous two lemmas we obtain the following theorem:

Theorem 5.2.12 (*Elimination theorem of pBPA*$_{drt}$). Let p be a closed *pBPA*$_{drt}$ term. Then there is a basic *pBPA*$_{drt}$ term q such that *pBPA*$_{drt} \vdash p = q$. □

Remark 5.2.13. If s is a closed $\mathcal{D}$(*pBPA*$_{drt}$) term, then the associated basic term which exists by the Elimination theorem is a term from the set $\mathcal{B}_+$(*pBPA*$_{drt}$).

We conclude this section with two properties of $\mathcal{D}$(*pBPA*$_{drt}$) terms.

Proposition 5.2.14. If $z_1, z_2 \in \mathcal{D}$(*pBPA*$_{drt}$) and $y = \nu_{rel}(z_1) + \nu_{rel}(z_2) + \sigma_{rel}(y)$, $y_1 = \nu_{rel}(z_1) + \sigma_{rel}(y_1)$ and $y_2 = \nu_{rel}(z_2) + \sigma_{rel}(y_2)$, then $y = y_1 + y_2$.

Proof. By the Elimination theorem we may consider, without loss of generality, only basic $\mathcal{B}_+$(*pBPA*$_{drt}$) terms. The proof is given by induction on $op(z_1) + op(z_2)$ and case distinction on the structure of basic $\mathcal{B}_+$(*pBPA*$_{drt}$) term z_1.

Case $z_1 \equiv \underline{\underline{a}}$ *or* $z_1 \equiv a$, $a \in A_\delta$. $y_1 = \underline{\underline{a}} + \sigma_{rel}(y_1)$ and $y = \underline{\underline{a}} + \nu_{rel}(z_2) + \sigma_{rel}(y)$. (1)
From $RSPDA2$ we get $y_1 = a$, and since $y_2 = \nu_{rel}(z_2) + \sigma_{rel}(y_2)$ by applying $RSPDA4$ on (1) we obtain $y = a + y_2 = y_1 + y_2$;

Case $z_1 \equiv \underline{\underline{a}} \cdot t$ *or* $z_1 \equiv a \cdot t$, $a \in A_\delta$. $y_1 = \underline{\underline{a}} \cdot t + \sigma_{rel}(y_1)$ and $y = \underline{\underline{a}} \cdot t + \nu_{rel}(z_2) + \sigma_{rel}(y)$. From $RSPDA5$ we obtain $y = a \cdot t + y_2$ where $y_2 = \nu_{rel}(z_2) + \sigma_{rel}(y_2)$. From $RSPDA3$ we obtain $y_1 = a \cdot t$. Hence, $y = y_1 + y_2$;

Case $z_1 \equiv w' + w''$. $y = \nu_{rel}(w') + \nu_{rel}(w'') + \nu_{rel}(z_2) + \sigma_{rel}(y)$ and by the induction hypothesis for $y'_1 = \nu_{rel}(w') + \sigma_{rel}(y'_1)$ and $y'_2 = \nu_{rel}(w'') + \nu_{rel}(z_2) + \sigma_{rel}(y'_2)$ we obtain that $y = y'_1 + y'_2$. (The induction hypothesis is applicable because $op(w') + op(w'') + op(z_2) < op(z_1) + op(z_2)$.) Furthermore, if we take $y''_2 = \nu_{rel}(w'') + \sigma_{rel}(y''_2)$ and since $y_2 = \nu_{rel}(z_2) + \sigma_{rel}(y_2)$, (2) by the induction hypothesis we obtain $y'_2 = y''_2 + y_2$. Thus, $y = y'_1 + y''_2 + y_2$ and (2) hold for y_2. Moreover,
$y'_1 + y''_2 = \nu_{rel}(w') + \nu_{rel}(w'') + \sigma_{rel}(y'_1) + \sigma_{rel}(y''_2) = \nu_{rel}(w' + w'') + \sigma_{rel}(y'_1 + y''_2) = \nu_{rel}(z_1) + \sigma_{rel}(y'_1 + y''_2)$. Taking $y_1 \equiv y'_1 + y''_2$ we obtain $y_1 = \nu_{rel}(z_1) + \sigma_{rel}(y_1)$. In conclusion we obtain that $y = y_1 + y_2$ for $y_1 = \nu_{rel}(z_1) + \sigma_{rel}(y_1)$ and $y_2 = \nu_{rel}(z_2) + \sigma_{rel}(y_2)$;

Case $z_1 \equiv \sigma_{rel}(w)$. $\nu_{rel}(z_1) = \underline{\underline{\delta}}$ and $y = \underline{\underline{\delta}} + \nu_{rel}(z_2) + \sigma_{rel}(y)$. By axiom $RSPDA4$ we obtain $y = \delta + y_2$ for $y_2 = \nu_{rel}(z_2) + \sigma_{rel}(y_2)$. For $y_1 = \nu_{rel}(z_1) + \sigma_{rel}(y_1)$, by axiom $RSPDA2$ we obtain $y_1 = \delta$. Thus, $y = y_1 + y_2$.

□

Proposition 5.2.15. If $z \in \mathcal{D}(pBPA_{drt})$ and $y = \nu_{rel}(z) + \sigma_{rel}(y)$ and $w = \nu_{rel}(z) + \sigma_{rel}(w)$ then $y = w$.

Proof. Using the Elimination theorem we can assume that z is a $\mathcal{B}_+(pBPA_{drt})$ term. The proposition is proved by case distinction on the structure of z.

Case $z \equiv \underline{\underline{a}}$ *or* $z \equiv a$ *for* $a \in A_\delta$. $\nu_{rel}(z) = \underline{\underline{a}}$ and $y = \underline{\underline{a}} + \sigma_{rel}(y)$ and $w = \underline{\underline{a}} + \sigma_{rel}(w)$. Using $RSPDA2$ axiom we obtain $y = a = w$;

Case $z \equiv \underline{\underline{a}} \cdot t$ *or* $z \equiv a \cdot t$ *for* $a \in A_\delta$. $\nu_{rel}(z) = \underline{\underline{a}} \cdot t$ and $y = \underline{\underline{a}} \cdot t + \sigma_{rel}(y)$ and $w = \underline{\underline{a}} \cdot t + \sigma_{rel}(w)$. Using $RSPDA3$ axiom we obtain $y = a \cdot t = w$;

Case $z \equiv z_1 + z_2$. $\nu_{rel}(z) = \nu_{rel}(z_1) + \nu_{rel}(z_2)$ and
$y = \nu_{rel}(z_1) + \nu_{rel}(z_2) + \sigma_{rel}(y)$ and $w = \nu_{rel}(z_1) + \nu_{rel}(z_2) + \sigma_{rel}(w)$. By Proposition 5.2.14 we obtain $y = u_1 + u_2$ where $u_1 = \nu_{rel}(z_1) + \sigma_{rel}(u_1)$ and $u_2 = \nu_{rel}(z_2) + \sigma_{rel}(u_2)$. And also $w = v_1 + v_2$ where $v_1 = \nu_{rel}(z_1) + \sigma_{rel}(v_1)$ and $u_2 = \nu_{rel}(v_2) + \sigma_{rel}(v_2)$. Then, by the induction hypothesis we have $u_1 = v_1$ and $u_2 = v_2$. Finally, $y = u_1 + u_2 = v_1 + v_2 = w$;

Case $z \equiv \sigma_{rel}(z_1)$. $\nu_{rel}(z) = \underline{\underline{\delta}}$ and $y = \underline{\underline{\delta}} + \sigma_{rel}(y)$ and $w = \underline{\underline{\delta}} + \sigma_{rel}(w)$. By axiom $RSPDA2$ we obtain $y = \delta = w$.

□

5.3 Structural operational semantics of $pBPA_{drt}$

The operational semantics consists of the following types of transition (deduction) rules: rules for probabilistic transition: $\rightsquigarrow$ (which are unlabelled), rules for action transitions: $\xrightarrow{a}$, rules for action termination $\xrightarrow{a} \surd$ (for $a \in A$), rules for time transition: $\xrightarrow{\sigma}$ and rules for the $\boldsymbol{D}$ predicate.

The $\boldsymbol{D}$ predicate characterizes those processes that have a sub-process that can be postponed for *two* time slices. This predicate is necessary to define the operational semantics of the parallel composition operator in the next section. There it will be discussed in more detail.

As we have mentioned already, the passage of time cannot resolve a probabilistic choice. In the algebra we have axiom $PrDRT1$ which makes terms $\sigma_{rel}(\underline{\underline{a}} \leftthreetimes_{0.5} \underline{\underline{b}})$ and $\sigma_{rel}(\underline{\underline{a}}) \leftthreetimes_{0.5} \sigma_{rel}(\underline{\underline{b}})$ to be considered equal. Hence, in the bisimulation model the interpretations of these two terms have to be bisimilar. This requirement can be met in at least two ways. The first option is if these two terms have two different operational interpretations. The most intuitive interpretation of these processes is given in Figure 5.1. In order to make them bisimilar we have to change the definition of bisimulation relation in a way that it would relate these processes, which means a complex and non-intuitive definition. Also a lot of deduction rules have to be added in order to cover all sequences which only differ in the order of $\rightsquigarrow$ and $\xrightarrow{\sigma}$'s. This approach is not appropriate for technical reasons as well. Namely, without any constraints about the order of $\rightsquigarrow$ and $\xrightarrow{\sigma}$ transitions the formulation of many propositions, and moreover their proofs, are difficult and unclear. Thus, we come up with another idea to interpret these two terms by the same process. In this way, we obtain simple deduction rules of the operational semantics that guarantee some useful properties about the order in which $\rightsquigarrow$ and $\xrightarrow{\sigma}$ transitions appear.

We only present the bisimulation model of $pBPA_{drt}$ and the model of $pBPA^{-}_{drt}$ can easily be derived from the given one.

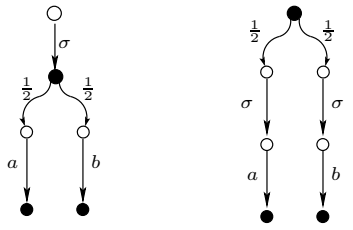


Figure 5.1: Transition systems of two processes

5.3.1 Model of $pBPA_{drt}$ and properties of the model

Like in the untimed probabilistic process algebras in Chapters 3 and 4 the operational semantics of $pBPA_{drt}$ is based on the alternating model. Namely, every probabilistic transition is followed by action transitions which may be delayed for an arbitrary number of time slices. An action transition can be an action termination or it is followed by a probabilistic transition.

The Operational semantics of $pBPA_{drt}$ is defined by the term-deduction system $\mathbf{T}_{pBPA_{drt}} = \left(\breve{\Sigma}_{pBPA_{drt}}, \mathbf{DR}_{pBPA_{drt}}\right)$ with $\breve{\Sigma}_{pBPA_{drt}} = (\underline{\underline{A}}_{\delta} \cup \breve{\underline{\underline{A}}}_{\delta} \cup A_{\delta} \cup \breve{A}_{\delta}, +, \cdot, \leftthreetimes_{\pi}, \sigma_{rel}, \nu_{rel})$ and with the deduction rules shown in Table 5.5+ 5.6+5.7+5.8. With PRA replaced by $pBPA_{drt}$ the items 1, 3-5 in Definition 3.3.2 (on page 49) together with the added ones in Definition 5.3.1 (according to the 7th item in Definition 3.3.2) define the set of static processes $\mathbb{SP}(pBPA_{drt})$; the items 1-3 in Definition 3.3.3 (on page 49) together with 1', 5.4 and 5.5 in Definition 5.3.2 define the set of trivial static processes $\mathbb{D}(pBPA_{drt})$; the items 1-3 in Definition 3.3.4 (on page 50) together with 1', 5.4 and 5.5 in Definition 5.3.3 define the set of dynamic processes, $\mathbb{DP}(pBPA_{drt})$; the PDF function μ on $\mathbb{PT}(pBPA_{drt})$ is defined by Definition 5.3.4 and the probabilistic bisimulation relation on $\mathbb{PT}(pBPA_{drt})$ is defined by Definition 5.3.5. In contrast to the previous chapters here we enumerate the deduction rules. This is because through this chapter we refer to different rules many times. The enumeration is given by the order the rules occur in the thesis.

Definition 5.3.1.

1'. $\underline{\underline{A}}_{\delta} \subseteq \mathbb{SP}(pBPA_{drt})$;

7.4. if $s \in \mathbb{SP}(pBPA_{drt})$, then $\sigma_{rel}(s) \in \mathbb{SP}(pBPA_{drt})$;

7.5 if $s \in \mathbb{SP}(pBPA_{drt})$, then $\nu_{rel}(s) \in \mathbb{SP}(pBPA_{drt})$.

Definition 5.3.2.

1'. $\underline{\underline{A}}_{\delta} \subseteq \mathbb{D}(pBPA_{drt})$;

5.4. if $s \in \mathbb{D}(pBPA_{drt})$, then $\sigma_{rel}(s) \in \mathbb{D}(pBPA_{drt})$;

5.5. if $s \in \mathbb{D}(pBPA_{drt})$, then $\nu_{rel}(s) \in \mathbb{D}(pBPA_{drt})$.

Definition 5.3.3.

1'. $\varphi(\underline{\underline{a}}) = \underline{\underline{\varphi(a)}}$;

5.4. $\varphi(\sigma_{rel}(s)) = \sigma_{rel}(\varphi(s))$;

5.5. $\varphi(\nu_{rel}(s)) = \nu_{rel}(\varphi(s))$.

Definition 5.3.4. (PDF for $pBPA_{drt}$) A probability distribution function on $\mathbb{PT}(pBPA_{drt})$ is defined by the equalities in Table 3.6, 3.7 and 5.9.

$$R1.1 : \underline{\underline{a}} \rightsquigarrow \breve{\underline{\underline{a}}} \qquad R1.2 : \underline{\underline{\delta}} \rightsquigarrow \breve{\underline{\underline{\delta}}} \qquad R1.3 : a \rightsquigarrow \breve{a} \qquad R1.4 : \delta \rightsquigarrow \breve{\delta}$$

$$R21 : \frac{x \rightsquigarrow x'}{\sigma_{rel}(x) \rightsquigarrow \sigma_{rel}(x')} \qquad R22 : \frac{x \rightsquigarrow x'}{\nu_{rel}(x) \rightsquigarrow \nu_{rel}(x')}$$

$$R13 : \frac{x \rightsquigarrow x'}{x \cdot y \rightsquigarrow x' \cdot y} \qquad R14 : \frac{x \rightsquigarrow x', y \rightsquigarrow y'}{x + y \rightsquigarrow x' + y'} \qquad R15 : \frac{x \rightsquigarrow z}{x \between_{\pi} y \rightsquigarrow z, y \between_{\pi} x \rightsquigarrow z}$$

Table 5.5: Probabilistic transitions in $pBPA_{drt}$.

Definition 5.3.5. Let R be an equivalence relation on the set of processes $\mathbb{PT}(pBPA_{drt})$. R is a *probabilistic bisimulation* if:

1. if $(p, q) \in R$ and $p \rightsquigarrow s$, then there is a term t such that $q \rightsquigarrow t$ and $(s, t) \in R$;
2. if $(s, t) \in R$ and $s \xrightarrow{a} p$ for some $a \in A$, then there is a term q such that $t \xrightarrow{a} q$ and $(p, q) \in R$;
3. if $(s, t) \in R$ and $s \xrightarrow{a} \surd$, then $t \xrightarrow{a} \surd$;
4. if $(s, t) \in R$ and $s \xrightarrow{\sigma} p$, then there is a term q such that $t \xrightarrow{\sigma} q$ and $(p, q) \in R$;

$$R1.5 : \underline{\breve{a}} \xrightarrow{a} \surd \qquad R1.6 : \breve{a} \xrightarrow{a} \surd \qquad R23 : \frac{x \xrightarrow{a} x'}{\nu_{rel}(x) \xrightarrow{a} x'}$$

$$R24 : \frac{x \xrightarrow{a} \surd}{\nu_{rel}(x) \xrightarrow{a} \surd} \qquad R2 : \frac{x \xrightarrow{a} x'}{x \cdot y \xrightarrow{a} x' \cdot y} \qquad R3 : \frac{x \xrightarrow{a} \surd}{x \cdot y \xrightarrow{a} y}$$

$$R4 : \frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x', y + x \xrightarrow{a} x'} \qquad R5 : \frac{x \xrightarrow{a} \surd}{x + y \xrightarrow{a} \surd, y + x \xrightarrow{a} \surd}$$

Table 5.6: Action transitions in *pBPA*$_{drt}$.

$$R1.7 : \breve{a} \xrightarrow{\sigma} \breve{a} \qquad R1.8 : \breve{\delta} \xrightarrow{\sigma} \breve{\delta} \qquad R25 : \frac{x \not\rightarrow}{\sigma_{rel}(x) \xrightarrow{\sigma} x}$$

$$R26 : \frac{x \xrightarrow{\sigma} x', y \not\xrightarrow{\sigma}}{x + y \xrightarrow{\sigma} x', y + x \xrightarrow{\sigma} x'} \qquad R27 : \frac{x \xrightarrow{\sigma} x', y \xrightarrow{\sigma} y'}{x + y \xrightarrow{\sigma} x' + y'} \qquad R28 : \frac{x \xrightarrow{\sigma} x'}{x \cdot y \xrightarrow{\sigma} x' \cdot y}$$

Table 5.7: Rules for time transitions.

5. if $(s, t) \in R$ and $\boldsymbol{D}(s)$, then $\boldsymbol{D}(t)$;

6. if $(p, q) \in R$, then $\mu(p, M) = \mu(q, M)$ for each $M \in \mathbb{PT}(pBPA_{drt})/R$.

We say that p is *probabilistically bisimilar* to q, denote $p \leftrightarrows q$, if there is a probabilistic bisimulation R such that $(p, q) \in R$.

Intuitively, by $\underline{\breve{a}}$ we denote a process that can successfully terminate by executing a within the current time slice. By $\underline{\breve{\delta}}$ we denote a process that can neither execute any action nor can idle till the next times slice. $\breve{a}$ is like $\underline{\breve{a}}$ but it may delay its execution for an arbitrary number of time slices. And $\breve{\delta}$ can idle indefinitely, but nothing else. These are all dynamic processes and they cannot perform a probabilistic transition. Informally, these constants can be viewed as $\underline{a}$, $\underline{\delta}$, a and δ, respectively, from non-probabilistic discrete time process algebras.

The $\boldsymbol{D}$ predicate is not essential in the operational semantics of *pBPA*$_{drt}$ and it can be expressed by means of the other transition relations (see Proposition 5.3.14 and 5.3.15). It selects those processes

$$R1.9 : \boldsymbol{D}(a) \qquad R1.10 : \boldsymbol{D}(\breve{a}) \qquad R29 : \boldsymbol{D}(\sigma_{rel}(x))$$

$$R30 : \frac{\boldsymbol{D}(x)}{\boldsymbol{D}(x \cdot y)} \qquad R31 : \frac{\boldsymbol{D}(x)}{\boldsymbol{D}(x + y), \boldsymbol{D}(y + x)} \qquad R32 : \frac{\boldsymbol{D}(x)}{\boldsymbol{D}(x \leftplus_{\pi} y), \boldsymbol{D}(y \leftplus_{\pi} x)}$$

Table 5.8: Deduction rules for predicate $\boldsymbol{D}$.

$\mu(\underline{\underline{a}}, \breve{\underline{\underline{a}}})$	$=$	1
$\mu(\underline{\underline{\delta}}, \underline{\underline{\delta}})$	$=$	1
$\mu(\sigma_{rel}(x), \sigma_{rel}(x'))$	$=$	$\mu(x, x')$
$\mu(\nu_{rel}(x), \nu_{rel}(x'))$	$=$	$\mu(x, x')$

Table 5.9: Equalities that defined PDF's for $pBPA_{drt}$ (part 3)

from $\mathbb{DP}(pBPA_{drt})$ that can do a time step, and processes from $\mathbb{SP}(pBPA_{drt})$ that with positive probability reach a process which can perform a time step. To simplify, it contains all processes which are still active (can still do a transition) after one time tick. By this, it become clear why it is $\boldsymbol{D}(a)$ and $\boldsymbol{D}(\breve{a})$ but not $\boldsymbol{D}(\underline{\underline{a}})$ or $\boldsymbol{D}(\breve{\underline{\underline{a}}})$. The $\boldsymbol{D}$ predicate is added to the semantics because it plays an important role in the definition of deduction rules for parallel composition defined in the next section. More details can be found on pg. 155.

Another rule which needs some explanation is $R25$. As we explained in the introduction by the processes shown in Figure 5.1 we do not allow a process to perform a time transition before it resolves its probabilistic choice. The negative premise expresses this exactly.

The remainder of the section will be used to present certain properties of transitions in $\mathbf{T}_{pBPA_{drt}}$ and the PDF function on $\mathbb{PT}(pBPA_{drt})$. Again, many properties given here have been already proved in Chapter 3 for *pBPA* and its model. In order to avoid repeating the proofs that already appear in that chapter (they remain valid in $\mathbf{T}_{pBPA_{drt}}$), here we mainly focus on the new operators added to *pBPA* to obtain $pBPA_{drt}$, and even more we skip proofs which are trivial.

Proposition 5.3.6. The PDF function μ is well defined on $\mathbb{PT}(pBPA_{drt})$.

Proof. Continuation of the proof of Proposition 3.3.18. The first part of the proof is to show that μ is well defined on $\mathbb{SP}(pBPA_{drt})$. Later, for $\mathbb{DP}(pBPA_{drt})$ processes we prove that the value of μ equals 0.

Case $p \equiv \underline{\underline{a}}$, $a \in A_\delta$. For any u, $\mu(\underline{\underline{a}}, u) = \begin{cases} 1, & if\ u \equiv \breve{\underline{\underline{a}}} \\ 0, & otherwise \end{cases}$. Hence, $\mu(\underline{\underline{a}}, u)$ is defined.

Case $p \equiv \sigma_{rel}(q)$. For any u, $\mu(\sigma_{rel}(p), u) = \begin{cases} \mu(q, v), & if\ u \equiv \sigma_{rel}(v) \\ 0, & otherwise \end{cases}$.
Since $\mu(q, v)$ is defined by the induction hypothesis, $\mu(\sigma_{rel}(q), u)$ is defined as well.

Case $p \equiv \nu_{rel}(q)$. For any u, $\mu(\nu_{rel}(p), u) = \begin{cases} \mu(q, v), & if\ u \equiv \nu_{rel}(v) \\ 0, & otherwise \end{cases}$.
Since $\mu(q, v)$ is defined by the induction hypothesis, $\mu(\nu_{rel}(q), u)$ is defined as well.

Let be $p \in \mathbb{DP}(pBPA_{drt})$. We prove that $\mu(p, u) = 0$.

Case $p \equiv \breve{\underline{\underline{a}}}$, $a \in A_\delta$. By the definition of the PDF $\mu(\breve{\underline{\underline{a}}}, u) = 0$ for any u.

Case $p \equiv \sigma_{rel}(q)$. $\mu(\sigma_{rel}(q), u) = \begin{cases} \mu(q, v), & if\ u \equiv \sigma_{rel}(v) \\ 0, & otherwise \end{cases}$.
Since $\mu(q, v) = 0$ by the induction hypothesis, it follows that $\mu(\sigma_{rel}(q), u) = 0$ for any u.

Case $p \equiv \nu_{rel}(q)$. $\mu(\nu_{rel}(q), u) = \begin{cases} \mu(q, v), & if\ u \equiv \nu_{rel}(v) \\ 0, & otherwise \end{cases}$.

Since $\mu(q, v) = 0$ by the induction hypothesis, $\mu(\nu_{rel}(q), u) = 0$ for any u.

□

Proposition 5.3.7. The cPDF function μ is well defined on $\mathbb{PT}(pBPA_{drt})$.

Proof. Continuation of the proof of Proposition 3.3.20

Case $p \equiv \underline{\underline{a}}$, $a \in A_\delta$. $\mu(\underline{\underline{a}}, M) = \sum_{x \in M} \mu(\underline{\underline{a}}, x) = \begin{cases} 1, & \breve{\underline{\underline{a}}} \in M \\ 0, & otherwise \end{cases}$.

Case $p \equiv \sigma_{rel}(q)$. $\mu(\sigma_{rel}(q), M) = \sum_{x \in M} \mu(\sigma_{rel}(q), x) = \sum_{x : x \in M \,\&\, \exists x' : x \equiv \sigma_{rel}(x')} \mu(\sigma_{rel}(s), x) = \sum_{x' : \sigma_{rel}(x') \in M} \mu(s, x') = \mu(s, \{x' \ : \ \sigma_{rel}(x') \in M\}) \in [0, 1]$

by the induction hypothesis.

Case $p \equiv \nu_{rel}(q)$. This case is similar to the previous case.

□

Proposition 5.3.8. Let be $p \in \mathbb{SP}(pBPA_{drt})$ and $K \subseteq \mathbb{PT}(pBPA_{drt})$. Then:

i. The equalities given in Proposition 3.3.21 are valid when $pBPA + PR$ is replaced by $pBPA_{drt}$;

ii. $\mu(\sigma_{rel}(p), \sigma_{rel}(K)) = \mu(p, K)$;

iii. $\mu(\nu_{rel}(p), \nu_{rel}(K)) = \mu(p, K)$.

Proof. In a similar way like the proof of Proposition 4.3.7 *iv*. □

Alternation of probabilistic on one side and action and time transitions on the other side is guaranteed by the following propositions.

Proposition 5.3.9. If $p \in \mathbb{SP}(pBPA_{drt})$ and $p \rightsquigarrow u$, then $u \in \mathbb{DP}(pBPA_{drt})$.

Proof. The proof is a continuation of the inductive proof of Proposition 3.3.22. Let us assume that $p \rightsquigarrow u$.

Case $p \equiv \underline{\underline{a}}$, $a \in A_\delta$. $\underline{\underline{a}} \rightsquigarrow \breve{\underline{\underline{a}}}$ is the only possible probabilistic transition and $\breve{\underline{\underline{a}}} \in \mathbb{DP}(pBPA_{drt})$;

Case $p \equiv \sigma_{rel}(q)$. $q \rightsquigarrow v$ and $u \equiv \sigma_{rel}(v)$. From the induction hypothesis $v \in \mathbb{DP}(pBPA_{drt})$ and $u \in \mathbb{DP}(pBPA_{drt})$;

Case $p \equiv \nu_{rel}(q)$. The case is similar to the previous case.

□

Corollary 5.3.10.

i. If p is an $\mathbb{SP}(pBPA_{drt})$ process and $p \rightsquigarrow \sigma_{rel}(x)$, then $x \in \mathbb{DP}(pBPA_{drt})$.

ii. If p is an $\mathbb{SP}(pBPA_{drt})$ process, then $p \not\stackrel{g}{\rightarrow}$.

□

Proposition 5.3.11. If u is a $\mathbb{D}(pBPA_{drt})$ process, then the only possible probabilistic transition of u is $u \rightsquigarrow \breve{u}$.

Proof. The cases that needed to be added to the inductive proof of Proposition 3.3.24 are trivial.

□

Corollary 5.3.12.

i. If u, v are $\mathbb{D}(pBPA_{drt})$ processes, then $u \rightsquigarrow \breve{v}$ iff $u \equiv v$.

ii. If p is an interpretation of a basic $pBPA_{drt}$ term $\mathbf{p}$ and $p \rightsquigarrow \breve{x}$ for some $x \in \mathbb{DP}(pBPA_{drt})$, then x is the interpretation of the basic $pBPA_{drt}$ term $\mathbf{x}$. Moreover $\mathbf{x} \in \mathcal{B}_+(pBPA_{drt})$. □

Proposition 5.3.13.

i. If u is a $\mathbb{DP}(pBPA_{drt})$ process and $u \xrightarrow{a} p$ for some $a \in A$, then $p \in \mathbb{SP}(pBPA_{drt})$.

ii. If u is a $\mathbb{DP}(pBPA_{drt})$ process and $u \xrightarrow{\sigma} v$, then $v \in \mathbb{DP}(pBPA_{drt})$.

Proof. It is easy to prove by induction on the structure of $\mathbb{DP}(pBPA_{drt})$ processes. □

In the sequel we show several properties that precisely describe the meaning of the $\boldsymbol{D}$ predicate.

Proposition 5.3.14. Let be $u \in \mathbb{DP}(pBPA_{drt})$. $\boldsymbol{D}(u)$ iff $\exists y \,:\, u \xrightarrow{\sigma} y$.

Proof. The proof is given by induction on the structure of u.

Case $u \equiv \underline{\breve{a}}$, $a \in A_\delta$ *or* $u \equiv \nu_{rel}(v)$. These cases do not occur;

Case $u \equiv \breve{a}, a \in A_\delta$ *or* $u \equiv \sigma_{rel}(v)$. The result is straightforward;

Case $u \equiv v + w$. $\boldsymbol{D}(u)$ iff ($\boldsymbol{D}(v)$ or $\boldsymbol{D}(w)$) iff (by the induction hypothesis) there is x such that $v \xrightarrow{\sigma} x$ or there is y such that $w \xrightarrow{\sigma} y$ iff (by the deduction rules) there is z such that $u \xrightarrow{\sigma} z$;

Case $u \equiv v \cdot p$. $\boldsymbol{D}(u)$ iff $\boldsymbol{D}(v)$ iff (by the induction hypothesis) there is x such that $v \xrightarrow{\sigma} x$ iff $v \cdot p \xrightarrow{\sigma} x \cdot p$ iff there is y such that $u \xrightarrow{\sigma} y$.

□

Proposition 5.3.15. Let be $p \in \mathbb{SP}(pBPA_{drt})$. $\boldsymbol{D}(p)$ iff $\exists x, y \,:\, p \rightsquigarrow x \,\&\, x \xrightarrow{\sigma} y$.

Proof. The proof is given by induction on the structure of p. We give each direction separately.
Let us assume that $\boldsymbol{D}(p)$.

Case $p \equiv a, a \in A_\delta$ *or* $p \equiv \sigma_{rel}(q)$. The result is straightforward;

Case $p \equiv q + r$. $\boldsymbol{D}(q)$ or $\boldsymbol{D}(r)$. From the induction hypothesis there are x, y such that $q \rightsquigarrow x \,\&\, x \xrightarrow{\sigma} y$ or there are z, w such that $r \rightsquigarrow z \,\&\, z \xrightarrow{\sigma} w$. If

Subcase $q \rightsquigarrow x \,\&\, x \xrightarrow{\sigma} y$ *and* $\forall z \,:\, (r \rightsquigarrow z \Rightarrow z \not\xrightarrow{\sigma})$. $p \rightsquigarrow x + z \xrightarrow{\sigma} y$;

Subcase $r \rightsquigarrow z \;\&\; z \xrightarrow{\sigma} w$ *and* $\forall x:\ (q \rightsquigarrow x \Rightarrow x \not\xrightarrow{\sigma})$. $p \rightsquigarrow x + z \xrightarrow{\sigma} w$;

Subcase $q \rightsquigarrow x \;\&\; x \xrightarrow{\sigma} y$ *and* $r \rightsquigarrow z \;\&\; z \xrightarrow{\sigma} w$. $p \rightsquigarrow x + z \xrightarrow{\sigma} y + w$.

Case $p \equiv q \cdot r$. Then $\boldsymbol{D}(q)$. From the induction hypothesis follows that there are u, v such that $q \rightsquigarrow u \;\&\; u \xrightarrow{\sigma} v$. Therefore, $p \rightsquigarrow u \cdot r$ and $u \cdot r \xrightarrow{\sigma} v \cdot r$;

Case $p \equiv q \leftplus_{\pi} r$. Then $\boldsymbol{D}(q)$ or $\boldsymbol{D}(r)$. From the induction hypothesis follows that there are x, y such that $q \rightsquigarrow x \;\&\; x \xrightarrow{\sigma} y$ or there are z, w such that $r \rightsquigarrow z \;\&\; z \xrightarrow{\sigma} w$. Therefore, either $p \rightsquigarrow x$ and $x \xrightarrow{\sigma} y$ or $p \rightsquigarrow z$ and $z \xrightarrow{\sigma} w$.

Let us assume that there are x, y such that $p \rightsquigarrow x$ and $x \xrightarrow{\sigma} y$.

Case $p \equiv a, a \in A_\delta$ *or* $p \equiv \sigma_{rel}(q)$. The result is straightforward;

Case $p \equiv q + r$. Then $q \rightsquigarrow x'$, $r \rightsquigarrow x''$, $x \equiv x' + x''$ and $x' + x'' \xrightarrow{\sigma} y$. If

Subcase $x' \xrightarrow{\sigma} y$ *and* $x'' \not\xrightarrow{\sigma}$. From the induction hypothesis follows that $\boldsymbol{D}(q)$ from which $\boldsymbol{D}(p)$ as well;

Subcase $x'' \xrightarrow{\sigma} y$ *and* $x' \not\xrightarrow{\sigma}$. From the induction hypothesis follows that $\boldsymbol{D}(r)$ from which $\boldsymbol{D}(p)$ as well;

Subcase $x' \xrightarrow{\sigma} y'$, $x'' \xrightarrow{\sigma} y''$ *and* $y \equiv y' + y''$. From the induction hypothesis follows that $\boldsymbol{D}(q)$ and $\boldsymbol{D}(r)$ from which $\boldsymbol{D}(p)$ as well;

Case $p \equiv q \cdot r$. $q \rightsquigarrow x'$, $x' \xrightarrow{\sigma} y'$ and $y \equiv y' \cdot r$. From the induction hypothesis $\boldsymbol{D}(q)$ from which $\boldsymbol{D}(p)$ as well;

Case $p \equiv q \leftplus_{\pi} r$. $q \rightsquigarrow x \;\&\; x \xrightarrow{\sigma} y$ or $r \rightsquigarrow z \;\&\; z \xrightarrow{\sigma} w$. Then either $\boldsymbol{D}(q)$ or $\boldsymbol{D}(r)$ but in both cases $\boldsymbol{D}(p)$.

□

Definition 5.3.16. If $M \subseteq \mathbb{PT}(pBPA_{drt})$, then $\boldsymbol{D}(M)$ iff $\boldsymbol{D}(m)$ for all $m \in M$.

Corollary 5.3.17. If R is a bisimulation relation and $M \in \mathbb{PT}(pBPA_{drt})/R$, then $\boldsymbol{D}(M)$ iff there is an element $m \in M$ such that $\boldsymbol{D}(m)$.

Proposition 5.3.18. Let be $u \in \mathbb{DP}(pBPA_{drt})$ and $u \xrightarrow{\sigma} x$ and $u \xrightarrow{\sigma} y$. Then $x \equiv y$.

Proof. The proof is given by the induction on the structure of u.

Case $u \equiv \underline{\breve{a}}$, $a \in A_\delta$ *or* $u \equiv \nu_{rel}(v)$. Then $u \not\xrightarrow{\sigma}$;

Case $u \equiv \breve{a}$, $a \in A_\delta$ *or* $u \equiv \sigma_{rel}(v)$. By the definition of the operational rules the conclusion follows;

Case $u \equiv v \cdot q$. By assumption $u \xrightarrow{\sigma} x$ and $u \xrightarrow{\sigma} y$ we have that $v \xrightarrow{\sigma} x'$ and $v \xrightarrow{\sigma} y'$ for some $x', y' \in \mathbb{DP}(pBPA_{drt})$ such that $x \equiv x' \cdot q$ and $y \equiv y' \cdot q$. By the induction hypothesis we get $x' \equiv y'$ from which the conclusion follows;

Case $u \equiv v + w$. By assumption $u \xrightarrow{\sigma} x$ and $u \xrightarrow{\sigma} y$ we have:

Subcase $v \xrightarrow{\sigma} x'$ *and* $w \xrightarrow{\sigma} x''$ *and* $v \xrightarrow{\sigma} y'$ *and* $w \xrightarrow{\sigma} y''$. By the induction hypothesis we get $x' \equiv y'$ and $x'' \equiv y''$ from which $x \equiv y$;

Subcase $w \not\xrightarrow{\sigma}$ *and* $v \xrightarrow{\sigma} x$ *and* $v \xrightarrow{\sigma} y$. By the induction hypothesis $x \equiv y$;
Subcase $v \not\xrightarrow{\sigma}$ *and* $w \xrightarrow{\sigma} x$ *and* $w \xrightarrow{\sigma} y$. By the induction hypothesis $x \equiv y$.

□

Proposition 5.3.19. If u is a $\mathbb{D}(pBPA_{drt})$ process, then $\mu(u, \breve{u}) = 1$. □

Proposition 5.3.20. Let be $p \in \mathbb{PT}(pBPA_{drt})$. Then $\mu(p, x) > 0$ iff $p \rightsquigarrow x$.

Proof. The proof is similar to the part of the proof of Proposition 3.3.28 that considers atomic actions and the projection operator (as an unary operator whose definition resembles the ones of ν_{rel} and σ_{rel}). □

Proposition 5.3.21. If $p \in \mathbb{SP}(pBPA_{drt})$, then $\mu(p, \mathbb{PT}(pBPA_{drt})) = 1$.

Proof. We just give the continuation of the inductive proof of Proposition 3.3.30.

Case $p \equiv \underline{\underline{a}}$, $a \in A_\delta$. $\mu(\underline{\underline{a}}, \mathbb{DP}(pBPA_{drt})) = \sum_{u \in \mathbb{DP}(pBPA_{drt})} \mu(\underline{\underline{a}}, u) = \mu(\underline{\underline{a}}, \breve{\underline{\underline{a}}}) = 1$;

Case $p \equiv \sigma_{rel}(q)$. Using Proposition 5.3.8 *ii.* and the induction hypothesis we obtain
$\mu(p, \mathbb{DP}(pBPA_{drt})) = \mu(\sigma_{rel}(q), \sigma_{rel}(\mathbb{DP}(pBPA_{drt}))) = \mu(q, \mathbb{DP}(pBPA_{drt})) = 1$.

Case $p \equiv \nu_{rel}(q)$. Using Proposition 5.3.8 *iii.* and the induction hypothesis we obtain
$\mu(p, \mathbb{DP}(pBPA_{drt})) = \mu(\nu_{rel}(q), \nu_{rel}(\mathbb{DP}(pBPA_{drt}))) = \mu(q, \mathbb{DP}(pBPA_{drt})) = 1$.

□

Corollary 5.3.22.

i. Let $p \in \mathbb{PT}(pBPA_{drt})$ and $M \subseteq \mathbb{PT}(pBPA_{drt})$. Then $\mu(p, M) > 0$ iff $\exists x \in M : p \rightsquigarrow x$;

ii. If $p \in \mathbb{SP}(pBPA_{drt})$ and $u \in \mathbb{D}(pBPA_{drt})$ and $\mu(p, [\breve{u}]_{\underline{\leftrightarrow}}) = 1$, then $p \underline{\leftrightarrow} u$.

iii. Proposition 3.3.32 is valid in $\mathbb{PT}(pBPA_{drt})$.

□

Remark 5.3.23. Remark 3.3.34 (pg. 63) can be reformulated for $pBPA_{drt}$ in the following way: from Proposition 5.3.9 and 5.3.13 we conclude that we can simplify proofs by taking into account:

1. $\rightsquigarrow \subseteq \mathbb{SP}(pBPA_{drt}) \times \mathbb{DP}(pBPA_{drt})$,
2. $\xrightarrow{a} \subseteq \mathbb{DP}(pBPA_{drt}) \times \mathbb{SP}(pBPA_{drt})$,
3. $\xrightarrow{a} \surd \subseteq \mathbb{DP}(pBPA_{drt})$,
4. $\xrightarrow{\sigma} \subseteq \mathbb{DP}(pBPA_{drt}) \times \mathbb{DP}(pBPA_{drt})$,
5. for every probabilistic bisimulation R on $\mathbb{PT}(pBPA_{drt})$ we have $R \subseteq \mathbb{SP}(pBPA_{drt}) \times \mathbb{SP}(pBPA_{drt}) \cup \mathbb{DP}(pBPA_{drt}) \times \mathbb{DP}(pBPA_{drt})$.
6. $\mu(p, M) = 0$ if $p \in \mathbb{SP}(pBPA_{drt})$ and $M \subseteq \mathbb{SP}(pBPA_{drt})$. In any other case $\mu(p, M) \geq 0$. In particular, if M is a bisimulation equivalence class then $\mu(p, M) \geq 0$ if $p \in \mathbb{SP}(pBPA_{drt})$ and $M \subseteq \mathbb{DP}(pBPA_{drt})$.

Furthermore, Remark 3.3.35 remains valid for the model of finite processes of $pBPA_{drt}$.

Proposition 5.3.24. Proposition 3.3.12 and 3.3.13 remain valid for the probabilistic bisimulation on $\mathbb{PT}(pBPA_{drt})$.

Theorem 5.3.25 (*Congruence theorem of* $pBPA_{drt}$). $\leftrightarrow$ is a congruence relation on $\mathbb{PT}(pBPA_{drt})$ with respect to the $+$, $\cdot$, $\leftthreetimes_\pi$, σ_{rel} and ν_{rel} operators.

Proof. For the proofs of the theorem concerning the operators of *pBPA* we refer to the proof of Congruence theorem of *pBPA*. To extend these proofs from *pBPA* to $pBPA_{drt}$ we have to check if the related processes as defined in the proof match on σ-transitions and the $\boldsymbol{D}$ predicate. However, given the fact that they can be easily checked, we will not give details. Moreover, from Proposition 3.3.13 we have that $\leftrightarrow$ is an equivalence relation. It remains to prove that the probabilistic bisimulation is preserved by the time operators: σ_{rel} and ν_{rel}.

The delay operator. Let x and y be $\mathbb{PT}(pBPA_{drt})$ processes such that $x \leftrightarrow y$. So, there exist probabilistic bisimulation R_1 such that $(x, y) \in R_1$. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup R_1)$,

where

$\alpha = \{(\sigma_{rel}(p), \sigma_{rel}(q)) \ : \ p, q \in \mathbb{SP}(pBPA_{drt}), (p, q) \in R_1\}$,

$\beta = \{(\sigma_{rel}(u), \sigma_{rel}(v)) \ : \ u, v \in \mathbb{DP}(pBPA_{drt}), (u, v) \in R_1\}$.

Let us note that:

D1: α and β are equivalence relations; α and R_1 contain pairs of static processes relevant to R;

D2: if $(\sigma_{rel}(p), \sigma_{rel}(q)) \in \alpha$ and $K \in \mathbb{PT}(pBPA_{drt})/\beta$, then $\sigma_{rel}(p) \rightsquigarrow K$ iff $\sigma_{rel}(q) \rightsquigarrow K$;

D3: if $\sigma_{rel}(p) \rightsquigarrow K$ for $K \in \mathbb{PT}(pBPA_{drt})/\beta$, then $K = [\sigma_{rel}(u)]_\beta$ for some u such that $p \rightsquigarrow u$. Moreover, from the definition of β we have that $K = \sigma_{rel}([u]_{R_1})$;

D4: since R_1 and β are subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(pBPA_{drt})/R$, then $M = \bigcup_{i \in I} M_i$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I and J and for some equivalence classes $M_i,\ i \in I$ and $K_j,\ j \in J$ of R_1 and β, respectively.

Now, suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}(pBPA_{drt})$ and $M \in \mathbb{DP}(pBPA_{drt})/R$. Then

1. if $(r, r_1) \in R_1$, having that $\mu(r, M_i) = \mu(r_1, M_i)$ for all $i \in I$ using Proposition 3.3.9 *ii.* the result follows.

2. if $(r, r_1) \in \alpha$, then $r \equiv \sigma_{rel}(p), r_1 \equiv \sigma_{rel}(q)$ for some p, q such that $(p, q) \in R_1$. According to **D3** and **D4**, $M = \bigcup_{j \in J} K_j$ and $K_j = [\sigma_{rel}(u_j)]_\beta$ and $p \rightsquigarrow u_j$. Then from Proposition 5.3.8 *ii.* we obtain:

   $\mu(\sigma_{rel}(p), K_j) = \mu(\sigma_{rel}(p), \sigma_{rel}([u_j]_{R_1})) = \mu(p, [u_j]_{R_1}) = \mu(q, [u_j]_{R_1}) =$

   $\mu(\sigma_{rel}(q), \sigma_{rel}([u_j]_{R_1})) = \mu(\sigma_{rel}(q), K_j)$.

   Finally, from Proposition 3.3.9 *ii.* follows that $\mu(r, M) = \mu(r_1, M)$.

The "now" operator. Let x and y be $\mathbb{PT}(\textit{pBPA}_{drt})$ processes such that $x \leftrightarrows y$. So, there exist probabilistic bisimulation R_1 such that $(x, y) \in R_1$. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup R_1)$,

where

$\alpha = \{(\nu_{rel}(p), \nu_{rel}(q)) \ : \ p, q \in \mathbb{SP}(\textit{pBPA}_{drt}), (p, q) \in R_1\}$,

$\beta = \{(\nu_{rel}(u), \nu_{rel}(v)) \ : \ u, v \in \mathbb{DP}(\textit{pBPA}_{drt}), (u, v) \in R_1\}$.

Let us note that:

NT1: α and β are equivalence relations; α and R_1 contain pairs of static processes relevant to R;

NT2: if $(\nu_{rel}(p), \nu_{rel}(q)) \in \alpha$ and $K \in \mathbb{PT}(\textit{pBPA}_{drt})/\beta$, then $\nu_{rel}(p) \rightsquigarrow K$ iff $\nu_{rel}(q) \rightsquigarrow K$;

NT3: if $\nu_{rel}(p) \rightsquigarrow K$ for $K \in \mathbb{PT}(\textit{pBPA}_{drt})/\beta$, then $K = [\nu_{rel}(u)]_\beta$ for some u such that $p \rightsquigarrow u$. Moreover, from the definition of β we have that $K = \nu_{rel}([u]_{R_1})$;

NT4: since R_1 and β are subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(\textit{pBPA}_{drt})/R$, then $M = \bigcup_{i \in I} M_i$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I and J and for some equivalence classes $M_i,\ i \in I$ and $K_j,\ j \in J$ of R_1 and β, respectively.

The rest of the proof is similar to the proof of the σ_{rel} operator.

□

Towards Soundness of *pBPA*$_{drt}$ For the axioms of *pBPA*$_{drt}$ in the form of an equation the soundness property is proved in the standard way: an equivalence relation is associated to the axiom for which we have to show that processes related by this relation simulate each other on all transitions on the value of the PDF function as well as on the $\boldsymbol{D}$ predicate. However, we will not show all details of this part of the proof. The most interesting part certainly is the proof for the conditional axioms $RSPDA2 - RSPDA5$. For processes that satisfy $z \leftrightarrows z + z$ we know from Section 4.3 that they can reach only a single equivalence class. This result remains valid in *pBPA*$_{drt}$ as well. Here we focus on the second condition that appears in the above mentioned axioms. We will prove that if the "now" part of one process y satisfies the condition $z \leftrightarrows z + z$ and the "delay" part is exactly y then the property of z to reach only a single equivalence class passes on to process y.

Lemma 5.3.26. Let x be a $\mathbb{PT}(\textit{pBPA}_{drt})$ process such that $x \leftrightarrows x + x$. Then if $x \rightsquigarrow x'$ and $x \rightsquigarrow x''$ for some $x', x'' \in \mathbb{DP}(\textit{pBPA}_{drt})$, then $x' \leftrightarrows x''$.

Proof. See Lemma 4.3.17 (pg. 106). □

Lemma 5.3.27. Let y be an $\mathbb{SP}(\textit{pBPA}_{drt})$ process and $y \leftrightarrows \nu_{rel}(z) + \sigma_{rel}(y)$ for some process z such that $z \leftrightarrows z + z$. And let $y \rightsquigarrow x_1$, $y \rightsquigarrow x_2$, ..., $y \rightsquigarrow x_n$ $(n \geq 1)$ be all possible probabilistic transitions of y. Then for all $i, j \in \{1, 2, \ldots, n\}$, $x_i \leftrightarrows x_j$.

Proof. Since $z \leftrightarrows z + z$ by Lemma 5.3.26 we can assume without loss of generality that z makes only one probabilistic transition $z \rightsquigarrow u$ and $\mu(z, u) = 1$ for some $u \in \mathbb{DP}(\textit{pBPA}_{drt})$. (1)

From the assumptions:

$$y \rightsquigarrow x_1, y \rightsquigarrow x_2, \ldots, y \rightsquigarrow x_n$$
$$y \leftrightarrows \nu_{rel}(z) + \sigma_{rel}(y) \tag{2}$$

it follows that

$$\nu_{rel}(z) + \sigma_{rel}(y) \rightsquigarrow \nu_{rel}(u) + \sigma_{rel}(x_{i'}),\ i' = 1, \ldots n, \tag{3}$$

are all possible probabilistic transition of $\nu_{rel}(z) + \sigma_{rel}(y)$. Then from (2) and (3)

$$\forall i : \exists i' : x_i \leftrightarrows \nu_{rel}(u) + \sigma_{rel}(x_{i'}). \tag{4}$$

If R is a bisimulation such that $(y, \nu_{rel}(z) + \sigma_{rel}(y)) \in R$ and $\forall i : \ (x_i, \nu_{rel}(u) + \sigma_{rel}(x_{i'})) \in R$ whose existence is guaranteed by (4), we define the following relation:

$$R' = Eq\Big(R \cup \{(x_i, x_j) \mid 1 \le i \le n, 1 \le j \le n\}\Big).$$

In order to prove that R' is a bisimulation it is sufficient to check pairs (x_i, x_j) because for the pairs in R the result is straightforward. Moreover, since $x_i, x_j \in \mathbb{DP}(pBPA_{drt})$ it is sufficient to investigate action transitions and σ-transitions (see Remark 5.3.23). Let us assume that $(x_i, x_j) \in R'$. By (4) there are $i', j' \in \{1, \ldots, n\}$ such that

$$(x_i, \nu_{rel}(u) + \sigma_{rel}(x_{i'})) \in R \subseteq R' \qquad \text{(4i)} \qquad \text{and} \qquad (x_j, \nu_{rel}(u) + \sigma_{rel}(x_{j'})) \in R \subseteq R'. \qquad \text{(4j)}$$

Action transition. If $x_i \xrightarrow{a} w_i$ for some $w_i \in \mathbb{SP}(pBPA_{drt})$ then from (4i) follows that $\nu_{rel}(u) \xrightarrow{a} w$ and from (4j) follows that $x_j \xrightarrow{a} w_j$ for some $w, w_j \in \mathbb{SP}(pBPA_{drt})$ and $(w_i, w), (w, w_j) \in R$. Clearly, $(w_i, w_j) \in R \subseteq R'$. We note that the assumption (1) is essential in this part, otherwise (4i) and (4j) are uncertain.

Action termination. In a similar way we prove $x_i \xrightarrow{a} \surd$ iff $x_j \xrightarrow{a} \surd$.

σ-transitions. From (4i) and (4j) we have that there exist $v_i, v_j \in \mathbb{DP}(pBPA_{drt})$ such that $x_i \xrightarrow{\sigma} v_i$ and $x_j \xrightarrow{\sigma} v_j$ and $(v_i, x_{i'}) \in R$ and $(v_j, x_{j'}) \in R$. Therefore, $(v_i, x_{i'}) \in R'$ and $(v_j, x_{j'}) \in R'$. Thus, $(x_{i'}, x_{j'}) \in R'$ from which $(v_i, v_j) \in R'$ (because of the symmetry and the transitivity of R').

$\boldsymbol{D}$ predicate. $\boldsymbol{D}(x_i)$ and $\boldsymbol{D}(x_j)$ because $\boldsymbol{D}(\sigma_{rel}(x_{i'}))$ and $\boldsymbol{D}(\sigma_{rel}(x_{j'}))$.

PDF. We still need to check the values of the PDF over R' equivalence classes. First note that $\mathbb{SP}(pBPA_{drt}) \times \mathbb{SP}(pBPA_{drt}) \cap R' = \mathbb{SP}(pBPA_{drt}) \times \mathbb{SP}(pBPA_{drt}) \cap R$, that is, $(p, q) \in R$ iff $(p, q) \in R'$ for $p, q \in \mathbb{SP}(pBPA_{drt})$. Second, from $R \subseteq R'$ we have that for every $M \in \mathbb{DP}(pBPA_{drt})/R'$ there are an index set I and equivalence classes $M_i \in \mathbb{DP}(pBPA_{drt})/R, i \in I$ such that $M = \bigcup_{i \in I} M_i$. Thus, if $(p, q) \in R'$ for some $p, q \in \mathbb{SP}(pBPA_{drt})$, then $(p, q) \in R$ and hence $\mu(p, M_i) = \mu(q, M_i)$ for each $i \in I$. The result $\mu(p, M) = \mu(q, M)$ follows from Proposition 3.3.9. □

Corollary 5.3.28. If y is a process as it is defined in the previous lemma then $\forall i : x_i \leftrightarrows \nu_{rel}(u) + \sigma_{rel}(x_i)$. □

Lemma 5.3.29. Let $x, u \in \mathbb{DP}(pBPA_{drt})$ be such that $x \leftrightarrows \nu_{rel}(u) + \sigma_{rel}(x)$ and let R be a probabilistic bisimulation relation such that $(x, \nu_{rel}(u) + \sigma_{rel}(x)) \in R$. Then for all processes t such that $x \xRightarrow{\sigma} t$[3] we have that $(x, t) \in R$.

Proof. The proof resembles the proof of Lemma 4.3.4.4 in [108]. □

Theorem 5.3.30 (*Soundness of pBPA$_{drt}$*). Let p and q be $\mathbb{PT}(pBPA_{drt})$ processes. If $pBPA_{drt} \vdash \mathbf{p} = \mathbf{q}$ then $p \leftrightarrows q$.

Proof. We only treat axioms added to *pBPA* to obtain *pBPA$_{drt}$*. The proofs about $\boldsymbol{D}$ predicate for the axioms of *pBPA* (that we do not treat here) are trivial. The proofs for the σ-transitions of the omitted axioms can easily be derived from the proof in [108] (Section 4.3, Theorem 4.3.1.4). For the same reason we omit the parts about action transitions and σ-transitions for axioms $DRTA3, DRTA6-7, DRT1-2$ and $DCS1-4$. For axioms $PrAC1-5$ σ-transitions do not need to be investigated (provided by Remark 5.3.23).

[3] Relation $\xRightarrow{\sigma}$ is the reflexive and transitive closure of $\xrightarrow{\sigma}$ as defined in Section 2.3.

Axiom DRTAA3. We define a relation R in the following way:

$$R = Eq\Big(\{(\underline{\underline{a}} + \underline{\underline{a}}, \underline{\underline{a}}), (\breve{\underline{\underline{a}}} + \breve{\underline{\underline{a}}}, \breve{\underline{\underline{a}}})\}\Big).$$

PDF. We only need to notice that $\mu(\underline{\underline{a}} + \underline{\underline{a}}, [\breve{\underline{\underline{a}}}]_R) = 1 = \mu(\underline{\underline{a}}, [\breve{\underline{\underline{a}}}]_R)$, and $\mu(\underline{\underline{a}} + \underline{\underline{a}}, M) = 0 = \mu(\underline{\underline{a}}, M)$ for any other equivalence class M.

$\boldsymbol{D}$ *predicate.* $\neg\boldsymbol{D}(\underline{\underline{a}} + \underline{\underline{a}})$ and $\neg\boldsymbol{D}(\underline{\underline{a}})$. $\neg\boldsymbol{D}(\breve{\underline{\underline{a}}} + \breve{\underline{\underline{a}}})$ and $\neg\boldsymbol{D}(\breve{\underline{\underline{a}}})$.

Axiom DRTA6. We define a relation R in the following way:

$$R = Eq\Big(\{(p + \underline{\underline{\delta}}, p) \ : \ p \in \mathbb{SP}(\boldsymbol{pBPA}_{drt})\} \ \cup \ \{(u + \breve{\underline{\underline{\delta}}}, u) \ : \ u \in \mathbb{DP}(\boldsymbol{pBPA}_{drt})\}\Big).$$

PDF. Since $\mu(p + \underline{\underline{\delta}}, u + \breve{\underline{\underline{\delta}}}) = \mu(p, u)$ and $(u + \breve{\underline{\underline{\delta}}} \in M$ iff $u \in M)$, from Proposition 3.3.10 follows that $\mu(p + \underline{\underline{\delta}}, M) = \mu(p, M)$ for each $M \in \mathbb{DP}(\boldsymbol{pBPA}_{drt})/R$.

$\boldsymbol{D}$ *predicate.* Since $\neg\boldsymbol{D}(\underline{\underline{\delta}})$, $\boldsymbol{D}(p + \underline{\underline{\delta}})$ iff $\boldsymbol{D}(p)$. And since $\neg\boldsymbol{D}(\breve{\underline{\underline{\delta}}})$, $\boldsymbol{D}(u + \breve{\underline{\underline{\delta}}})$ iff $\boldsymbol{D}(u)$.

Axiom DRTA7. We define a relation R in the following way:

$$R = Eq\Big(\{(\underline{\underline{\delta}} \cdot p, \underline{\underline{\delta}}) \ : \ p \in \mathbb{SP}(\boldsymbol{pBPA}_{drt})\} \cup \{(\breve{\underline{\underline{\delta}}} \cdot p, \breve{\underline{\underline{\delta}}}) \ : \ p \in \mathbb{SP}(\boldsymbol{pBPA}_{drt})\}\Big).$$

PDF. Since $\mu(\underline{\underline{\delta}} \cdot p, \breve{\underline{\underline{\delta}}} \cdot p) = \mu(\underline{\underline{\delta}}, \breve{\underline{\underline{\delta}}}) = 1$ and $[\breve{\underline{\underline{\delta}}} \cdot p]_R = [\breve{\underline{\underline{\delta}}}]_R$ it follows that $\mu(\breve{\underline{\underline{\delta}}} \cdot p, [\breve{\underline{\underline{\delta}}} \cdot p]_R) = \mu(\breve{\underline{\underline{\delta}}}, [\breve{\underline{\underline{\delta}}}]_R) = 1$. For every other equivalence class $M \in \mathbb{DP}(\boldsymbol{pBPA}_{drt})/R$, $\mu(\breve{\underline{\underline{\delta}}} \cdot p, M) = \mu(\breve{\underline{\underline{\delta}}}, M) = 0$.

$\boldsymbol{D}$ *predicate.* $\neg\boldsymbol{D}(\underline{\underline{\delta}})$ and $\neg\boldsymbol{D}(\underline{\underline{\delta}} \cdot p)$. And also $\neg\boldsymbol{D}(\breve{\underline{\underline{\delta}}})$ and $\neg\boldsymbol{D}(\breve{\underline{\underline{\delta}}} \cdot p)$

Axiom DRT1. We define a relation R in the following way:

$$\begin{aligned} R \ = \ Eq\Big(\ & \{(\sigma_{rel}(p + q), \sigma_{rel}(p) + \sigma_{rel}(q)) \ : \ p, q \in \mathbb{SP}(\boldsymbol{pBPA}_{drt})\} \\ & \cup\{(\sigma_{rel}(u + v), \sigma_{rel}(u) + \sigma_{rel}(v)) \ : \ u, v \in \mathbb{DP}(\boldsymbol{pBPA}_{drt})\}\Big). \end{aligned}$$

PDF. Suppose that $(\sigma_{rel}(p + q), \sigma_{rel}(p) + \sigma_{rel}(q)) \in R$ for some $p, q \in \mathbb{SP}(\boldsymbol{pBPA}_{drt})$ and $M \in \mathbb{DP}(\boldsymbol{pBPA}_{drt})/R$. Then, $\mu(\sigma_{rel}(p+q), \sigma_{rel}(u+v)) = \mu(p+q, u+v) = \mu(p, u) \cdot \mu(q, v)$ and $\mu(\sigma_{rel}(p)+\sigma_{rel}(q), \sigma_{rel}(u)+\sigma_{rel}(v)) = \mu(\sigma_{rel}(p), \sigma_{rel}(u))\cdot\mu(\sigma_{rel}(q), \sigma_{rel}(v)) = \mu(p, u)\cdot\mu(q, v)$. From Proposition 3.3.10 we conclude that $\mu(\sigma_{rel}(p + q), M) = \mu(\sigma_{rel}(p) + \sigma_{rel}(q), M)$ for every equivalence class M.

$\boldsymbol{D}$ *predicate.* $\boldsymbol{D}(\sigma_{rel}(p + q))$ and $\boldsymbol{D}(\sigma_{rel}(p) + \sigma_{rel}(q))$ for all $p, q \in \mathbb{PT}(\boldsymbol{pBPA}_{drt})$.

Axiom DRT2. We define a relation R in the following way:

$$\begin{aligned} R \ = \ Eq\Big(\ & \{(\sigma_{rel}(p \cdot q), \sigma_{rel}(p) \cdot q) \ : \ p, q \in \mathbb{SP}(\boldsymbol{pBPA}_{drt})\} \\ & \cup\{(\sigma_{rel}(u \cdot q), \sigma_{rel}(u) \cdot q) \ : \ u \in \mathbb{DP}(\boldsymbol{pBPA}_{drt}), q \in \mathbb{SP}(\boldsymbol{pBPA}_{drt})\}\Big). \end{aligned}$$

PDF. Suppose that $(\sigma_{rel}(p \cdot q), \sigma_{rel}(p) \cdot q) \in R$ for some $p, q \in \mathbb{SP}(\mathbf{pBPA}_{drt})$ and $M \in \mathbb{DP}(\mathbf{pBPA}_{drt})/R$. Then, $\mu(\sigma_{rel}(p \cdot q), \sigma_{rel}(u \cdot q)) = \mu(p \cdot q, u \cdot q) = \mu(p, u)$ and $\mu(\sigma_{rel}(p) \cdot q, \sigma_{rel}(u) \cdot q) = \mu(\sigma_{rel}(p), \sigma_{rel}(u)) = \mu(p, u)$. The conclusion $\mu(\sigma_{rel}(p \cdot q), M) = \mu(\sigma_{rel}(p) \cdot q, M)$ follows from Proposition 3.3.10.

***D** predicate.* $\boldsymbol{D}(\sigma_{rel}(p \cdot q))$ and $\boldsymbol{D}(\sigma_{rel}(p) \cdot q)$ for all $p, q \in \mathbb{PT}(\mathbf{pBPA}_{drt})$.

Axiom PrDRT1. We define a relation R in the following way:

$$R = Eq\Big(\{(\sigma_{rel}(p \leftthreetimes_\pi q), \sigma_{rel}(p) \leftthreetimes_\pi \sigma_{rel}(q)) \ : \ p, q \in \mathbb{SP}(\mathbf{pBPA}_{drt})\}\Big).$$

PDF. Suppose that $(\sigma_{rel}(p \leftthreetimes_\pi q), \sigma_{rel}(p) \leftthreetimes_\pi \sigma_{rel}(q)) \in R$ for some $p, q \in \mathbb{SP}(\mathbf{pBPA}_{drt})$ and $M \in \mathbb{DP}(\mathbf{pBPA}_{drt})/R$. Then $\mu(\sigma_{rel}(p \leftthreetimes_\pi q), \sigma_{rel}(u)) = \mu(p \leftthreetimes_\pi q, u) = \pi \cdot \mu(p, u) + (1-\pi) \cdot \mu(q, u)$ and
$\mu(\sigma_{rel}(p) \leftthreetimes_\pi \sigma_{rel}(q), \sigma_{rel}(u)) = \pi \cdot \mu(\sigma_{rel}(p), \sigma_{rel}(u)) + (1-\pi) \cdot \mu(\sigma_{rel}(q), \sigma_{rel}(u)) = \pi \cdot \mu(p, u) + (1-\pi) \cdot \mu(q, u)$. The conclusion $\mu(\sigma_{rel}(p \leftthreetimes_\pi q), M) = \mu(\sigma_{rel}(p) \leftthreetimes_\pi \sigma_{rel}(q), M)$ follows from Proposition 3.3.10.

***D** predicate.* $\boldsymbol{D}(\sigma_{rel}(p \leftthreetimes_\pi q))$ and $\boldsymbol{D}(\sigma_{rel}(p) \leftthreetimes_\pi \sigma_{rel}(q))$.

Axiom DCS1. We define a relation R in the following way:

$$R = Eq\Big(\{(\nu_{rel}(\underline{a}), \underline{a}), (\nu_{rel}(\breve{\underline{a}}), \breve{\underline{a}})\}\Big).$$

PDF. Since $[\nu_{rel}(\breve{\underline{a}})]_R = [\breve{\underline{a}}]_R$ we obtain $\mu(\nu_{rel}(\underline{a}), \nu_{rel}(\breve{\underline{a}})) = 1 = \mu(\underline{a}, \breve{\underline{a}})$. For any other equivalence class M, we have $\mu(\nu_{rel}(\underline{a}), M) = 0 = \mu(\underline{a}, M)$.

***D** predicate.* $\neg\boldsymbol{D}(\nu_{rel}(\underline{a}))$ and $\neg\boldsymbol{D}(\underline{a})$. And also $\neg\boldsymbol{D}(\nu_{rel}(\breve{\underline{a}}))$ and $\neg\boldsymbol{D}(\breve{\underline{a}})$.

Axiom DCS2. We define a relation R in the following way:

$$\begin{aligned} R \ = \ Eq\Big(\ & \{(\nu_{rel}(p+q), \nu_{rel}(p) + \nu_{rel}(q)) \ : \ p, q \in \mathbb{SP}(\mathbf{pBPA}_{drt})\} \\ & \cup \{(\nu_{rel}(u+v), \nu_{rel}(u) + \nu_{rel}(v)) \ : \ u, v \in \mathbb{DP}(\mathbf{pBPA}_{drt})\}\Big). \end{aligned}$$

PDF. Suppose that $(\nu_{rel}(p+q), \nu_{rel}(p) + \nu_{rel}(q)) \in R$ for some $p, q \in \mathbb{SP}(\mathbf{pBPA}_{drt})$ and $M \in \mathbb{DP}(\mathbf{pBPA}_{drt})/R$. Then, $\mu(\nu_{rel}(p+q), \nu_{rel}(u+v)) = \mu(p+q, u+v) = \mu(p, u) \cdot \mu(q, v)$ and
$\mu(\nu_{rel}(p) + \nu_{rel}(q), \nu_{rel}(u) + \nu_{rel}(v)) = \mu(\nu_{rel}(p), \nu_{rel}(u)) \cdot \mu(\nu_{rel}(q), \nu_{rel}(v)) = \mu(p, u) \cdot \mu(q, v)$. Using Proposition 3.3.10 we conclude that $\mu(\nu_{rel}(p+q), M) = \mu(\nu_{rel}(p) + \nu_{rel}(q), M)$.

***D** predicate.* $\neg\boldsymbol{D}(\nu_{rel}(p+q))$ and $\neg\boldsymbol{D}(\nu_{rel}(p) + \nu_{rel}(q))$ for all $p, q \in \mathbb{PT}(\mathbf{pBPA}_{drt})$.

Axiom DCS3. We define a relation R in the following way:

$$\begin{aligned} R \ = \ Eq\Big(\ & \{(\nu_{rel}(p \cdot q), \nu_{rel}(p) \cdot q) \ : \ p, q \in \mathbb{SP}(\mathbf{pBPA}_{drt})\} \\ & \cup \{(\nu_{rel}(u \cdot q), \nu_{rel}(u) \cdot q) \ : \ u \in \mathbb{DP}(\mathbf{pBPA}_{drt}), q \in \mathbb{SP}(\mathbf{pBPA}_{drt})\}\Big). \end{aligned}$$

PDF. Suppose that $(\nu_{rel}(p \cdot q), \nu_{rel}(p) \cdot q) \in R$ for some $p, q \in \mathbb{SP}(\textit{pBPA}_{drt})$ and $M \in \mathbb{DP}(\textit{pBPA}_{drt})/R$. Then,
$\mu(\nu_{rel}(p \cdot q), \nu_{rel}(u \cdot q)) = \mu(p \cdot q, u \cdot q) = \mu(p, u)$ and $\mu(\nu_{rel}(p) \cdot q, \nu_{rel}(u) \cdot q) = \mu(\nu_{rel}(p), \nu_{rel}(u)) = \mu(p, u)$. The conclusion $\mu(\nu_{rel}(p \cdot q), M) = \mu(\nu_{rel}(p) \cdot q, M)$ follows from Proposition 3.3.10.

D *predicate.* $\neg \boldsymbol{D}(\nu_{rel}(p \cdot q))$ and $\neg \boldsymbol{D}(\nu_{rel}(p) \cdot q)$ for all $p, q \in \mathbb{PT}(\textit{pBPA}_{drt})$.

Axiom DCS4. We define a relation R in the following way:

$$R = Eq\Big(\{(\nu_{rel}(\sigma_{rel}(p)), \underline{\delta}) \ : \ p \in \mathbb{SP}(\textit{pBPA}_{drt})\} \cup \{(\nu_{rel}(\sigma_{rel}(u)), \breve{\underline{\delta}}) \ : \ u \in \mathbb{DP}(\textit{pBPA}_{drt})\}\Big).$$

PDF. It is sufficient to notice that $\mu(\underline{\delta}, \left[\breve{\underline{\delta}}\right]_R) = \mu(\underline{\delta}, \breve{\underline{\delta}}) = 1$ and $\mu(\nu_{rel}(\sigma_{rel}(p)), \left[\breve{\underline{\delta}}\right]_R) = \mu(\nu_{rel}(\sigma_{rel}(p)), \{\nu_{rel}(\sigma_{rel}(u)) \ : \ u \in \mathbb{DP}(\textit{pBPA}_{drt})\}) = 1$. If $M \in \mathbb{DP}(\textit{pBPA}_{drt})/R, M \neq \left[\breve{\underline{\delta}}\right]_R$, then both $\mu(\underline{\delta}, M) = 0$ and $\mu(\nu_{rel}(\sigma_{rel}(p)), M) = 0$.

D *predicate.* $\neg \boldsymbol{D}(\nu_{rel}(\sigma_{rel}(p)))$ and $\neg \boldsymbol{D}(\underline{\delta})$. And $\neg \boldsymbol{D}(\nu_{rel}(\sigma_{rel}(u)))$ and $\neg \boldsymbol{D}(\breve{\underline{\delta}})$.

Axiom PrDCS1. We define a relation R in the following way:

$$R = Eq\Big(\{(\nu_{rel}(p \leftthreetimes_\pi q), \nu_{rel}(p) \leftthreetimes_\pi \nu_{rel}(q)) \ : \ p, q \in \mathbb{SP}(\textit{pBPA}_{drt})\}\Big).$$

PDF. Suppose that $(\nu_{rel}(p \leftthreetimes_\pi q), \nu_{rel}(p) \leftthreetimes_\pi \nu_{rel}(q)) \in R$ for some $p, q \in \mathbb{SP}(\textit{pBPA}_{drt})$ and $M \in \mathbb{DP}(\textit{pBPA}_{drt})/R$. Then, $\mu(\nu_{rel}(p \leftthreetimes_\pi q), \nu_{rel}(u)) = \mu(p \leftthreetimes_\pi q, u) = \pi \cdot \mu(p, u) + (1 - \pi) \cdot \mu(q, v)$ and
$\mu(\nu_{rel}(p) \leftthreetimes_\pi \nu_{rel}(q), \nu_{rel}(u)) = \pi \cdot \mu(\nu_{rel}(p), \nu_{rel}(u)) + (1 - \pi) \cdot \mu(\nu_{rel}(q), \nu_{rel}(u))$
$= \pi \cdot \mu(p, u) + (1 - \pi) \cdot \mu(q, u)$.
The conclusion $\mu(\nu_{rel}(p \leftthreetimes_\pi q), M) = \mu(\nu_{rel}(p) \leftthreetimes_\pi \nu_{rel}(q), M)$ follows from Proposition 3.3.10.

D *predicate.* $\neg \boldsymbol{D}(\nu_{rel}(p \leftthreetimes_\pi q))$ and $\neg \boldsymbol{D}(\nu_{rel}(p) \leftthreetimes_\pi \nu_{rel}(q))$.

Axiom RSPDA1. We define a relation R in the following way:

$$R = Eq\Big(\{(a, \underline{a} + \sigma_{rel}(a)), (\breve{a}, \breve{\underline{a}} + \sigma_{rel}(\breve{a}))\}\Big).$$

PDF. It is sufficient to notice that $\mu\left(a, [\breve{a}]_R\right) = 1 = \mu(\underline{a} + \sigma_{rel}(a), \left[\breve{\underline{a}} + \sigma_{rel}(\breve{a})\right]_R)$ and $[\breve{a}]_R = \left[\breve{\underline{a}} + \sigma_{rel}(\breve{a})\right]_R$.

D *predicate.* $\boldsymbol{D}(a)$ and $\boldsymbol{D}(\sigma_{rel}(a))$ from which $\boldsymbol{D}(\underline{a} + \sigma_{rel}(a))$ as well.

Axiom RSPDA2. Let us assume that $y \leftrightarrow \underline{a} + \sigma_{rel}(y)$. Lemma 5.3.27 allows us to assume without loss of generality that y makes only one probabilistic transition. Namely, there is $x \in \mathbb{DP}(\textit{pBPA}_{drt})$ such that $y \rightsquigarrow x$ and $\mu(y, x) = 1$ and $x \leftrightarrow \breve{\underline{a}} + \sigma_{rel}(x)$. (2.1)
Let R be a probabilistic bisimulation such that
$(y, \underline{a} + \sigma_{rel}(y)) \in R$ and $(x, \breve{\underline{a}} + \sigma_{rel}(x)) \in R$. (2.2)
Then we define the following relation:

$$R' = Eq\Big(R \cup \{(y, a)\} \cup \{(t, \breve{a}) \mid \forall t : x \stackrel{\sigma}{\Longrightarrow} t\}\Big).$$

Note that $(x, \breve{a}) \in R'$. Moreover, (y, a) is the only new pair of static processes and $(t, \breve{a})$ are all pairs of dynamic processes.

PDF. For (y, a), since $[x]_{R'} = [\breve{a}]_{R'}$ and $\mu(y, [x]_{R'}) = 1$ (from (2.1)) and $\mu(a, [\breve{a}]_{R'}) = 1$ (from the definition) the result follows.

Now, let us consider the pair $(t, \breve{a}) \in R'$ where $x \stackrel{\sigma}{\Longrightarrow} t$. By Lemma 5.3.29 we have $(x, t) \in R$. (2.3)

Action termination. From (2.2) and (2.3) we obtain that $x \stackrel{a}{\to} \surd$ and also $t \stackrel{a}{\to} \surd$ are the only possible action transitions of x and t respectively. Also, $\breve{a} \stackrel{a}{\to} \surd$.

σ-transitions. Clearly, $\breve{a} \stackrel{\sigma}{\to} \breve{a}$. From (2.2) it follows that x makes a σ-transition. Therefore, from (2.3) follows that $t \stackrel{\sigma}{\to} t'$ for some $t' \in \mathbb{DP}(\textit{pBPA}_{drt})$. Thus $x \stackrel{\sigma}{\Longrightarrow} t'$. From the definition of R' we obtain $(\breve{a}, t') \in R'$.

***D* predicate.** $\boldsymbol{D}(a)$, and since $\boldsymbol{D}(\sigma_{rel}(y))$ according to (2.2) we obtain $\boldsymbol{D}(y)$. Similarly, $\boldsymbol{D}(\breve{a})$, and since $\boldsymbol{D}(x)$ according to (2.2) and (2.3) we obtain $\boldsymbol{D}(t)$.

Axiom RSPDA3. The proof of this conditional axiom is similar to the previous proof. For this axiom instead of action terminations we should consider action transitions.

Axiom RSPDA4. Let be $y \leftrightarrows \underline{a} + \nu_{rel}(z) + \sigma_{rel}(y)$ and $y_1 \leftrightarrows \nu_{rel}(z) + \sigma_{rel}(y_1)$ and $z \leftrightarrows z + z$. Lemma 5.3.27 and Lemma 4.3.17 allow us to assume without loss of generality that y, y_1 and z make only one probabilistic transition. This we assume that $y \rightsquigarrow x$ and $\mu(y, x) = 1$, $y_1 \rightsquigarrow x_1$ and $\mu(y_1, x_1) = 1$, $z \rightsquigarrow u$ and $\mu(z, u) = 1$ for some $x, x_1, z \in \mathbb{DP}(\textit{pBPA}_{drt})$. Let R be a probabilistic bisimulation such that:

$(y, \underline{a} + \nu_{rel}(z) + \sigma_{rel}(y)) \in R$, (4.1) $(x, \breve{\underline{a}} + \nu_{rel}(u) + \sigma_{rel}(x)) \in R$, (4.4)
$(y_1, \nu_{rel}(z) + \sigma_{rel}(y_1)) \in R$, (4.2) $(x_1, \nu_{rel}(u) + \sigma_{rel}(x_1)) \in R$, (4.5)
$(z, z + z) \in R$, (4.3) $(u, u + u) \in R$. (4.6)

The existence of such a relation is guaranteed by the fact that all related processes are bisimilar. Furthermore, from Lemma 5.3.29 we have that if $x \stackrel{\sigma}{\Longrightarrow} t$ and $x_1 \stackrel{\sigma}{\Longrightarrow} t_1$, then

$(x, t) \in R$ (4.7) and $(x_1, t_1) \in R$. (4.8)

We define the following relation:

$$R' = Eq\Big(R \cup \{(y, a + y_1)\} \cup \{(t, \breve{a} + t_1) \mid \forall t, t_1 : x \stackrel{\sigma}{\Longrightarrow} t \;\&\; x_1 \stackrel{\sigma}{\Longrightarrow} t_1\}\Big).$$

Note that $(x, a + x_1) \in R'$; $(y, a + y_1)$ is the only new pair of static processes; $(t, \breve{a} + t_1)$ are pairs of dynamic processes.

Probabilistic transitions. For the pair $(y, a + y_1)$: from the definition of R' we have $[x]_{R'} = [\breve{a} + x_1]_{R'}$. Thus we have $\mu(y, [x]_{R'}) = 1$ and $\mu(a + y_1, [\breve{a} + x_1]_{R'}) = 1$. For any other equivalence class M we have $\mu(y, M) = 0 = \mu(a + y_1, M)$.

Action transitions. For the pairs $(t, \breve{a} + t_1)$: Let $(t, \breve{a} + t_1) \in R'$ and $x \stackrel{\sigma}{\Longrightarrow} t$ and $x_1 \stackrel{\sigma}{\Longrightarrow} t_1$. And let us assume that $\breve{a} + t_1 \stackrel{b}{\to} r_1$ for some $r_1 \in \mathbb{SP}(\textit{pBPA}_{drt})$. Then for some $s_1, o, s, r \in \mathbb{SP}(\textit{pBPA}_{drt})$,

$t_1 \stackrel{b}{\to} r_1$ (from the deduction rules), $x_1 \stackrel{b}{\to} s_1$ and $(r_1, s_1) \in R$ (from (4.8)),

$\nu_{rel}(u) \stackrel{b}{\to} o$ and $(s_1, o) \in R$ (from (4.5)),

$x \stackrel{b}{\to} s$ and $(o, s) \in R$ (from (4.4)),

$t \stackrel{b}{\to} r$ and $(s, r) \in R$ (from (4.7)).

Thus, if $\breve{a} + t_1 \stackrel{b}{\to} r_1$ then $t \stackrel{b}{\to} r$ and $(r_1, r) \in R \subseteq R'$.

If $t \xrightarrow{b} r$ for some $r \in \mathbb{SP}(pBPA_{drt})$, then for some $s, o, s_1, r_1 \in \mathbb{SP}(pBPA_{drt})$,
$x \xrightarrow{b} r$ and $(r, s) \in R$ (from (4.7)),
$\nu_{rel}(u) \xrightarrow{b} o$ and $(s, o) \in R$ (from (4.4)),
$x_1 \xrightarrow{b} s_1$ and $(o, s_1) \in R$ (from (4.5)),
$t_1 \xrightarrow{b} r_1$ and $(s_1, r_1) \in R$ (from (4.8)), and $\breve{a} + t_1 \xrightarrow{b} r_1$ (from the deduction rules).
Thus, if $t \xrightarrow{b} r$ then $\breve{a} + t_1 \xrightarrow{b} r_1$ and $(r, r_1) \in R \subseteq R'$.

Action termination. For the pairs $(t, \breve{a} + t_1)$: If $\breve{a} + t_1 \xrightarrow{b} \surd$ then either $b \equiv a$ in which case the result follows from (4.4) and (4.7). Or $t_1 \xrightarrow{b} \surd$ and the result can be proven in a similar way (with the same trace) as in the case of action transition.
If $t \xrightarrow{b} \surd$ then from (4.7) we have $x \xrightarrow{b} \surd$ and from (4.4) we have that either $b \equiv a$ and then $\breve{a} + t_1 \xrightarrow{a} \surd$ or $\nu_{rel}(u) \xrightarrow{b} \surd$ in which case from (4.5) and (4.8) we obtain $t_1 \xrightarrow{b} \surd$ and $\breve{a} + t_1 \xrightarrow{b} \surd$ as well.

σ-transitions. For the pairs $(t, \breve{a}+t_1)$: From (4.8) and (4.5) we have that for certain s_1, $t_1 \xrightarrow{\sigma} s_1$. Since $\breve{a} \xrightarrow{\sigma} \breve{a}$ we obtain $\breve{a}+t_1 \xrightarrow{\sigma} \breve{a}+s_1$. Moreover, $x_1 \xRightarrow{\sigma} t_1$ and $t_1 \xrightarrow{\sigma} s_1$ imply $x_1 \xRightarrow{\sigma} s_1$. On the other side, from (4.7) and (4.4) it follows that $t \xrightarrow{\sigma} s$ for some s. Thus $x \xRightarrow{\sigma} t$ and $t \xrightarrow{\sigma} s$ from which $x \xRightarrow{\sigma} s$. Finally, from the definition of R' we conclude that $(s, \breve{a} + s_1) \in R'$.

***D* predicate.** $\boldsymbol{D}(a + y_1)$, and from (4.1) follows that $\boldsymbol{D}(y)$. Similarly, $\boldsymbol{D}(\breve{a} + x_1)$ and from (4.4) and (4.7) we obtain $\boldsymbol{D}(t)$ as well.

Axiom RSPDA5. The proof of this conditional axiom is similar to the proof of RSPDA4. They differ slightly in the part of the proof considering action transitions.

□

Completeness of *pBPA*$_{drt}$

To prove completeness for *pBPA*$_{drt}$ with respect to the presented model $\mathcal{M}_{pBPA_{drt}}$ we use the direct method. The proof is based on steps comparable to those in the proof of the completeness property of *pBPA* in Section 3.3.3. Again we split the proof into two lemmas, one concerning the basic $\mathcal{B}(pBPA_{drt}) \setminus \mathcal{B}_+(pBPA_{drt})$ terms, and the other one concerning the basic $\mathcal{B}_+(pBPA_{drt})$ terms. The completeness property of *pBPA*$_{drt}$ follows easily from these lemmas.

Proposition 5.3.31. Proposition 3.3.27, 3.3.52, 3.3.56 Corollary 3.3.53, Lemma 3.3.54 remain valid in *pBPA*$_{drt}$ when *pBPA* is replaced by *pBPA*$_{drt}$.

Proposition 5.3.32. If $x, y, z \in \mathbb{D}(pBPA_{drt})$, then $z \leftrightarrows x + y$ implies $z \leftrightarrows x + z$.

Proof. Consider the following relation:

$$R' = Eq\Big(\{(z, x + z)\} \quad \cup \quad \{(v + u, u) \ : \ \exists w : (v + w, u) \in R \ \& \ u, v, w \in \mathbb{DP}(pBPA_{drt})\}$$
$$\cup \quad \{(v + u, u) \ : \ (v, u) \in R \ \& \ u, v \in \mathbb{DP}(pBPA_{drt})\} \cup R\Big),$$

where R is a bisimulation relation such that $(x + y, z) \in R$.

Probabilistic transitions. As $x, y, z \in \mathbb{D}(pBPA_{drt})$ from Proposition 5.3.11 we obtain that $x \rightsquigarrow \breve{x}$, $y \rightsquigarrow \breve{y}$ and $z \rightsquigarrow \breve{z}$ are the only possible probabilistic transitions of x, y and z, respectively, with $\mu(x, \breve{x}) = 1$, $\mu(y, \breve{y}) = 1$ and $\mu(z, \breve{z}) = 1$. Thus we have that the only possible probabilistic transition of $x + z$ is $x + z \rightsquigarrow \breve{x} + \breve{z}$ and $\mu(x + z, \breve{x} + \breve{z}) = 1$. Moreover from $(x + y, z) \in R$ we obtain easily that $(\breve{x} + \breve{y}, \breve{z}) \in R$ from which by the definition of R' we have $(\breve{x} + \breve{z}, \breve{z}) \in R'$.

Let us assume that $(v + u, u) \in R'$ for some $u, v \in \mathbb{DP}(pBPA_{drt})$ and let $w \in \mathbb{DP}(pBPA_{drt})$ such that $(v + w, u) \in R$.

Action transitions. If $u \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathbb{SP}(pBPA_{drt})$, then $v + u \xrightarrow{a} p$ as well and $(p, p) \in R'$. If $v + u \xrightarrow{a} p$ and $v \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathbb{SP}(pBPA_{drt})$, then $v + w \xrightarrow{a} p$ and therefore $u \xrightarrow{a} q$ for some $q \in \mathbb{SP}(pBPA_{drt})$ such that $(p, q) \in R$ which implies that $(p, q) \in R'$.

Action termination. If $u \xrightarrow{a} \surd$ for some $a \in A$, then $v + u \xrightarrow{a} \surd$. If $v + u \xrightarrow{a} \surd$ and $v \xrightarrow{a} \surd$ for some $a \in A$, then $v + w \xrightarrow{a} \surd$ from which $u \xrightarrow{a} \surd$ as well.

σ-transitions. If $u \xrightarrow{\sigma} s$ for some $s \in \mathbb{DP}(pBPA_{drt})$. Then $v + w \xrightarrow{\sigma} r$ for some r such that $(r, s) \in R$. The following situations are possible:

1. if $v \xrightarrow{\sigma} r$ and $w \not\xrightarrow{\sigma}$ then $v + u \xrightarrow{\sigma} r + s$ and $(r + s, s) \in R'$ since $(r, s) \in R$;
2. if $v \not\xrightarrow{\sigma}$ and $w \xrightarrow{\sigma} r$ then $v + u \xrightarrow{\sigma} s$ and $(s, s) \in R'$;
3. if $v \xrightarrow{\sigma} p$ and $w \xrightarrow{\sigma} q$ for some p, q such that $r \equiv p + q$, then $v + u \xrightarrow{\sigma} p + s$ and $(p + s, s) \in R'$ since there is q such that $(p + q, s) \in R$.

If $v + u \xrightarrow{\sigma} r$ for $r \in \mathbb{DP}(pBPA_{drt})$, then either $u \xrightarrow{\sigma} r$ and $v \not\xrightarrow{\sigma}$ and this case is trivial, or $v \xrightarrow{\sigma} p$, $u \xrightarrow{\sigma} q$ and $r \equiv p + q$. There are two cases:

1. if $w \xrightarrow{\sigma} s$ for some s, then $v + w \xrightarrow{\sigma} p + s$ and $(p + s, q) \in R$ and therefore, $(p + q, q) \in R'$;
2. if $w \not\xrightarrow{\sigma}$, then $v + w \xrightarrow{\sigma} p$ and $(p, q) \in R$ and therefore, $(p, q) \in R'$.

Now, we investigate the pairs $(v + u, u) \in R'$ for some $u, v \in \mathbb{DP}(pBPA_{drt})$ such that $(v, u) \in R$.

Action transitions. If $u \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathbb{SP}(pBPA_{drt})$, then $v + u \xrightarrow{a} p$ as well and $(p, p) \in R'$. If $v + u \xrightarrow{a} p$ and $v \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathbb{SP}(pBPA_{drt})$, because $(v, u) \in R$ we have that $u \xrightarrow{a} q$ for some q such that $(p, q) \in R$ which implies that $(p, q) \in R'$.

Action termination. Since $(v, u) \in R$ it follows easily that $v + u \xrightarrow{a} \surd$ iff $u \xrightarrow{a} \surd$ for some $a \in A$.

σ-transitions. If $u \xrightarrow{\sigma} s$ for some $s \in \mathbb{DP}(pBPA_{drt})$, then $v \xrightarrow{\sigma} r$ for some r such that $(r, s) \in R$. Therefore $v + u \xrightarrow{\sigma} r + s$ and $(r + s, s) \in R'$ since $(r, s) \in R$. If $v + u \xrightarrow{\sigma} s$ for some $s \in \mathbb{DP}(pBPA_{drt})$, then because $(v, u) \in R$ it must be that both processes can perform σ-transitions. Thus we have that $v \xrightarrow{\sigma} s'$ and $u \xrightarrow{\sigma} s''$ for s', s'' such that $s \equiv s' + s''$. Finally, we obtain $u \xrightarrow{\sigma} s''$ and $(s'', s) \in R'$ because there is an s' such that $(s'' + s', s) \in R$.

***D** predicate.* The proof for the $\boldsymbol{D}$ predicate for all pairs in R' is trivial.

□

Proposition 5.3.33. Let x be a $\mathbb{D}(pBPA_{drt})$ process and $a \in A$. Then:

i. if $\breve{x} \xrightarrow{a} \surd$, then $pBPA_{drt} \vdash \mathbf{x} = \underline{\mathbf{a}} + \mathbf{x}$;

ii. if $\breve{x} \xrightarrow{a} x'$, then $pBPA_{drt} \vdash \mathbf{x} = \underline{\underline{\mathbf{a}}} \cdot \mathbf{x}' + \mathbf{x}$ and $op(x') < op(x)$;

iii. if $\breve{x} \not\xrightarrow{g}$, then $pBPA_{drt} \vdash \mathbf{x} = \nu_{rel}(\mathbf{x})$;

iv. if $\breve{x} \not\xrightarrow{g}$ for each $a \in A$, then $pBPA_{drt} \vdash \nu_{rel}(\mathbf{x}) = \underline{\underline{\boldsymbol{\delta}}}$;

v. if $\breve{x} \xrightarrow{\sigma} \breve{x'}$, then $pBPA_{drt} \vdash \mathbf{x} = \sigma_{rel}(\mathbf{x}') + \nu_{rel}(\mathbf{x})$ and either $x \not\equiv x'$ and $op(y) < op(x)$ or $x \equiv x'$.

Proof. The proofs of *i.* and *ii.* are similar to the proof of Proposition 3.3.55.

iii. Let us suppose that $\breve{x} \not\xrightarrow{g}$. The Elimination theorem and the Soundness theorems allow us to assume, without loss of generality, that $\mathbf{x}$ is a basic term. Moreover, $x \in \mathbb{D}(pBPA_{drt})$ implies $\mathbf{x} \in \mathcal{B}_+(pBPA_{drt})$.

Case $\mathbf{x} \equiv \underline{\underline{\mathbf{a}}}$, $a \in A_\delta$. The result follows from the axiom $DCS1$;

Case $\mathbf{x} \equiv \underline{\underline{\mathbf{a}}} \cdot \mathbf{x}'$, $a \in A_\delta$. $pBPA_{drt} \vdash \nu_{rel}(\mathbf{x}) = \nu_{rel}(\underline{\underline{\mathbf{a}}} \cdot \mathbf{x}') = \nu_{rel}(\underline{\underline{\mathbf{a}}}) \cdot \mathbf{x}' = \underline{\underline{\mathbf{a}}} \cdot \mathbf{x}' = \mathbf{x}$;

Case $\mathbf{x} \equiv \mathbf{y} + \mathbf{z}$. From the assumption $\breve{x} \not\xrightarrow{g}$ it follows that both $\breve{y} \not\xrightarrow{g}$ and $\breve{z} \not\xrightarrow{g}$. By the induction hypothesis we have that $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y})$ and $pBPA_{drt} \vdash \mathbf{z} = \nu_{rel}(\mathbf{z})$. Finally, we obtain: $pBPA_{drt} \vdash \mathbf{x} = \mathbf{y} + \mathbf{z} = \nu_{rel}(\mathbf{y}) + \nu_{rel}(\mathbf{z}) = \nu_{rel}(\mathbf{y} + \mathbf{z}) = \nu_{rel}(\mathbf{x})$;

Case $\mathbf{x} \equiv \mathbf{a}$ *or* $\mathbf{x} \equiv \mathbf{a} \cdot \mathbf{x}'$ *or* $\mathbf{x} \equiv \sigma_{rel}(\mathbf{x}')$, $a \in A_\delta$. This case does not apply because the assumption $x \not\xrightarrow{g}$ is not fulfilled.

iv. Let us assume that $x \not\xrightarrow{g}$ for every $a \in A$. The proof is given by induction on the structure of $\mathbb{D}(pBPA_{drt})$ process x.

Case $x \equiv \underline{\underline{\delta}}$ *or* $x \equiv \delta$ The result follows directly from the axioms;

Case $x \equiv \underline{\underline{a}}$ *or* $x \equiv a$, $a \in A$. The assumption is not satisfied;

Case $x \equiv y \cdot z$. From the assumption $x \not\xrightarrow{g}$ for every $a \in A$ by the operational semantics we obtain that $y \not\xrightarrow{g}$ for every $a \in A$. Then by the induction hypothesis we have $pBPA_{drt} \vdash \nu_{rel}(\mathbf{y}) = \underline{\underline{\boldsymbol{\delta}}}$. Thus, $pBPA_{drt} \vdash \nu_{rel}(\mathbf{x}) = \nu_{rel}(\mathbf{y} \cdot \mathbf{z}) = \nu_{rel}(\mathbf{y}) \cdot \mathbf{z} = \underline{\underline{\boldsymbol{\delta}}} \cdot \mathbf{z} = \underline{\underline{\boldsymbol{\delta}}}$;

Case $x \equiv y + z$. From the assumption $x \not\xrightarrow{g}$ for every $a \in A$ by the operational semantics we obtain that $y \not\xrightarrow{g}$ and $z \not\xrightarrow{g}$ for every $a \in A$. Then by the induction hypothesis we have $pBPA_{drt} \vdash \nu_{rel}(\mathbf{y}) = \underline{\underline{\boldsymbol{\delta}}}$ and $\nu_{rel}(\mathbf{z}) = \underline{\underline{\boldsymbol{\delta}}}$. Thus, $pBPA_{drt} \vdash \nu_{rel}(\mathbf{x}) = \nu_{rel}(\mathbf{y}) + \nu_{rel}(\mathbf{z}) = \underline{\underline{\boldsymbol{\delta}}} + \underline{\underline{\boldsymbol{\delta}}} = \underline{\underline{\boldsymbol{\delta}}}$;

Case $x \equiv \sigma_{rel}(y)$. The result follows from the axiom $DCS4$;

Case $x \equiv \nu_{rel}(y)$. From the assumption $x \not\xrightarrow{g}$ for every $a \in A$, follows that $y \not\xrightarrow{g}$ for every $a \in A$. By the induction hypothesis we have $pBPA_{drt} \vdash \nu_{rel}(\mathbf{y}) = \underline{\underline{\boldsymbol{\delta}}}$. It implies $pBPA_{drt} \vdash \nu_{rel}(\mathbf{x}) = \nu_{rel}(\nu_{rel}(\mathbf{y})) = \nu_{rel}(\underline{\underline{\boldsymbol{\delta}}}) = \underline{\underline{\boldsymbol{\delta}}}$.

v. Let us assume that $\breve{x} \xrightarrow{\sigma} \breve{x}'$. The proof is given by the induction on the structure of x.

Case $x \equiv \underline{\underline{a}}$, $a \in A_\delta$ *or* $x \equiv \nu_{rel}(y)$. This cases do not apply because the assumption is not satisfied;

Case $x \equiv a$, $a \in A_\delta$. $\breve{a} \xrightarrow{\sigma} \breve{a}$ is the only possible σ-transition and $x \equiv x'$. Then, $pBPA_{drt} \vdash \mathbf{x} = \mathbf{a} = \underline{\underline{\mathbf{a}}} + \sigma_{rel}(\mathbf{a}) = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x})$;

Case $x \equiv y \cdot z$. $\breve{y} \xrightarrow{\sigma} \breve{y}'$ and $x' \equiv y' \cdot z$. By applying the induction hypothesis on y' we obtain:

Subcase $y \not\equiv y'$ *and* $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$ *and* $op(y') < op(y)$. Then $x \not\equiv x'$, $op(x') = op(y' \cdot z) = op(y') + op(z) + 1 < op(y) + op(z) + 1 = op(x)$ and $pBPA_{drt} \vdash \mathbf{x} = \mathbf{y}\cdot\mathbf{z} = (\nu_{rel}(\mathbf{y})+\sigma_{rel}(\mathbf{y}'))\cdot\mathbf{z} = \nu_{rel}(\mathbf{y})\cdot\mathbf{z}+\sigma_{rel}(\mathbf{y}')\cdot\mathbf{z} = \nu_{rel}(\mathbf{y}\cdot\mathbf{z})+\sigma_{rel}(\mathbf{y}'\cdot\mathbf{z}) = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x}')$;

Subcase $y \equiv y'$ *and* $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y})$. Then $x \equiv y \cdot z \equiv y' \cdot z \equiv x'$ and $pBPA_{drt} \vdash \mathbf{x} = \mathbf{y} \cdot \mathbf{z} = (\nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y})) \cdot \mathbf{z} = \nu_{rel}(\mathbf{y} \cdot \mathbf{z}) + \sigma_{rel}(\mathbf{y} \cdot \mathbf{z}) = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x})$;

Case $x \equiv \sigma_{rel}(y)$. From the definition of the deduction rules it is clear that $y \equiv x'$. Moreover, $op(x') < op(x)$ and:
$pBPA_{drt} \vdash \mathbf{x} = \sigma_{rel}(\mathbf{x}') = \underline{\underline{\boldsymbol{\delta}}} + \sigma_{rel}(\mathbf{x}') = \nu_{rel}(\sigma_{rel}(\mathbf{x})) + \sigma_{rel}(\mathbf{x}') = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x}')$;

Case $x \equiv y + z$. From the assumption $\breve{x} \xrightarrow{\sigma} x'$ we obtain that one of the following situations is possible:

Subcase $\breve{y} \xrightarrow{\sigma} \breve{y}'$ *and* $\breve{z} \xrightarrow{\sigma} \breve{z}'$. By the induction hypothesis we have:

1. $y \not\equiv y'$, $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$, $op(y') < op(y)$ and $z \not\equiv z'$, $pBPA_{drt} \vdash \mathbf{z} = \nu_{rel}(\mathbf{z}) + \sigma_{rel}(\mathbf{z}')$, $op(z') < op(z)$: then $x \not\equiv x'$, $op(x') = op(y') + op(z') + 1 < op(y) + op(z) + 1 = op(x)$ and $pBPA_{drt} \vdash \mathbf{x} = \mathbf{y}+\mathbf{z} = \nu_{rel}(\mathbf{y})+\sigma_{rel}(\mathbf{y}')+\nu_{rel}(\mathbf{z})+\sigma_{rel}(\mathbf{z}') = \nu_{rel}(\mathbf{y}+\mathbf{z})+\sigma_{rel}(\mathbf{y}'+\mathbf{z}') = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x}')$;
2. $y \not\equiv y'$, $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$, $op(y') < op(y)$ and $z \equiv z'$, $pBPA_{drt} \vdash \mathbf{z} = \nu_{rel}(\mathbf{z}) + \sigma_{rel}(\mathbf{z})$: then $x \not\equiv x'$, $op(x') = op(y') + op(z) + 1 < op(y) + op(z) + 1 = op(x)$ and $pBPA_{drt} \vdash \mathbf{x} = \mathbf{y}+\mathbf{z} = \nu_{rel}(\mathbf{y})+\sigma_{rel}(\mathbf{y}')+\nu_{rel}(\mathbf{z})+\sigma_{rel}(\mathbf{z}) = \nu_{rel}(\mathbf{y}+\mathbf{z})+\sigma_{rel}(\mathbf{y}'+\mathbf{z}) = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x}')$;
3. $y \equiv y'$, $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y})$ and $z \not\equiv z'$, $pBPA_{drt} \vdash \mathbf{z} = \nu_{rel}(\mathbf{z}) + \sigma_{rel}(\mathbf{z}')$, $op(z') < op(z)$: it can be proved in a similar way as the previous case;
4. $y \equiv y'$, $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y})$ and $z \equiv z'$, $pBPA_{drt} \vdash \mathbf{z} = \nu_{rel}(\mathbf{z}) + \sigma_{rel}(\mathbf{z})$: then $x \equiv y' + z' \equiv x'$ and $pBPA_{drt} \vdash \mathbf{x} = \mathbf{y} + \mathbf{z} = \nu_{rel}(\mathbf{y} + \mathbf{z}) + \sigma_{rel}(\mathbf{y} + \mathbf{z}) = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x})$;

Subcase $\breve{y} \xrightarrow{\sigma} \breve{y}'$ *and* $\breve{z} \not\xrightarrow{g}$ *and* $x' \equiv y'$. From *iv.* we have $pBPA_{drt} \vdash \mathbf{z} = \nu_{rel}(\mathbf{z})$. By the induction hypothesis the following cases can occur:

1. $y \not\equiv y'$, $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$ and $op(y') < op(y)$: then $x \not\equiv x'$, $op(x') = op(y') < op(y) < op(y) + op(z) + 1 = op(x)$ and $pBPA_{drt} \vdash \mathbf{x} = \mathbf{y} + \mathbf{z} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') + \nu_{rel}(\mathbf{z}) = \nu_{rel}(\mathbf{y} + \mathbf{z}) + \sigma_{rel}(\mathbf{y}') = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x}')$;
2. $y \equiv y'$, $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y})$: then $x \not\equiv x'$, $op(x') = op(y') < op(y) + op(z) + 1 = op(x)$ and $pBPA_{drt} \vdash \mathbf{x} = \mathbf{y} + \mathbf{z} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}) + \nu_{rel}(\mathbf{z}) = \nu_{rel}(\mathbf{y} + \mathbf{z}) + \sigma_{rel}(\mathbf{y}) = \nu_{rel}(\mathbf{x}) + \sigma_{rel}(\mathbf{x}')$.

Subcase $\breve{z} \xrightarrow{\sigma} \breve{z}'$ *and* $\breve{y} \not\xrightarrow{g}$ *and* $x' \equiv z'$. The proof is similar to the proof of the previous subcase. □

Lemma 5.3.34. If $\mathbf{u}$ and $\mathbf{v}$ are basic terms such that at least one of them belongs to $\mathcal{B}(pBPA_{drt}) \setminus \mathcal{B}_+(pBPA_{drt})$ and if

$$\forall \mathbf{x}, \mathbf{y} \in \mathcal{B}_+(pBPA_{drt}) \; : \; op(\mathbf{x}) + op(\mathbf{y}) < op(\mathbf{u}) + op(\mathbf{v}) \Rightarrow (x + y \leftrightarrows y \Rightarrow \mathbf{x} + \mathbf{y} = \mathbf{y}), \qquad (5.3)$$

then $u \leftrightarrows v \Rightarrow pBPA_{drt} \vdash \mathbf{u} = \mathbf{v}$.

Proof. The proof is almost the same as the proof of Lemma 3.3.58, only *pBPA* should be replaced by $pBPA_{drt}$ and the relevant properties of $pBPA_{drt}$ should be used instead of the used properties of *pBPA*. □

Lemma 5.3.35. If $\mathbf{x}$ and $\mathbf{y}$ are basic $\mathcal{B}_+(pBPA_{drt})$ terms, then:

$$x + y \leftrightarrows y \Rightarrow pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{y}.$$

Proof. The lemma is proved by induction on $op(\mathbf{x}) + op(\mathbf{y})$ and case distinction on the structure of $\mathbf{x}$.

Case $\mathbf{x} \equiv \underline{\underline{\boldsymbol{\delta}}}$. The result follows from the axiom DRTA6;

Case $\mathbf{x} \equiv \underline{\underline{\mathbf{a}}}$, $a \in A$. $\breve{x} \xrightarrow{a} \surd$ from which $\breve{x} + \breve{y} \xrightarrow{a} \surd$. From the assumption $x + y \leftrightarrows y$ we have that $\breve{y} \xrightarrow{a} \surd$. Then $pBPA_{drt} \vdash \mathbf{y} = \underline{\underline{\mathbf{a}}} + \mathbf{y}$ (from Proposition 5.3.33 *i.*) and also $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \underline{\underline{\mathbf{a}}} + \mathbf{y} = \mathbf{y}$;

Case $\mathbf{x} \equiv \boldsymbol{\delta}$. Since $\breve{x} \xrightarrow{\sigma} \breve{\delta}$ it follows that $\breve{y} \xrightarrow{\sigma} \breve{y}'$ and $\delta + y' \leftrightarrows y'$. From Proposition 5.3.33 *v.* we obtain $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$ and:

Subcase $y \equiv y'$. $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \boldsymbol{\delta} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}) = \underline{\underline{\boldsymbol{\delta}}} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\boldsymbol{\delta} + \mathbf{y}) = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{x} + \mathbf{y})$. Since $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y})$ from Proposition 5.2.15 it follows that $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{y}$;

Subcase $y \not\equiv y'$ *and* $op(y') < op(y)$. From $\delta + y' \leftrightarrows y'$ and the induction hypothesis we obtain $pBPA_{drt} \vdash \boldsymbol{\delta} + \mathbf{y}' = \mathbf{y}'$. Therefore, $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \boldsymbol{\delta} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \underline{\underline{\boldsymbol{\delta}}} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\boldsymbol{\delta} + \mathbf{y}') = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \mathbf{y}$;

Case $\mathbf{x} \equiv \mathbf{a}$, $a \in A$. $\breve{x} \xrightarrow{a} \surd$ from which $\breve{x} + \breve{y} \xrightarrow{a} \surd$. From the assumption $x + y \leftrightarrows y$ we have that $\breve{y} \xrightarrow{a} \surd$. Then by Proposition 5.3.33 *i.* we have that $pBPA_{drt} \vdash \mathbf{y} = \underline{\underline{\mathbf{a}}} + \mathbf{y}$. Then,
$pBPA_{drt} \vdash \nu_{rel}(\mathbf{y}) = \underline{\underline{\mathbf{a}}} + \nu_{rel}(\mathbf{y})$. (1)
Moreover, from $\breve{x} \xrightarrow{\sigma} \breve{a}$ it follows that $\breve{y} \xrightarrow{\sigma} \breve{y}'$ and $a + y' \leftrightarrows y'$. (2)
From Proposition 5.3.33 *v.* and (2) follows that $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$. (3)
We investigate the two possibilities:

Subcase $y \equiv y'$. $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y})$. (3')
and from (3') and (1) we obtain
$pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{a} + \mathbf{y} = \mathbf{a} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}) = \underline{\underline{\mathbf{a}}} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{a} + \mathbf{y})$
$= \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{x} + \mathbf{y})$. (4)
Finally, from (3') and (4) and Proposition 5.2.15 we obtain $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{y}$;

Subcase $y \not\equiv y'$ *and* $op(y') < op(y)$. From (2) and the induction hypothesis we obtain that $pBPA_{drt} \vdash \mathbf{a} + \mathbf{y}' = \mathbf{y}'$. Then from (1) and (3) it follows that
$pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{a} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \underline{\underline{\mathbf{a}}} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{a} + \mathbf{y}') = \underline{\underline{\mathbf{a}}} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \mathbf{y}$.

Case $\mathbf{x} \equiv \underline{\underline{\boldsymbol{\delta}}} \cdot \mathbf{t}$. $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \underline{\underline{\boldsymbol{\delta}}} \cdot \mathbf{t} + \mathbf{y} = \underline{\underline{\boldsymbol{\delta}}} + \mathbf{y} = \mathbf{y}$;

Case $\mathbf{x} \equiv \underline{\underline{\mathbf{a}}} \cdot \mathbf{t}$, $a \in A$. From the assumption $\underline{\underline{a}} \cdot t + y \leftrightarrow y$ and since $\breve{\underline{\underline{a}}} \cdot t \xrightarrow{a} t$ we obtain that $\breve{y} \xrightarrow{a} s$ and $t \leftrightarrow s$. The rest of the proof of this case resembles the fourth case in the proof of Lemma 3.3.59 on page 84.

Case $\mathbf{x} \equiv \boldsymbol{\delta} \cdot \mathbf{t}$. Since $\breve{x} \xrightarrow{\sigma} \breve{\delta} \cdot t$ it follows that $\breve{y} \xrightarrow{\sigma} \breve{y}'$ and $\delta \cdot t + y' \leftrightarrow y'$. From Proposition 5.3.33 *v.* we obtain $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$ and:

- *Subcase* $y \equiv y'$. $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \boldsymbol{\delta} \cdot \mathbf{t} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}) = \underline{\underline{\boldsymbol{\delta}}} \cdot \mathbf{t} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\boldsymbol{\delta} \cdot \mathbf{t} + \mathbf{y}) = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{x} + \mathbf{y})$. Since $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y})$ from Proposition 5.2.15 it follows that $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{y}$;
- *Subcase* $y \not\equiv y'$ *and* $op(y') < op(y)$. From $\delta \cdot t + y' \leftrightarrow y'$ and the induction hypothesis we obtain $pBPA_{drt} \vdash \boldsymbol{\delta} \cdot \mathbf{t} + \mathbf{y}' = \mathbf{y}'$. Finally, $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \boldsymbol{\delta} \cdot \mathbf{t} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \underline{\underline{\boldsymbol{\delta}}} \cdot \mathbf{t} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\boldsymbol{\delta} \cdot \mathbf{t} + \mathbf{y}') = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \mathbf{y}$;

Case $\mathbf{x} \equiv \mathbf{a} \cdot \mathbf{t}$, $a \in A$. From the assumption $a \cdot t + y \leftrightarrow y$ and since $\breve{a} \cdot t \xrightarrow{a} t$ we obtain $\breve{y} \xrightarrow{a} s$ and $t \leftrightarrow s$. Note that $\mathbf{s}$ is a basic term. In a similar way as in the sixth case using Lemma 5.3.34 we can obtain that $pBPA_{drt} \vdash \mathbf{t} = \mathbf{s}$. (5)
Moreover, from Proposition 5.3.33 *ii.* we obtain that $pBPA_{drt} \vdash \mathbf{y} = \underline{\underline{\mathbf{a}}} \cdot \mathbf{s} + \mathbf{y}$. Now it follows that $pBPA_{drt} \vdash \nu_{rel}(\mathbf{y}) = \underline{\underline{\mathbf{a}}} \cdot \mathbf{s} + \nu_{rel}(\mathbf{y})$. (6)
Since $\breve{a} \cdot t \xrightarrow{\sigma} \breve{a} \cdot t$, it follows that $\breve{y} \xrightarrow{\sigma} \breve{y}'$ and $a \cdot t + y' \leftrightarrow y'$. (7)
From Proposition 5.3.33 *v.* and (7) we obtain $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$ (8)
and

- *Subcase* $y \equiv y'$. From (5) and (8) it follows that
  $pBPA_{drt} \vdash \mathbf{x}+\mathbf{y} = \mathbf{a}\cdot\mathbf{t}+\nu_{rel}(\mathbf{y})+\sigma_{rel}(\mathbf{y}) = \underline{\underline{\mathbf{a}}}\cdot\mathbf{t}+\nu_{rel}(\mathbf{y})+\sigma_{rel}(\mathbf{x}+\mathbf{y}) = \nu_{rel}(\mathbf{y})+\sigma_{rel}(\mathbf{x}+\mathbf{y})$
  from which applying Proposition 5.2.15 and (8) we obtain $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{y}$;
- *Subcase* $y \not\equiv y'$ *and* $op(y') < op(y)$. Since $op(x) + op(y') < op(x) + op(y)$ by applying the induction hypothesis on (7) we obtain $pBPA_{drt} \vdash \mathbf{a} \cdot \mathbf{t} + \mathbf{y}' = \mathbf{y}'$. Then using (5), (6) and (8) we have:
  $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{a} \cdot \mathbf{t} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \underline{\underline{\mathbf{a}}} \cdot \mathbf{t} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{a} \cdot \mathbf{t} + \mathbf{y}') = \underline{\underline{\mathbf{a}}} \cdot \mathbf{s} + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \mathbf{y}$;

Case $\mathbf{x} \equiv \mathbf{x_1} + \mathbf{x_2}$. From the assumption $x_1 + x_2 + y \leftrightarrow y$ using Proposition 5.3.32 we obtain $x_1 + y \leftrightarrow y$ and $x_2 + y \leftrightarrow y$. By the induction hypothesis $pBPA_{drt} \vdash \mathbf{x_1} + \mathbf{y} = \mathbf{y}$ and $pBPA_{drt} \vdash \mathbf{x_2}+\mathbf{y} = \mathbf{y}$. Hence, $pBPA_{drt} \vdash \mathbf{x}+\mathbf{y} = \mathbf{x_1}+\mathbf{x_2}+\mathbf{y} = \mathbf{x_1}+\mathbf{x_2}+\mathbf{y}+\mathbf{y} = (\mathbf{x_1}+\mathbf{y})+(\mathbf{x_2}+\mathbf{y}) = \mathbf{y} + \mathbf{y} = \mathbf{y}$;

Case $\mathbf{x} \equiv \sigma_{rel}(\mathbf{x_1})$. From assumption $\sigma_{rel}(x_1) + y \leftrightarrow y$ and since $\sigma_{rel}(\breve{x}_1) \xrightarrow{\sigma} \breve{x}_1$ it follows that $\breve{y} \xrightarrow{\sigma} \breve{y}'$. Also $x_1 + y' \leftrightarrow y'$. Note that $\mathbf{y}'$ is a basic $\mathcal{B}_+(pBPA_{drt})$ term. Since $op(x_1) < op(x)$ and $op(y') \leq op(y)$ (the latter follows from Proposition 5.3.33 *v.*), $op(x_1)+op(y') < op(x)+op(y)$. Therefore, $pBPA_{drt} \vdash \mathbf{x_1} + \mathbf{y}' = \mathbf{y}'$ from the induction hypothesis. Moreover, from Proposition 5.3.33 *v.* we obtain $pBPA_{drt} \vdash \mathbf{y} = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}')$. Now it follows that $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \sigma_{rel}(\mathbf{x_1}) + \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{x_1} + \mathbf{y}') = \nu_{rel}(\mathbf{y}) + \sigma_{rel}(\mathbf{y}') = \mathbf{y}$. Hence, $pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{y}$.

□

Theorem 5.3.36 (*Completeness theorem for* $pBPA_{drt}$). If $\mathbf{z}$ and $\mathbf{u}$ are closed $pBPA_{drt}$ terms, then $z \leftrightarrow u \Rightarrow pBPA_{drt} \vdash \mathbf{z} = \mathbf{u}$.

Proof. By the Elimination theorem and the Soundness theorem it is sufficient to prove that this result is valid for basic terms.

Let us assume that $\mathbf{z}$ and $\mathbf{u}$ are basic $pBPA_{drt}$ terms and $z \leftrightarrows u$.

Case $\mathbf{z}, \mathbf{u} \in \mathcal{B}_+(pBPA_{drt})$. From the assumption we have: $z+u \leftrightarrows z+z \leftrightarrows z$, $z+u \leftrightarrows u+u \leftrightarrows u$. From Lemma 5.3.35 we obtain $pBPA_{drt} \vdash \mathbf{z}+\mathbf{u} = \mathbf{z}$, $pBPA_{drt} \vdash \mathbf{z}+\mathbf{u} = \mathbf{u}$ and also $pBPA_{drt} \vdash \mathbf{z} = \mathbf{u}$.

Case $\mathbf{z} \in \mathcal{B}(pBPA_{drt}) \setminus \mathcal{B}_+(pBPA_{drt})$ *or* $\mathbf{u} \in \mathcal{B}(pBPA_{drt}) \setminus \mathcal{B}_+(pBPA_{drt})$ From above we have that $\forall \mathbf{x}, \mathbf{y} \in \mathcal{B}_+(pBPA_{drt}) \; : \; x + y \leftrightarrows y \Rightarrow pBPA_{drt} \vdash \mathbf{x} + \mathbf{y} = \mathbf{y}$. Since this holds for all basic $\mathcal{B}_+(pBPA_{drt})$ terms, then it holds for all basic $\mathcal{B}_+(pBPA_{drt})$ terms $\mathbf{x}$ and $\mathbf{y}$ such that $op(\mathbf{x}) + op(\mathbf{y}) < op(\mathbf{z}) + op(\mathbf{u})$. Therefore, from Lemma 5.3.34 and the assumption $z \leftrightarrows u$ it follows that $pBPA_{drt} \vdash \mathbf{z} = \mathbf{u}$.

□

5.4 Extension with merge and communication

The concept of parallel composition will now be brought into the timed probabilistic process algebra $pBPA_{drt}$. The intuition about parallel processes which we discussed in Chapter 4 when we introduced $pACP^+$ remains valid here as well. We recall that , two parallel probabilistic processes can synchronize (communicate) but they can also autonomously perform actions in which case they perform chosen actions independently of each other. As a result of such independent activities, one process can start its activities before or after the other process has resolved its probabilistic choice. Now, in the presence of time, there are more situations for which the activities of parallel composition are restricted. A choice made by one process may restrict the further activities of the parallel composition such that time consistency is obeyed. A similar situation can be found in non-probabilistic time settings. But since we have here probabilistic processes and their probability distributions, restriction of the activities of one process immediately leads to a renormalization of the probability distribution of that process. Thus, we come to a point at which it is necessary to introduce a new operator as a means to restrain certain activities and that eventually enforces the renormalization of the probability distribution of one process.

Again, we focus our attention on an extension of $pBPA_{drt}$ with parallel composition and do not consider an extended version of $pBPA^-_{drt}$. We believe that one will have no difficulties to obtain it by following the tactic we use for $pBPA_{drt}$.

5.4.1 Axiomatization of $pACP^+_{drt}$

Next, we extend $pBPA_{drt}$ with the parallel composition operator and the additional operators introduced in Chapter 4. As one can notice, there is another additional operator $\overline{\sigma}$ which does exactly what we have explained in the introduction: restrain activities and renormalize probabilities. Thus the signature $\Sigma_{pACP^+_{drt}}$ of our new process algebra $pACP^+_{drt}$ contains: the constants and operators of $pBPA_{drt}$, the operators of $pACP^+$ and the new operator $\overline{\sigma}$ called the *renormalization operator*. The set of axioms of $pACP^+_{drt}$ consists of the axioms of $pBPA_{drt}$ (Table 3.1+5.1+5.2+ 5.3), the axioms of $pACP^+$ given in Table 4.2+4.4 without axiom $PrMM4$ and the new axioms given in Table 5.10, 5.11 and 5.12.

It is clear that the axioms $PrDRTMM4 - 7$ (Table 5.12) are timed counterparts of $PrMM4$ from $pACP^+$. They express the idea behind the $\between$ operator as it was a case with $PrMM4$, except that each of them shows how this concept is applied on terms with particular structure. By Proposition

$\underline{\underline{a}} \mid \underline{\underline{b}}$	=	$\underline{\underline{\gamma(a,b)}}$		$DRTCF$
$\underline{\underline{a}} \mid \underline{\underline{b}} \cdot x$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot x$		$DRTCM2$
$\underline{\underline{a}} \cdot x \mid \underline{\underline{b}}$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot x$		$DRTCM3$
$\underline{\underline{a}} \cdot x \mid \underline{\underline{b}} \cdot y$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot (x \parallel y)$		$DRTCM4$
$\sigma_{rel}(x) \mid \nu_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTCM5$
$\nu_{rel}(x) \mid \sigma_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTCM6$
$\sigma_{rel}(x) \mid \sigma_{rel}(y)$	=	$\sigma_{rel}(x \mid y)$		$DRTCM7$
$(x \dot{+}_\pi y) \mid z$	=	$x \mid z \dot{+}_\pi y \mid z$		$PrCM2$
$z \mid (x \dot{+}_\pi y)$	=	$z \mid x \dot{+}_\pi z \mid y$		$PrCM3$
$\underline{\underline{a}} \lfloor\!\lfloor x$	=	$\underline{\underline{a}} \cdot x$		$DRTM2$
$\underline{\underline{a}} \cdot x \lfloor\!\lfloor y$	=	$\underline{\underline{a}} \cdot (x \parallel y)$		$DRTM3$
$(x + y) \lfloor\!\lfloor z$	=	$x \lfloor\!\lfloor z + y \lfloor\!\lfloor z$		$DRTM4$
$(x \dot{+}_\pi y) \lfloor\!\lfloor z$	=	$x \lfloor\!\lfloor z \dot{+}_\pi y \lfloor\!\lfloor z$		$PrCM1$
$\sigma_{rel}(x) \lfloor\!\lfloor \nu_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTM5$
$\sigma_{rel}(x) \lfloor\!\lfloor (\nu_{rel}(y) + \sigma_{rel}(z))$	=	$\sigma_{rel}(x \lfloor\!\lfloor z)$		$DRTM6$
$\partial_H(\underline{\underline{a}})$	=	$\underline{\underline{a}}$	if $a \notin H$	$DRTD1$
$\partial_H(\underline{\underline{a}})$	=	$\underline{\underline{\delta}}$	if $a \in H$	$DRTD2$
$\partial_H(x + y)$	=	$\partial_H(x) + \partial_H(y)$		$D3$
$\partial_H(x \cdot y)$	=	$\partial_H(x) \cdot \partial_H(y)$		$D4$
$\partial_H(\sigma_{rel}(x))$	=	$\sigma_{rel}(\partial_H(x))$		$DRTD5$

Table 5.10: Axioms for $pACP^+_{drt}$ - part 1.

5.2.7 and 5.2.8, axioms $PrMM2-3$ and the Elimination theorem of $pACP^+_{drt}$, which is proved later, it is clear that the forms of terms captured by these axioms (terms that occur on the left-hand sides of the axioms) cover the entire set of closed terms of $pACP^+_{drt}$. As we can notice these axioms do not take care of time consistency since z and w can be arbitrary terms with arbitrary time activities. This is the role given to the $\lfloor\!\lfloor$ operator which is expressed by axioms $DRTM2$, $DRTM3$, $DRTM5$ and $DRTM6$ that also occur in the non-probabilistic discrete time *ACP* together with the new axioms $PrDRTM7$ and $PrDRTM8$. $PrDRTM7$ and $PrDRTM8$ handle the time-step behaviour of the left merge. Actually they express that when the left process of the left merge can only do a time step, then the right process has to restrict its probability distribution over its sub-processes which can do a time step as well. In particular, $PrDRTM7$ says that if one sub-process of the right argument of the left merge which is assigned probability π has to be initiated immediately, that is, it cannot idle, then after the time step it cannot be an outcome of the probabilistic choice of the right process, so it is removed and the probability π is distributed over the possible outcome. The idea of $PrDRTM8$ is similar, but it expresses that only those summands of each sub-process of the right argument have to be removed which cannot idle. If at least one summand can idle, then it remains as a possible outcome with the probability assigned to the original sub-process (before cutting out the "now" parts).

$\overline{\boldsymbol{\sigma}}(\nu_{rel}(x))$	=	$\underline{\underline{\delta}}$	$PrRN1$
$\overline{\boldsymbol{\sigma}}(\nu_{rel}(x) + \sigma_{rel}(y))$	=	y	$PrRN2$
$\overline{\boldsymbol{\sigma}}(\nu_{rel}(x) \leftplus_\pi y)$	=	$\overline{\boldsymbol{\sigma}}(y)$	$PrRN3$
$\overline{\boldsymbol{\sigma}}((\nu_{rel}(x) + \sigma_{rel}(y)) \leftplus_\pi z)$	=	$\overline{\boldsymbol{\sigma}}(\sigma_{rel}(y) \leftplus_\pi z)$	$PrRN4$
$\sigma_{rel}(x) \between (\nu_{rel}(y) \leftplus_\pi z)$	=	$\sigma_{rel}(x) \between z$	$PrDRTM7$
$\sigma_{rel}(x) \between ((\nu_{rel}(y) + \sigma_{rel}(z)) \leftplus_\pi w)$	=	$\sigma_{rel}(x) \between (\sigma_{rel}(z) \leftplus_\pi w)$	$PrDRTM8$

Table 5.11: Additional axioms for $pACP^+_{drt}$.

$x'' = x'' + x'', y'' = y'' + y'' \Rightarrow$ $PrDRTMM4$
$(\nu_{rel}(x') + \sigma_{rel}(x''), z) \between (\nu_{rel}(y') + \sigma_{rel}(y''), w) =$
$(\nu_{rel}(x'), z) \between (\nu_{rel}(y'), w)) + \big(\sigma_{rel}(x'') \between w + \sigma_{rel}(y'') \between z + \sigma_{rel}(x'') \mid \sigma_{rel}(y'')\big)$

$x = x + x, y = y + y \Rightarrow$ $PrDRTMM5$
$(\nu_{rel}(x), z) \between (\nu_{rel}(y), w) = \nu_{rel}(x) \between w + \nu_{rel}(y) \between z + \nu_{rel}(x) \mid \nu_{rel}(y)$

$(\nu_{rel}(x) + \sigma_{rel}(x'), z) \between (\nu_{rel}(y), w) = (\nu_{rel}(x), z) \between (\nu_{rel}(y), w) + \sigma_{rel}(x') \between w$ $PrDRTMM6$

$(\nu_{rel}(x), z) \between (\nu_{rel}(y) + \sigma_{rel}(y'), w) = (\nu_{rel}(x), z) \between (\nu_{rel}(y), w) + \sigma_{rel}(y') \between w$ $PrDRTMM7$

Table 5.12: Additional axioms for $\between$ in $pACP^+_{drt}$.

The renormalization operator $\overline{\boldsymbol{\sigma}}$ does almost the same as the left merge with a left argument that can only do a time step. The difference is that it is a unary operator and when it is applied to a process, the resulting process contains those sub-processes of the original one which can perform a time step. Obviously, this operator is not needed for the axiomatization of parallel composition, but it is needed in the next section where the operational semantics of $pACP^+_{drt}$ will be defined. We have it here in the signature just to make $pACP^+_{drt}$ a complete axiomatization with respect to the operational semantics defined later.

Definition 5.4.1. The set of basic terms of $pACP^+_{drt}$ is defined in the same way like the set of the basic terms in $pBPA_{drt}$ (Definition 5.2.3).

Definition 5.4.2. $\mathcal{SP}(pACP^+_{drt})$ denotes the set of all closed terms over the signature $\Sigma_{pACP^+_{drt}}$.

Proposition 5.4.3. If t_1 and t_2 are basic $\mathcal{B}_+(pBPA_{drt})$ terms, then $pACP^+_{drt} \vdash \overline{\boldsymbol{\sigma}}(t_1 + t_2) = \overline{\boldsymbol{\sigma}}(t_1) + \overline{\boldsymbol{\sigma}}(t_2)$.

Proof. Let us assume that t_1, t_2 are basic $\mathcal{B}_+(pBPA_{drt})$ term. From Proposition 5.2.7 either $pACP^+_{drt} \vdash t_1 = \nu_{rel}(s_1) + \sigma_{rel}(r_1)$ or $pACP^+_{drt} \vdash t_1 = \nu_{rel}(s_1)$ and $pACP^+_{drt} \vdash t_2 = \nu_{rel}(s_2) + \sigma_{rel}(r_2)$ or $pACP^+_{drt} \vdash t_2 = \nu_{rel}(s_2)$ for some basic $\mathcal{B}_+(pBPA_{drt})$ terms s_1, r_1, s_2 and r_2. Hence,
$pACP^+_{drt} \vdash \overline{\boldsymbol{\sigma}}(t_1 + t_2) = \overline{\boldsymbol{\sigma}}(\nu_{rel}(s_1) + \sigma_{rel}(r_1) + \nu_{rel}(s_2) + \sigma_{rel}(r_2)) = r_1 + r_2 = \overline{\boldsymbol{\sigma}}(t_1) + \overline{\boldsymbol{\sigma}}(t_2)$ or
$pACP^+_{drt} \vdash \overline{\boldsymbol{\sigma}}(t_1 + t_2) = \overline{\boldsymbol{\sigma}}(\nu_{rel}(s_1) + \sigma_{rel}(r_1) + \nu_{rel}(s_2)) = r_1 + \underline{\underline{\delta}} = \overline{\boldsymbol{\sigma}}(t_1) + \overline{\boldsymbol{\sigma}}(t_2)$ or

$pACP^+_{drt} \vdash \overline{\sigma}(t_1 + t_2) = \overline{\sigma}(\nu_{rel}(s_1) + \nu_{rel}(s_2) + \sigma_{rel}(r_2)) = \underline{\underline{\delta}} + r_2 = \overline{\sigma}(t_1) + \overline{\sigma}(t_2)$ or
$pACP^+_{drt} \vdash \overline{\sigma}(t_1 + t_2) = \overline{\sigma}(\nu_{rel}(s_1) + \nu_{rel}(s_2)) = r_1 + r_2 = \overline{\sigma}(t_1) + \overline{\sigma}(t_2)$. □

Lemma 5.4.4. Let p and q be basic $pBPA_{drt}$ terms. Then there are closed $pBPA_{drt}$ terms r, s, t, u and v such that $pACP^+_{drt} \vdash p \between q = r$, $pACP^+_{drt} \vdash p \mid q = s$, $pACP^+_{drt} \vdash p \parallel q = t$, $pACP^+_{drt} \vdash \partial_H(p) = u$, $H \subseteq A$ and $pACP^+_{drt} \vdash \overline{\sigma}(p) = v$.

Proof. For the operators that occur in $pACP^+$ see the proof of Lemma 4.2.3. Here we give only the part of the inductive proof which considers the $\overline{\sigma}$ operator. It is based on case distinction of the structure of p in the same way it was done in Lemma 4.2.3.

Case $p \equiv \underline{\underline{a}}$ *or* $p \equiv \underline{\underline{a}} \cdot p_1$, $a \in A_\delta$. $pACP^+_{drt} \vdash \overline{\sigma}(p) = \underline{\underline{\delta}}$ and it is a closed $pBPA_{drt}$ term;

Case $p \equiv a$, $a \in A_\delta$. $pACP^+_{drt} \vdash \overline{\sigma}(p) = a$ which is a closed $pBPA_{drt}$ term;

Case $p \equiv a \cdot p_1$, $a \in A_\delta$. $pACP^+_{drt} \vdash \overline{\sigma}(p) = a \cdot p_1$ and it is closed $pBPA_{drt}$ term;

Case $p \equiv p_1 + p_2$. Since $p_1, p_2 \in \mathcal{B}_+(pBPA_{drt})$ from Proposition 5.4.3 follows that:
$pACP^+_{drt} \vdash \overline{\sigma}(p) = \overline{\sigma}(p_1 + p_2) = \overline{\sigma}(p_1) + \overline{\sigma}(p_2)$. By the induction hypothesis there are closed $pBPA_{drt}$ terms r_1 and r_2 such that $pACP^+_{drt} \vdash \overline{\sigma}(p_1) = r_1$ and $pACP^+_{drt} \vdash \overline{\sigma}(p_2) = r_2$. Finally, $pACP^+_{drt} \vdash \overline{\sigma}(p) = r_1 + r_2$ which is a closed $pBPA_{drt}$ term;

Case $p \equiv \sigma_{rel}(p_1)$. Using the axiom $PrRN2$ we obtain:
$pACP^+_{drt} \vdash \overline{\sigma}(p) = \overline{\sigma}(\nu_{rel}(\underline{\underline{\delta}}) + \sigma_{rel}(p_1)) = p_1$ and by the assumption p_1 is a closed $pBPA_{drt}$ term;

Case $p \equiv p_1 \between_\pi p_2$. Since $p \in \mathcal{B}(pBPA_{drt}) \setminus \mathcal{B}_+(pBPA_{drt})$ using Proposition 5.2.8 we obtain that
$pBPA_{drt} \vdash p = \nu_{rel}(s_1 \between_{\pi_1} s_2 \between_{\pi_2} \ldots s_{n-1} \between_{\pi_{n-1}} s_n) \between_\rho$
$\Big((\nu_{rel}(r_1) + \sigma_{rel}(u_1)) \between_{\alpha_1} (\nu_{rel}(r_2) + \sigma_{rel}(u_2)) \between_{\alpha_2} \ldots$
$\between_{\alpha_{m-2}} (\nu_{rel}(r_{m-1}) + \sigma_{rel}(u_{m-1})) \between_{\alpha_{m-1}} (\nu_{rel}(r_m) + \sigma_{rel}(u_m))\Big)$ for some $n, m \in \mathbb{N}$ and some basic terms $s_i, r_j, u_j \in \mathcal{B}_+(pBPA_{drt})$, $1 \leq i \leq n, 1 \leq j \leq m$. Then,
$pACP^+_{drt} \vdash \overline{\sigma}(p) = \overline{\sigma}\Big((\nu_{rel}(r_1) + \sigma_{rel}(u_1)) \between_{\alpha_1} (\nu_{rel}(r_2) + \sigma_{rel}(u_2)) \between_{\alpha_2} \ldots$
$(\nu_{rel}(r_{m-1}) + \sigma_{rel}(u_{m-1})) \between_{\pi_{m-1}} (\nu_{rel}(r_m) + \sigma_{rel}(u_m))\Big) \overset{PrRN3\times m}{=}$
$\overline{\sigma}\Big(\sigma_{rel}(u_1) \between_{\alpha_1} \sigma_{rel}(u_2) \between_{\alpha_2} \ldots \sigma_{rel}(u_{m-1}) \between_{\alpha_{m-1}} \sigma_{rel}(u_m)\Big) =$
$\overline{\sigma}\Big(\sigma_{rel}(u_1 \between_{\alpha_1} u_2 \between_{\alpha_2} \ldots u_{m-1} \between_{\alpha_{m-1}} u_m)\Big) =$
$u_1 \between_{\alpha_1} u_2 \between_{\alpha_2} \ldots u_{m-1} \between_{\alpha_{m-1}} u_m$ and $u_1 \between_{\alpha_1} u_2 \between_{\alpha_2} \ldots u_{m-1} \between_{\alpha_{m-1}} u_m$ is a closed $pBPA_{drt}$ term.

□

Lemma 5.4.5. If p, q, z and w are basic terms, then there is a closed $pBPA_{drt}$ term r such that $pACP^+_{drt} \vdash (p, z) \between (q, w) = r$.

Proof. See the proof of Lemma 4.2.4. □

Theorem 5.4.6 (*Elimination theorem of* $pACP^+_{drt}$). Let p be a closed $pACP^+_{drt}$ term. Then there is a closed $pBPA_{drt}$ term q such that $pACP^+_{drt} \vdash p = q$.

Proof. The proof of the theorem is based on the results in Proposition 5.4.3, 5.4.4 and 5.4.5 and it resembles the proof of the Elimination theorem of $pACP^+$ (Theorem 4.2.5). □

5.5 Structured operational semantics of $pACP^+_{drt}$

Next we define the operational semantics of $pACP^+_{drt}$ and the bisimulation model $\mathcal{M}_{pACP^+_{drt}}$. There are a few interesting points about the term-deduction system $\mathbf{T}_{pACP^+_{drt}}$ which will be described in more detail later. First, in order to formulate σ-transitions of the merge operator (by means of the left merge), keeping in mind the time restriction that parallel composition or left merge of two processes can do a time step only if both arguments can do so, we need the additional operator $\overline{\boldsymbol{\sigma}}$ and the additional predicate $\boldsymbol{D}$. They have been defined earlier, but here we will justify them. As a consequence, a second interesting issue arises, which is the formulation of the deduction rules for the $\overline{\boldsymbol{\sigma}}$ operator. Finally, as a result of non-trivial deduction rules for the $\overline{\boldsymbol{\sigma}}$ operator and the $\boldsymbol{D}$ predicate we end up with the conclusion that the defined term-deduction system is not stratifiable. We elaborate all these issues after we formally introduce the operational semantics of $pACP^+_{drt}$.

5.5.1 Model of $pACP^+_{drt}$ and properties of the model

The operational semantics of $pACP^+_{drt}$ is defined by the term-deduction system $\mathbf{T}_{pACP^+_{drt}} = (\breve{\Sigma}_{pACP^+_{drt}}, \mathbf{DR}_{pACP^+_{drt}})$ with $\breve{\Sigma}_{pACP^+_{drt}} = (\underline{\underline{A}}_\delta \cup \breve{\underline{\underline{A}}}_\delta \cup A_\delta \cup \breve{A}_\delta, +, \cdot, \leftthreetimes_\pi, \sigma_{rel}, \nu_{rel}, \between, \lfloor\!\lfloor, |, \rangle\!\langle, \partial_H, \overline{\boldsymbol{\sigma}}, \boldsymbol{D})$ and with the deduction rules given in Table(s) 5.5+ 5.6+5.7+5.8 (deduction rules of $pBPA_{drt}$) and the deduction rules given in Tables 5.13 and 5.14 (deduction rules of $pACP^+$) as well as the deduction rules in Tables 5.15 and 5.16. Furthermore, the items 1, 3-5 in Definition 3.3.2 (pg. 49), together with Definition 4.3.1 (pg. 96) and Definition 5.3.1 (pg. 129), when the process algebras used in these definitions are replaced by $pACP^+_{drt}$, and the added item in Definition 5.5.1 define the set of static processes $\mathbb{SP}(pACP^+_{drt})$; the items 1-3 in Definition 3.3.3 (pg. 3.3.3) together with Definition 4.3.2 (pg. 96) and Definition 5.3.2 (pg. 129) (all occurring process algebras are replaced by $pACP^+_{drt}$) define the set of trivial static processes $\mathbb{D}(pACP^+_{drt})$; the items 1-3 in Definition 3.3.4 (pg. 50) together with Definition 4.3.3 (pg. 96) and Definition 5.3.3 (pg. 129) (all occurring process algebras are replaced by $pACP^+_{drt}$) define the set of dynamic processes $\mathbb{DP}(pACP^+_{drt})$; the PDF function μ on $\mathbb{PT}(pACP^+_{drt})$ is defined by Definition 5.5.2 (pg. 154) and the probabilistic bisimulation relation on $\mathbb{PT}(pACP^+_{drt})$ is defined by Definition 5.3.5 (pg. 130) when $pBPA_{drt}$ is replaced by $pACP^+_{drt}$.

Definition 5.5.1.

7.6. if $s \in \mathbb{SP}(pACP^+_{drt})$, then $\overline{\boldsymbol{\sigma}}(s) \in \mathbb{SP}(pACP^+_{drt})$.

$$R16: \frac{x \rightsquigarrow x', y \rightsquigarrow y'}{x \between y \rightsquigarrow x' \lfloor\!\lfloor y + y' \lfloor\!\lfloor x + x' \mid y'} \qquad R17: \frac{x \rightsquigarrow x', y \rightsquigarrow y'}{(x,z) \rangle\!\langle (y,w) \rightsquigarrow x' \lfloor\!\lfloor w + y' \lfloor\!\lfloor z + x' \mid y'}$$

$$R18: \frac{x \rightsquigarrow x'}{x \lfloor\!\lfloor y \rightsquigarrow x' \lfloor\!\lfloor y} \qquad R19: \frac{x \rightsquigarrow x', y \rightsquigarrow y'}{x \mid y \rightsquigarrow x' \mid y'} \qquad R20: \frac{x \rightsquigarrow x'}{\partial_H(x) \rightsquigarrow \partial_H(x')}$$

Table 5.13: Probabilistic transitions of $pACP^+_{drt}$ - part 2.

$$R6: \frac{x \xrightarrow{a} x'}{x \between y \xrightarrow{a} x' \parallel y} \qquad R7: \frac{x \xrightarrow{a} \surd}{x \between y \xrightarrow{a} y}$$

$$R8: \frac{x \xrightarrow{a} x', y \xrightarrow{b} y', \gamma(a,b) = c}{x \mid y \xrightarrow{c} x' \parallel y'} \qquad R9: \frac{x \xrightarrow{a} x', y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \mid y \xrightarrow{c} x', y \mid x \xrightarrow{c} x'}$$

$$R10: \frac{x \xrightarrow{a} \surd, y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \mid y \xrightarrow{c} \surd} \qquad R11: \frac{x \xrightarrow{a} x', a \notin H}{\partial_H(x) \xrightarrow{a} \partial_H(x')} \qquad R12: \frac{x \xrightarrow{a} \surd, a \notin H}{\partial_H(x) \xrightarrow{a} \surd}$$

Table 5.14: Action transitions of $pACP^+_{drt}$ - part 2.

$$R33: \frac{x \rightsquigarrow x', x' \xrightarrow{\sigma} x''}{\overline{\boldsymbol{\sigma}}(x) \rightsquigarrow x''} \qquad R34: \frac{\neg \boldsymbol{D}(x)}{\overline{\boldsymbol{\sigma}}(x) \rightsquigarrow \breve{\underline{\underline{\delta}}}}$$

$$R35: \frac{x \xrightarrow{\sigma} x', \boldsymbol{D}(y)}{x \between y \xrightarrow{\sigma} x' \between \overline{\boldsymbol{\sigma}}(y)} \qquad R36: \frac{x \xrightarrow{\sigma} x', y \xrightarrow{\sigma} y'}{x \mid y \xrightarrow{\sigma} x' \mid y'} \qquad R37: \frac{x \xrightarrow{\sigma} x'}{\partial_H(x) \xrightarrow{\sigma} \partial_H(x')}$$

Table 5.15: Additional rules of $pACP^+_{drt}$.

Definition 5.5.2. (PDF for $pACP^+_{drt}$) A probability distribution function on $\mathbb{PT}(pACP^+_{drt})$ is defined by the equalities in Table 3.6, 3.7, 4.7, 5.9 and 5.17.

As one can notice the crucial rule in which $\overline{\boldsymbol{\sigma}}$ is incorporated is the deduction rule for time transition of the left merge (Table 5.15). Let us consider the following composition: $u \equiv \sigma_{rel}(\breve{\underline{\underline{a}}}) \between \big(\underline{\underline{b}} \leftthreetimes_{1/2} \sigma_{rel}(\underline{\underline{c}} \leftthreetimes_{1/6} \underline{\underline{d}})\big)$. Note that u is a dynamic process. Because the left argument can only do a time step, u is also forced to do a time step. But u can do a time step only if the right argument can do a time step. In other words, we cannot permit u to do a time step and then check the second argument, but we have to block any execution of a σ-transition if the second argument cannot progress time. And that is the reason to have the $\boldsymbol{D}$ premise in rule $R35$. Thus, with the $\boldsymbol{D}$ predicate we "check" if the right argument can do a time step or not. In the setting of non-probabilistic discrete time process algebra the counterpart of this rule is $\dfrac{x \xrightarrow{\sigma} x', y \xrightarrow{\sigma} y'}{x \between y \xrightarrow{\sigma} x' \between y'}$. But since the right argument in the left merge in $\mathbf{T}_{pACP^+_{drt}}$ is a probabilistic process (a static process from $\mathbb{SP}(pACP^+_{drt})$) the premise $y \xrightarrow{\sigma} y'$ can never be proved (due to the deduction rule $R25$ in Table 5.7 on pg. 130). What we actually need as a premise in the left merge rule is: $\exists y' : y \rightsquigarrow y' \;\&\; y' \xrightarrow{\sigma} y''$. Back to Proposition 5.3.15 and its extension in $\mathbf{T}_{pACP^+_{drt}}$ given later in Proposition 5.5.7 we see that predicate $\boldsymbol{D}$ expresses exactly this property. This is one use of the predicate $\boldsymbol{D}$. However, this predicate is essential for the formulation of rule $R34$. The premise $\neg \boldsymbol{D}(x)$ expresses that $\forall x' : \neg(x \rightsquigarrow x')$ *or* $x' \not\xrightarrow{\sigma}$ (see Proposition 5.5.7) in which case we conclude that $\overline{\boldsymbol{\sigma}}(x) \rightsquigarrow \breve{\underline{\underline{\delta}}}$. Clearly, we do not want a universal quantifier in the premises.

Back to our example, we can derive from the deduction rules that $\boldsymbol{D}\big(\underline{\underline{b}} \leftthreetimes_{1/2} \sigma_{rel}(\underline{\underline{c}} \leftthreetimes_{1/6} \underline{\underline{d}})\big)$. Then, u can make a time transition, but the question is: which part of the right argument does not conflict

$$R38: \frac{\boldsymbol{D}(x), \boldsymbol{D}(y)}{\boldsymbol{D}(x \parallel y)} \qquad R39: \frac{\boldsymbol{D}(x), \boldsymbol{D}(y)}{\boldsymbol{D}((x,z) \between (y,w))} \qquad R40: \frac{\boldsymbol{D}(x), \boldsymbol{D}(y)}{\boldsymbol{D}(x \between y)}$$

$$R41: \frac{\boldsymbol{D}(x), \boldsymbol{D}(y)}{\boldsymbol{D}(x \mid y)} \qquad R42: \frac{\boldsymbol{D}(x)}{\boldsymbol{D}(\partial_H(x))} \qquad R43: \frac{x \rightsquigarrow x', x' \xrightarrow{\sigma} x'', \boldsymbol{D}(x'')}{\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(x))}$$

Table 5.16: Deduction rules of $pACP^+_{drt}$ (predicates).

$$\begin{array}{lcll} \mu(\overline{\boldsymbol{\sigma}}(p), \breve{\underline{\delta}}) & = & 1, & \text{if } \neg \boldsymbol{D}(p) \\ \mu(\overline{\boldsymbol{\sigma}}(p), y) & = & \Big(\sum\limits_{\{x \,:\, \mu(p,x)>0 \;\&\; x \xrightarrow{\sigma} y\}} \mu(p,x) \Big) \Big/ \Big(\sum\limits_{\{x \,:\, \mu(p,x)>0 \;\&\; x \xrightarrow{\sigma}\}} \mu(p,x) \Big) & \text{if } \boldsymbol{D}(p) \end{array}$$

Table 5.17: Equalities that defined PDF for $pACP^+_{drt}$ (part 4)

time consistency? In other words, all "now" sub-processes of $\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})$ have to be dropped out after the time tick. This concept is captured by the $\overline{\boldsymbol{\sigma}}$ operator. Rule $R33$ expresses exactly that the $\overline{\boldsymbol{\sigma}}$ operator looks only at those sub-processes of x which "have survived" the last time tick. It prohibits all activities of x that cannot do a time tick. Therefore, for process u we can derive that:

$$\dfrac{\dfrac{\dfrac{\sigma_{rel}(\breve{\underline{a}}) \xrightarrow{\sigma} \breve{\underline{a}}, \boldsymbol{D}\big(\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})\big)}{\sigma_{rel}(\breve{\underline{a}}) \between \big(\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})\big) \xrightarrow{\sigma} \breve{\underline{a}} \between \overline{\boldsymbol{\sigma}}\big(\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})\big)}(R35) \quad \breve{\underline{a}} \xrightarrow{a} \surd}{\breve{\underline{a}} \between \overline{\boldsymbol{\sigma}}\big(\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})\big) \xrightarrow{a} \overline{\boldsymbol{\sigma}}\big(\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})\big)}(R39) \quad \dfrac{\sigma_{rel}(\underline{c} \between_{1/6} \underline{d}) \rightsquigarrow \sigma_{rel}(\breve{\underline{c}}), \sigma_{rel}(\breve{\underline{c}}) \xrightarrow{\sigma} \breve{\underline{c}}}{\overline{\boldsymbol{\sigma}}\big(\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})\big) \rightsquigarrow \breve{\underline{c}}}(R33) \quad \dfrac{\sigma_{rel}(\underline{c} \between_{1/6} \underline{d}) \rightsquigarrow \sigma_{rel}(\breve{\underline{c}}), \sigma_{rel}(\breve{\underline{c}}) \xrightarrow{\sigma} \breve{\underline{d}}}{\overline{\boldsymbol{\sigma}}\big(\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})\big) \rightsquigarrow \breve{\underline{d}}}(R33)$$

...

but we cannot derive that $\overline{\boldsymbol{\sigma}}\big(\underline{b} \between_{1/2} \sigma_{rel}(\underline{c} \between_{1/6} \underline{d})\big) \rightsquigarrow \breve{\underline{b}}$.

Properties of PDF and transitions From this point on we use a slightly different strategy than in the previous sections. The reason is the following: as before we need to prove that μ is well defined on $\mathbb{PT}(pACP^+_{drt})$ and the proof will be inductive on the structure of $\mathbb{SP}(pACP^+_{drt})$ process. But, in that proof, in the step for the $\overline{\boldsymbol{\sigma}}$ operator, due to the definition of μ, we need to formulate a relation between the $\boldsymbol{D}$ predicate and the value of μ (see Proposition 5.5.7). In most of the proofs of properties we give now, we consider only the new operator. The proof given for the relevant property in one of the previous chapters remains valid for the other operators here as well.

Proposition 5.5.3.

i. If u is a $\mathbb{DP}(pACP^+_{drt})$ process and $u \xrightarrow{a} p$ for some $a \in A$, then $p \in \mathbb{SP}(pACP^+_{drt})$.

ii. If u is a $\mathbb{DP}(pACP^+_{drt})$ process and $u \xrightarrow{\sigma} v$, then $v \in \mathbb{DP}(pACP^+_{drt})$.

□

Proposition 5.5.4. If $p \in \mathbb{SP}(pACP^{+}_{drt})$ and $p \rightsquigarrow u$, then $u \in \mathbb{DP}(pACP^{+}_{drt})$.

Proof. The proof is a continuation of the inductive proof of Proposition 4.3.8 and 5.3.9. Let us assume that $p \rightsquigarrow u$ and $p \equiv \overline{\boldsymbol{\sigma}}(q)$ for some process q. Then $q \rightsquigarrow v$ and $v \xrightarrow{\sigma} u$. From the induction hypothesis $v \in \mathbb{DP}(pACP^{+}_{drt})$ and from Proposition 5.5.3*ii.* the conclusion follows. □

Proposition 5.5.5. Let $p \in \mathbb{PT}(pACP^{+}_{drt})$. If $\mu(p, x)$ is defined, then $p \rightsquigarrow x$ implies $\mu(p, x) > 0$.

Proof. The proof of the proposition is given by induction on the structure on p. Since the formulation differs from the similar properties in the previous chapters, we give almost all steps of the inductive proof except the most trivial cases.

Let us assume that $\mu(p, x)$ is defined and $p \rightsquigarrow x$.

Case $p \equiv \underline{\underline{a}}$ *or* $p \equiv a$, $a \in A_\delta$. These cases are trivial;

Case $p \equiv \sigma_{rel}(q)$. Then $q \rightsquigarrow y$ with $x \equiv \sigma_{rel}(y)$. Since $\mu(p, x)$ is defined, $\mu(q, y)$ is defined as well (follows directly from the definition of the PDF). From the induction hypothesis follows that $\mu(q, y) > 0$ from which $\mu(p, x) > 0$;

Case $p \equiv \nu_{rel}(q)$. This case is similar to the previous one;

Case $p \equiv q + r$. Then $q \rightsquigarrow y$ and $r \rightsquigarrow z$ with $x \equiv y + z$. Since $\mu(p, x)$ is defined, $\mu(q, y)$ and $\mu(r, z)$ are defined as well. To conclude, $\mu(q, y) > 0$ and $\mu(r, z) > 0$ from the induction hypothesis which implies $\mu(p, x) > 0$;

Case $p \equiv q \cdot r$. Then $q \rightsquigarrow y$ with $x \equiv y \cdot r$. Since $\mu(p, x)$ is defined, $\mu(q, y)$ is defined as well. The result follows from the induction hypothesis and the definition of the PDF;

Case $p \equiv q \leftplus_\pi r$. $q \rightsquigarrow x$ or $r \rightsquigarrow x$. From the definition of the PDF we have that $\mu(p, x) = \pi \cdot \mu(q, x) + (1 - \pi) \cdot \mu(r, x)$. Therefore, well defined $\mu(p, x)$ implies well defined $\mu(q, x)$ and $\mu(r, x)$. The conclusion follows than easily;

Case $p \equiv q \parallel r$. Then $q \rightsquigarrow y$ and $r \rightsquigarrow z$ with $x \equiv y \between r + z \between q + y \mid z$. Since $\mu(p, x) = \mu(q, y) \cdot \mu(r, z)$ is defined, follows that $\mu(q, y)$ and $\mu(r, z)$ are defined as well. To conclude, $\mu(q, y) > 0$ and $\mu(r, z) > 0$ from the induction hypothesis which implies $\mu(p, x) > 0$;

Case $p \equiv (q, z) \between (r, w)$. This case is similar to the previous one;

Case $p \equiv q \mid r$. This case is similar to the fourth case;

Case $p \equiv q \between r$. This case is similar to the fourth case;

Case $p \equiv \partial_H(q)$. This case is similar to the second case;

Case $p \equiv \overline{\boldsymbol{\sigma}}(q)$. If $\neg \boldsymbol{D}(q)$ then $x \equiv \breve{\underline{\underline{\delta}}}$ and from the definition $\mu(p, \breve{\underline{\underline{\delta}}}) = 1 > 0$. If $\boldsymbol{D}(q)$, then $q \rightsquigarrow y$ and $y \xrightarrow{\sigma} x$ for some y. Furthermore, $\mu(p, x) = \mu(\overline{\boldsymbol{\sigma}}(q), x) = \frac{\sum\limits_{\{u \,:\, \mu(q,u)>0 \;\&\; u \xrightarrow{\sigma} x\}} \mu(q,u)}{\sum\limits_{\{v \,:\, \mu(q,v)>0 \;\&\; v \xrightarrow{\sigma}\}} \mu(q,v)}$.

Since $\mu(p, x)$ is define, $\sum\limits_{\{u \,:\, \mu(q,u)>0 \;\&\; u \xrightarrow{\sigma} x\}} \mu(q, u)$ and $\sum\limits_{\{v \,:\, \mu(q,v)>0 \;\&\; v \xrightarrow{\sigma}\}} \mu(q, v)$ are defined as

well and $\sum_{\{v\,:\,\mu(q,v)>0\ \&\ v\xrightarrow{\sigma}\}} \mu(q,v) \neq 0$. Then, $\mu(q,u)$ is defined for all u such that $u \xrightarrow{\sigma} x$. Therefore, $\mu(q,y)$ is defined as well. From the induction hypothesis now we obtain that $\mu(q,y) > 0$ which implies $\sum_{\{u\,:\,\mu(q,u)>0\ \&\ u\xrightarrow{\sigma}x\}} \mu(q,u) > 0$. Finally,

$$\mu(p,x) = \mu(\overline{\boldsymbol{\sigma}}(q),x) = \frac{\sum_{\{u\,:\,\mu(q,u)>0\ \&\ u\xrightarrow{\sigma}x\}} \mu(q,u)}{\sum_{\{v\,:\,\mu(q,v)>0\ \&\ v\xrightarrow{\sigma}\}} \mu(q,v)} > 0.$$

□

Proposition 5.5.6. Let $u \in \mathbb{DP}(pACP^{+}_{drt})$. $\boldsymbol{D}(u)$ iff $\exists y\ :\ u \xrightarrow{\sigma} y$.

Proof. The proof is a continuation of the inductive proof of Proposition 5.3.14.

Case $u \equiv v \,|\, w$. $\boldsymbol{D}(u)$ iff $\boldsymbol{D}(v)$ and $\boldsymbol{D}(w)$ iff (by the induction hypothesis) there are x, y such that $v \xrightarrow{\sigma} x$ and $w \xrightarrow{\sigma} y$ iff $u \xrightarrow{\sigma} x \,|\, y$;

Case $u \equiv v \between p$. $\boldsymbol{D}(u)$ iff $\boldsymbol{D}(v)$ and $\boldsymbol{D}(p)$ iff (by the induction hypothesis) there are x such that $v \xrightarrow{\sigma} x$ and $\boldsymbol{D}(p)$ iff $v \between p \xrightarrow{\sigma} x \between \overline{\boldsymbol{\sigma}}(p)$;

Case $u \equiv \partial_H(v)$. $\boldsymbol{D}(u)$ iff $\boldsymbol{D}(v)$ iff (by the induction hypothesis) there is x such that $v \xrightarrow{\sigma} x$ iff $u \xrightarrow{\sigma} \partial_H(x)$.

□

Proposition 5.5.7. Let $p \in \mathbb{SP}(pACP^{+}_{drt})$. $\boldsymbol{D}(p)$ iff $\exists x, y\ :\ p \rightsquigarrow x\ \&\ x \xrightarrow{\sigma} y$.

Proof. The proof is a continuation of the inductive proof of Proposition 5.3.15.
Let us assume that $\boldsymbol{D}(p)$. If

Case $p \equiv q \between r$. Then $\boldsymbol{D}(q)$ and $\boldsymbol{D}(r)$. By the induction hypothesis follows that there are u, v such that $q \rightsquigarrow u\ \&\ u \xrightarrow{\sigma} v$. Therefore, $q \between r \rightsquigarrow u \between r$. Since $\boldsymbol{D}(r)$, $u \between r \xrightarrow{\sigma} v \between \overline{\boldsymbol{\sigma}}(r)$;

Case $p \equiv q \,\|\, r$. Then $\boldsymbol{D}(q)$ and $\boldsymbol{D}(r)$. By the induction hypothesis follows that there are u, v such that $q \rightsquigarrow u\ \&\ u \xrightarrow{\sigma} v$ and there are w, z such that $r \rightsquigarrow w\ \&\ w \xrightarrow{\sigma} z$. Therefore, $p \rightsquigarrow u \between r + w \between q + u \,|\, w$. Since $\boldsymbol{D}(r)$ and $\boldsymbol{D}(q)$, $u \between r + w \between q + u \,|\, w \xrightarrow{\sigma} v \between \overline{\boldsymbol{\sigma}}(r) + z \between \overline{\boldsymbol{\sigma}}(q) + v \,|\, z$;

Case $p \equiv (q, z) \between (r, w)$. This case is similar to the previous case;

Case $p \equiv \overline{\boldsymbol{\sigma}}(q)$. From the assumption $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(q))$ follows that $q \rightsquigarrow u\ \&\ u \xrightarrow{\sigma} v\ \&\ \boldsymbol{D}(v)$ for some u, v. Then, $\overline{\boldsymbol{\sigma}}(q) \rightsquigarrow v$. From Proposition 5.5.6 since $\boldsymbol{D}(v)$ and $v \in \mathbb{DP}(pACP^{+}_{drt})$ follows that $v \xrightarrow{\sigma} w$ for some w;

Case $p \equiv \partial_H(q)$. Then $\boldsymbol{D}(q)$. From the induction hypothesis follows that there are u, v such that $q \rightsquigarrow u\ \&\ u \xrightarrow{\sigma} v$. Therefore, $\partial_H(q) \rightsquigarrow \partial_H(u)$ and $\partial_H(u) \xrightarrow{\sigma} \partial_H(v)$.

Let us assume that there are x, y such that $p \rightsquigarrow x$ and $x \xrightarrow{\sigma} y$.

Case $p \equiv q \between r$. The assumption implies that $q \rightsquigarrow u$ and $x \equiv u$, so $u \between r \xrightarrow{\sigma} y$. Therefore, $u \xrightarrow{\sigma} v$ and $\boldsymbol{D}(r)$ and $y \equiv v \between \overline{\boldsymbol{\sigma}}(r)$. We have obtained that $q \rightsquigarrow u$ and $u \xrightarrow{\sigma} v$ which implies by the induction hypothesis that $\boldsymbol{D}(q)$. Since $\boldsymbol{D}(r)$, it follows $\boldsymbol{D}(p)$ as well;

Case $p \equiv q \,\|\, r$. The assumption implies that $q \rightsquigarrow u$, $r \rightsquigarrow v$, $x \equiv u \between r + v \between q + u \,|\, v \xrightarrow{\sigma} y$. The following cases can occur:

Subcase $u \between r \xrightarrow{\sigma} y$ *and* $v \between q \not\xrightarrow{\sigma}$ *and* $u \,|\, v \not\xrightarrow{\sigma}$. Then $u \xrightarrow{\sigma} u'$, $\boldsymbol{D}(r)$ and $y \equiv u' \between \overline{\boldsymbol{\sigma}}(r)$. By the induction hypothesis $\boldsymbol{D}(q)$ and thus $\boldsymbol{D}(p)$;

Subcase $v \between q \xrightarrow{\sigma} y$ *and* $u \between r \not\xrightarrow{\sigma}$ *and* $u \,|\, v \not\xrightarrow{\sigma}$. This case is similar to the previous one;

Subcase $u \between r \xrightarrow{\sigma} y'$, $v \between q \xrightarrow{\sigma} y''$ *and* $u \,|\, v \xrightarrow{\sigma} y'''$ *and* $y \equiv y' + y'' + y'''$. Then $\boldsymbol{D}(r)$ and $\boldsymbol{D}(q)$ from which $\boldsymbol{D}(p)$.

Case $p \equiv (q, z) \between (r, w)$. This case is similar to the previous one;

Case $p \equiv \overline{\boldsymbol{\sigma}}(q)$. From $\overline{\boldsymbol{\sigma}}(q) \rightsquigarrow x$ follows that $q \rightsquigarrow u$ and $u \xrightarrow{\sigma} x$. Moreover, from the assumption $x \xrightarrow{\sigma} y$ using Proposition 5.5.6 we conclude that $\boldsymbol{D}(x)$. Hence, $\boldsymbol{D}(p)$;

Case $p \equiv \partial_H(q)$. Then $q \rightsquigarrow u$, $x \equiv \partial_H(u)$, $u \xrightarrow{\sigma} v$ and $y \equiv \partial_H(v)$. From the induction hypothesis follows that $\boldsymbol{D}(q)$ from which $\boldsymbol{D}(p)$.

□

Proposition 5.5.8. Let $u \in \mathbb{DP}(pACP^+_{drt})$ and $u \xrightarrow{\sigma} x$ and $u \xrightarrow{\sigma} y$ then $x \equiv y$.

Proof. Continuation of the proof of Proposition 5.3.18.

Case $u \equiv v \between q$. By the assumption $u \xrightarrow{\sigma} x$ and $u \xrightarrow{\sigma} y$ we have that $v \xrightarrow{\sigma} x'$, $\boldsymbol{D}(q)$ and $v \xrightarrow{\sigma} y'$, $\boldsymbol{D}(q)$ and $x \equiv x' \between \overline{\boldsymbol{\sigma}}(q)$ and $y \equiv y' \between \overline{\boldsymbol{\sigma}}(q)$. By the induction hypothesis we get $x' \equiv y'$ from which the conclusion follows;

Case $u \equiv v \,|\, w$. By the assumption $u \xrightarrow{\sigma} x$ and $u \xrightarrow{\sigma} y$ we have that $v \xrightarrow{\sigma} x'$, $w \xrightarrow{\sigma} x''$ and $v \xrightarrow{\sigma} y'$ and $w \xrightarrow{\sigma} y''$ and $x \equiv x' \,|\, x''$ and $y \equiv y' \,|\, y''$. By the induction hypothesis we get $x' \equiv y'$ and $x'' \equiv y''$ from which the conclusion follows;

Case $u \equiv \partial_H(v)$. It is similar to the second case.

□

Corollary 5.5.9. Let $u \in \mathbb{DP}(pACP^+_{drt})$ and $M \subseteq \mathbb{PT}(pACP^+_{drt})$ and $u \xrightarrow{\sigma} M$. Then there is exactly one $v \in M$ such that $u \xrightarrow{\sigma} v$.

Proposition 5.5.10. The PDF function μ is well defined on $\mathbb{PT}(pACP^+_{drt})$.

Proof. See proofs of Proposition 4.3.5 and 5.3.6. Here we continue the inductive proof, the step for the $\overline{\boldsymbol{\sigma}}$ operator. Let us assume that $p \equiv \overline{\boldsymbol{\sigma}}(q)$ for some $q \in \mathbb{SP}(pACP^+_{drt})$.

If $\neg \boldsymbol{D}(q)$, then $\mu(\overline{\boldsymbol{\sigma}}(q), u) = \begin{cases} 1, & if\ u \equiv \breve{\underline{\delta}} \\ 0, & otherwise \end{cases}$

Let us suppose that $\boldsymbol{D}(q)$. Proposition 5.5.7 implies that $\{x \,:\, q \rightsquigarrow x \,\&\, x \xrightarrow{\sigma}\} \neq \emptyset$. Using Proposition 5.5.5, which is applicable because from the induction hypothesis $\mu(q, x)$ is well defined for any x, we obtain that $\sum_{\{x \,:\, \mu(q,x)>0 \,\&\, x \xrightarrow{\sigma}\}} \mu(q, x) \neq 0$. From $\{x \,:\, \mu(q, x) > 0 \,\&\, x \xrightarrow{\sigma} u\} \subseteq \{x \,:\, \mu(q, x) > 0 \,\&\, x \xrightarrow{\sigma}\}$ follows that $\sum_{\{x \,:\, \mu(q,x)>0 \,\&\, x \xrightarrow{\sigma} u\}} \mu(q, x) \leq \sum_{\{x \,:\, \mu(q,x)>0 \,\&\, x \xrightarrow{\sigma}\}} \mu(q, x)$. Hence, $\mu(\overline{\boldsymbol{\sigma}}(p), u)$ is defined and $\mu(\overline{\boldsymbol{\sigma}}(p), u) \in [0, 1]$. □

Proposition 5.5.11. Let $p \in \mathbb{PT}(pACP^{+}_{drt})$. Then $\mu(p,x) > 0$ implies $p \rightsquigarrow x$.

Proof. We give only the part of the inductive proof which concerns the $\overline{\boldsymbol{\sigma}}$ operator. For the other inductive steps (the other operators) see the proofs of Proposition 4.3.12 and 5.3.20. Note that the other direction follows from Proposition 5.5.5 and 5.5.10.

Let be $\mu(p,x) > 0$ and $p \equiv \overline{\boldsymbol{\sigma}}(q)$ for $q \in \mathbb{SP}(pACP^{+}_{drt})$.

If $\neg \boldsymbol{D}(q)$ then the assumption implies $x \equiv \underline{\underline{\delta}}$ and then $\overline{\boldsymbol{\sigma}}(q) \rightsquigarrow \underline{\underline{\delta}}$ as well.

Let $\boldsymbol{D}(q)$. The assumption $\mu(\overline{\boldsymbol{\sigma}}(q),x) > 0$ implies that $\mu(q,\{z \ : \ \mu(q,z) > 0 \ \& \ z \xrightarrow{\sigma} x\}) > 0$. Hence, $\{z \ : \ \mu(q,z) > 0 \ \& \ z \xrightarrow{\sigma} x\} \neq \emptyset$. Thus, we have obtained that there is z such that $q \rightsquigarrow z$ and $z \xrightarrow{\sigma} x$ from which $\overline{\boldsymbol{\sigma}}(q) \rightsquigarrow x$. □

Proposition 5.5.12. The cPDF μ is well defined on $\mathbb{PT}(pACP^{+}_{drt})$.

Proof. Continuation of the proof of Proposition 4.3.6 and 5.3.7.

Let us assume that $p \equiv \overline{\boldsymbol{\sigma}}(q)$ for some $q \in \mathbb{SP}(pACP^{+}_{drt})$ and $M \subseteq \mathbb{PT}(pACP^{+}_{drt})$.

If $\neg \boldsymbol{D}(q)$, then $\mu(\overline{\boldsymbol{\sigma}}(q),M) = \begin{cases} 1, & if \ \underline{\underline{\delta}} \in M \\ 0, & otherwise \end{cases}$

Let us suppose that $\boldsymbol{D}(q)$. $\mu(\overline{\boldsymbol{\sigma}}(q),M) = \sum\limits_{u \in M} \mu(\overline{\boldsymbol{\sigma}}(q),u) = \sum\limits_{u \in M} \dfrac{\left(\sum\limits_{\{x_u \ : \ \mu(q,x_u) > 0 \ \& \ x_u \xrightarrow{\sigma} u\}} \mu(q,x_u) \right)}{\left(\sum\limits_{\{x \ : \ \mu(q,x) > 0 \ \& \ x \xrightarrow{\sigma}\}} \mu(q,x) \right)}$

$$= \frac{\sum\limits_{u \in M} \sum\limits_{\{x_u \ : \ \mu(q,x_u) > 0 \ \& \ x_u \xrightarrow{\sigma} u\}} \mu(q,x_u)}{\sum\limits_{\{x \ : \ \mu(q,x) > 0 \ \& \ x \xrightarrow{\sigma}\}} \mu(q,x)} = \frac{\sum\limits_{u \in M} \mu\left(q,\{x_u \ : \ \mu(q,x_u) > 0 \ \& \ x_u \xrightarrow{\sigma} u\}\right)}{\mu\left(q,\{x \ : \ \mu(q,x) > 0 \ \& \ x \xrightarrow{\sigma}\}\right)}$$

and by the induction hypothesis we have that these values of μ are well defined. Moreover, Corollary 5.5.9 guarantees that for different elements u and v in M the sets $\{x_u \ : \ \mu(q,x_u) > 0 \ \& \ x_u \xrightarrow{\sigma} u\}$ and $\{x_v \ : \ \mu(q,x_v) > 0 \ \& \ x_v \xrightarrow{\sigma} v\}$ are disjoint (x_u and x_v can reach only a single process by σ-transition). Thus, having that $\bigcup\limits_{u \in M} \{x_u \ : \ \mu(q,x_u) > 0 \ \& \ x_u \xrightarrow{\sigma} u\} \subseteq \{x \ : \ \mu(q,x) > 0 \ \& \ x \xrightarrow{\sigma}\}$ we obtain that $\mu(\overline{\boldsymbol{\sigma}}(q),M) \in [0,1]$. □

Thus, after we proved Proposition 5.5.5, 5.5.7 and 5.5.11 we can conclude that $\{x \ : \ \mu(p,x) > 0 \ \& \ x \xrightarrow{\sigma}\} = \{x \ : \ p \rightsquigarrow x \ \& \ x \xrightarrow{\sigma}\} = \{x \ : \ p \rightsquigarrow x \ \& \ \boldsymbol{D}(x)\}$. Let us denote this set by $\mathcal{RP}_{\pi \cdot \sigma}(p)$ for process p. We can also define a function $\mathsf{rf} \ : \ \mathbb{SP}(pACP^{+}_{drt}) \mapsto [0,1]$ as: $\mathsf{rf}(p) = \mu(p,\mathcal{RP}_{\pi \cdot \sigma}(p))$. Then the PDF may be reformulate as $\mu(\overline{\boldsymbol{\sigma}}(p),y) = \frac{1}{\mathsf{rf}(p)} \cdot \sum\limits_{\{x \ : \ p \rightsquigarrow x \ \& \ x \xrightarrow{\sigma} y\}} \mu(p,x)$. We call $\mathsf{rf}(p)$ *renormalizing factor*.

Proposition 5.5.13. The equalities given in Proposition 4.3.7 and 5.3.8 are valid in $pACP^{+}_{drt}$. □

Proposition 5.5.14. If u is a $\mathbb{D}(pACP^{+}_{drt})$ process, then the only possible probabilistic transition of u is $u \rightsquigarrow \breve{u}$.

Proof. See the proofs of Proposition 3.3.24, 4.3.10 and 5.3.11. □

Proposition 5.5.15. If u is a $\mathbb{D}(pACP^{+}_{drt})$ process, then $\mu(u,\breve{u}) = 1$. □

Proposition 5.5.16. If $p \in \mathbb{SP}(pACP^{+}_{drt})$ then $\mu(p,\mathbb{PT}(pACP^{+}_{drt})) = 1$.

Proof. We continue the inductive proof of Proposition 4.3.13 and 5.3.21. Let assume that $p \equiv \overline{\boldsymbol{\sigma}}(q)$ for $q \in \mathbb{SP}(pACP^+_{drt})$. If $\neg \boldsymbol{D}(q)$, then $\mu(\overline{\boldsymbol{\sigma}}(q), \mathbb{DP}(pACP^+_{drt})) = \mu(\overline{\boldsymbol{\sigma}}(q), \underline{\breve{\delta}}) = 1$.

If $\boldsymbol{D}(q)$, then

$\mu(\overline{\boldsymbol{\sigma}}(q), \mathbb{DP}(pACP^+_{drt})) = \sum_{u \in \mathbb{DP}(pACP^+_{drt})} \frac{1}{\mathsf{rf}(q)} \cdot \mu(q, \{x \,:\, q \rightsquigarrow x \,\&\, x \xrightarrow{\sigma} u\})$

$= \frac{1}{\mathsf{rf}(q)} \cdot \sum_{u \in \mathbb{DP}(pACP^+_{drt})} \mu(q, \{x \,:\, q \rightsquigarrow x \,\&\, x \xrightarrow{\sigma} u\})$

$= \frac{1}{\mathsf{rf}(q)} \cdot \mu(q, \bigcup_{u \in \mathbb{DP}(pACP^+_{drt})} \{x \,:\, q \rightsquigarrow x \,\&\, x \xrightarrow{\sigma} u\}) = \frac{\mathsf{rf}(q)}{\mathsf{rf}(q)} = 1.$ □

Corollary 5.5.17.

1. Let $p \in \mathbb{PT}(pACP^+_{drt})$ and $M \subseteq \mathbb{PT}(pACP^+_{drt})$. Then $\mu(p, M) > 0$ iff $\exists x \in M : p \rightsquigarrow x$;
2. If $p \in \mathbb{SP}(pACP^+_{drt})$ and $u \in \mathbb{D}(pACP^+_{drt})$ and $\mu(p, [\breve{u}]_{\underline{\leftrightarrow}}) = 1$, then $p \underline{\leftrightarrow} u$;
3. Proposition 3.3.32 is valid for $\mathbb{PT}(pACP^+_{drt})$.

□

Proposition 5.5.18. Proposition 3.3.12 and 3.3.13 remain valid for the probabilistic bisimulation on $\mathbb{PT}(pACP^+_{drt})$.

Properties of rf From the definition of the rf function we obtain directly:

Proposition 5.5.19. If $p \in \mathbb{SP}(pACP^+_{drt})$, then $\mathsf{rf}(\nu_{rel}(p)) = 0$. □

Proposition 5.5.20. If $p, q \in \mathbb{SP}(pACP^+_{drt})$, then $\mathsf{rf}(\nu_{rel}(p) + \sigma_{rel}(q)) = 1$. □

Proposition 5.5.21. $\mathsf{rf}(p \leftthreetimes_\pi q) = \pi \cdot \mathsf{rf}(p) + (1 - \pi) \cdot \mathsf{rf}(q)$. □

Proposition 5.5.22. Let $p, q \in \mathbb{SP}(pACP^+_{drt})$ and $p \underline{\leftrightarrow} q$. Then $\mathsf{rf}(p) = \mathsf{rf}(q)$.

Proof. From the assumption $p \underline{\leftrightarrow} q$ it follows that there exists a bisimulation relation R such that $(p, q) \in R$. From the definition of rf we have that $\mathsf{rf}(p) = \mu(p, \mathcal{RP}_{\pi\cdot\sigma}(p))$ and $\mathsf{rf}(q) = \mu(q, \mathcal{RP}_{\pi\cdot\sigma}(q))$.

Let $M \in \mathbb{PT}(pACP^+_{drt})/R$ such that $M \cap \mathcal{RP}_{\pi\cdot\sigma}(p) \neq \emptyset$. Then $\boldsymbol{D}(M)$ and furthermore, since $(p, q) \in R$, $\mathcal{RP}_{\pi\cdot\sigma}(p) \cap M \neq \emptyset$ iff $\mathcal{RP}_{\pi\cdot\sigma}(q) \cap M \neq \emptyset$. (1)

Thus, if $\{M_i : i \in I\}$ is the greatest set of R equivalence classes such that $\mathcal{RP}_{\pi\cdot\sigma}(p) \cap M_i \neq \emptyset$ for every $i \in I$, then $\mathcal{RP}_{\pi\cdot\sigma}(p) = \bigcup_{i \in I}(M_i \cap \mathcal{RP}_{\pi\cdot\sigma}(p))$ and it is clear that $\mu(p, M_i \setminus \mathcal{RP}_{\pi\cdot\sigma}(p)) = 0$.

We obtain:

$$\begin{aligned} \mu(p, \mathcal{RP}_{\pi\cdot\sigma}(p)) &= \mu(p, \bigcup_{i \in I}(M_i \cap \mathcal{RP}_{\pi\cdot\sigma}(p))) = \sum_{i \in I} \mu(p, M_i \cap \mathcal{RP}_{\pi\cdot\sigma}(p)) \\ &= \sum_{i \in I} \mu(p, (M_i \cap \mathcal{RP}_{\pi\cdot\sigma}(p)) \cup (M_i \setminus \mathcal{RP}_{\pi\cdot\sigma}(p))) = \sum_{i \in I} \mu(p, M_i). \end{aligned}$$

Due to (1) we obtain $\mu(q, \mathcal{RP}_{\pi\cdot\sigma}(q)) = \sum_{i \in I} \mu(q, M_i)$ as well, for the same index set I. Having $\mu(p, M_i) = \mu(q, M_i)$ for each $i \in I$ (because $(p, q) \in R$ and M_i is an R equivalence class), we obtain $\mu(p, \mathcal{RP}_{\pi\cdot\sigma}(p)) = \mu(q, \mathcal{RP}_{\pi\cdot\sigma}(q))$ and also $\mathsf{rf}(p) = \mathsf{rf}(q)$. □

Theorem 5.5.23 (*Congruence theorem of $pACP^+_{drt}$ - part 1*). Let be $p, q \in \mathbb{SP}(pACP^+_{drt})$ and $p \underline{\leftrightarrow} q$. Then $\overline{\boldsymbol{\sigma}}(p) \underline{\leftrightarrow} \overline{\boldsymbol{\sigma}}(q)$.

Proof. Let R_1 be a bisimulation relation such that $(p,q) \in R_1$. We define the following relation:

$$R = Eq\Big(R_1 \cup \alpha\Big)$$

where $\alpha = \{(\overline{\boldsymbol{\sigma}}(p), \overline{\boldsymbol{\sigma}}(q)) \ : \ p,q \in \mathbb{SP}(pACP^{+}_{drt}) \ \& \ (p,q) \in R_1\}$. Let us note that:

RO1: $\alpha \subseteq \mathbb{SP}(pACP^{+}_{drt}) \times \mathbb{SP}(pACP^{+}_{drt})$ and $R \setminus R_1 \subseteq \mathbb{SP}(pACP^{+}_{drt}) \times \mathbb{SP}(pACP^{+}_{drt})$ which implies $K \in \mathbb{DP}(pACP^{+}_{drt})/R$ iff $K \in \mathbb{DP}(pACP^{+}_{drt})/R_1$;

RO2: If $K \in \mathbb{DP}(pACP^{+}_{drt})/R_1$, then $\mu(p,K) = \mu(q,K)$, since $(p,q) \in R_1$;

RO3: if $(p,q) \in R_1$, then $\mathsf{rf}(p) = \mathsf{rf}(q)$ from Proposition 5.5.22.

PDF. From the definition of the PDF and Proposition 5.3.18 we obtain:

$$\begin{aligned}\mu(\overline{\boldsymbol{\sigma}}(p), M) &= \sum_{y \in M} \mu(\overline{\boldsymbol{\sigma}}(p), y) = \sum_{y \in M} \tfrac{1}{\mathsf{rf}(p)} \cdot \mu(p, \{x : p \rightsquigarrow x \ \& \ x \xrightarrow{\sigma} y\}) \\ &= \tfrac{1}{\mathsf{rf}(p)} \cdot \mu(p, \bigcup_{y \in M} \{x \ : \ p \rightsquigarrow x \ \& \ x \xrightarrow{\sigma} y\}) \\ &= \tfrac{1}{\mathsf{rf}(p)} \cdot \mu(p, \{x \ : \ p \rightsquigarrow x \ \& \ \exists y \in M : x \xrightarrow{\sigma} y\}).\end{aligned}$$

Let we denote $\mathcal{RP}_{\pi\cdot\sigma}(p,M) = \{x \ : \ p \rightsquigarrow x \ \& \ \exists y \in M : x \xrightarrow{\sigma} y\}$. Since $\mathcal{RP}_{\pi\cdot\sigma}(p,M) \subseteq \mathbb{DP}(pACP^{+}_{drt})$ there is the greatest set of R_1 equivalence classes $\{K_j \ : \ j \in J\}$ such that for each $j \in J$, $\mathcal{RP}_{\pi\cdot\sigma}(p,M) \cap K_j \neq \emptyset$. Then $\mathcal{RP}_{\pi\cdot\sigma}(p,M) = \bigcup_{i \in J} (\mathcal{RP}_{\pi\cdot\sigma}(p,M) \cap K_j)$ and moreover $\mu(p, K_j \setminus \mathcal{RP}_{\pi\cdot\sigma}(p,M)) = 0$ for every $j \in J$. Thus we obtain:

$$\begin{aligned}\mu(p, \mathcal{RP}_{\pi\cdot\sigma}(p,M)) &= \mu(p, \bigcup_{j \in J} (\mathcal{RP}_{\pi\cdot\sigma}(p,M) \cap K_j)) = \sum_{j \in J} \mu(p, \mathcal{RP}_{\pi\cdot\sigma}(p,M) \cap K_j) \\ &= \sum_{j \in J} \big(\mu(p, \mathcal{RP}_{\pi\cdot\sigma}(p,M) \cap K_j) + \mu(p, K_j \setminus \mathcal{RP}_{\pi\cdot\sigma}(p,M))\big) = \sum_{j \in J} \mu(p, K_j).\end{aligned}$$

Now let denote $\mathcal{RP}_{\pi\cdot\sigma}(q,M) = \{z \ : \ q \rightsquigarrow z \ \& \ \exists w \in M : z \xrightarrow{\sigma} w\}$. We investigate the value of $\mu(q,M)$. From assumption $(p,q) \in R$ and **RO2** follows that $\{K_j \ : \ j \in J\}$ is the greatest set of R_1 equivalence classes such that for each $j \in J$, $\mathcal{RP}_{\pi\cdot\sigma}(q,M) \cap K_j \neq \emptyset$, too. In a similar way as we did for p we can obtain $\mu(\overline{\boldsymbol{\sigma}}(q), M) = \frac{1}{\mathsf{rf}(q)} \cdot \mu(q, \mathcal{RP}_{\pi\cdot\sigma}(q,M))$ and $\mu(q, \mathcal{RP}_{\pi\cdot\sigma}(q,M)) = \sum_{j \in J} \mu(q, K_j)$. Then from **RO2** and **RO3** we obtain $\mu(\overline{\boldsymbol{\sigma}}(p), M) = \frac{1}{\mathsf{rf}(p)} \cdot \sum_{j \in J} \mu(p, K_j) = \frac{1}{\mathsf{rf}(q)} \cdot \sum_{j \in J} \mu(q, K_j) = \mu(\overline{\boldsymbol{\sigma}}(q), M)$.

***D** predicate.* If $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(p))$, then $p \rightsquigarrow x$, $x \xrightarrow{\sigma} y$ and $\boldsymbol{D}(y)$ for some $x,y \in \mathbb{DP}(pACP^{+}_{drt})$. Since $(p,q) \in R_1$, $q \rightsquigarrow z$ and $(x,z) \in R_1$ and also $z \xrightarrow{\sigma} w$ and $(y,w) \in R_1$. We conclude $\boldsymbol{D}(w)$, which implies $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(q))$ as well.

□

Lemma 5.5.24. Let be R a bisimulation relation. We define the following chain of relations:

$$R_0 = R,$$

$$R_{i+1} = Eq\Big(R_i \cup \{(\overline{\boldsymbol{\sigma}}(p), \overline{\boldsymbol{\sigma}}(q)) : p,q \in \mathbb{SP}(pACP^{+}_{drt}) \ \& \ (p,q) \in R_i\}\Big), \text{for } i \geq 1,$$

and let be $\overline{\boldsymbol{R}} = \bigcup_{i \geq 0} R_i$. Then $\overline{\boldsymbol{R}}$ is a bisimulation relation.

Proof. From Lemma 5.5.23 it follows that for each $i \geq 1$ the relation R_i is a bisimulation relation. Thus we obtain that $\{R_i : i \geq 0\}$ is a chain of bisimulation relations with $\overline{\boldsymbol{R}}$ as the upper bound of this set. Therefore $\overline{\boldsymbol{R}}$ is an equivalence relation. We will prove that $\overline{\boldsymbol{R}}$ is a bisimulation. Let us note that

RCLR1: $R_i \setminus R_0 \subseteq \mathbb{SP}(pACP^+_{drt}) \times \mathbb{SP}(pACP^+_{drt})$ for each $i \geq 1$. Also $\overline{\boldsymbol{R}} \setminus R_0 \subseteq \mathbb{SP}(pACP^+_{drt}) \times \mathbb{SP}(pACP^+_{drt})$ which implies $M \in \mathbb{DP}(pACP^+_{drt})/\overline{\boldsymbol{R}}$ iff $M \in \mathbb{DP}(pACP^+_{drt})/R_i$ iff $M \in \mathbb{DP}(pACP^+_{drt})/R$;

RCLR2: if $M \in \mathbb{DP}(pACP^+_{drt})/\overline{\boldsymbol{R}}$, then $\mu(p, M) = \mu(q, M)$ because $(p, q) \in R_i$ for all $i \geq 1$;

RCLR3: if $(p, q) \in R_i$ then $\mathsf{rf}(p) = \mathsf{rf}(q)$.

The technical part of the proof is similar to the proof of Theorem 5.5.23. □

From now on we will refer to $\overline{\boldsymbol{R}}$ as the $\overline{\boldsymbol{\sigma}}$ closure of R.

Corollary 5.5.25. If $p \in \mathbb{SP}(pACP^+_{drt})$ we denote:

$$\overline{\boldsymbol{\sigma}}^0(p) = p,$$
$$\overline{\boldsymbol{\sigma}}^i(p) = \overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}^{i-1}(p)),\ for\ i \geq 1.$$

If $p, q \in \mathbb{SP}(pACP^+_{drt})$ and $(p, q) \in \overline{\boldsymbol{R}}$, then for each $i \geq 0$, $(\overline{\boldsymbol{\sigma}}^i(p), \overline{\boldsymbol{\sigma}}^i(q)) \in \overline{\boldsymbol{R}}$.

Theorem 5.5.26 (*Congruence theorem of $pACP^+_{drt}$ - part 2*). $\leftrightarrow$ is a congruence relation on $\mathbb{PT}(pACP^+_{drt})$ with respect to the operators of $pACP^+_{drt}$.

Proof. We give the part of the proof which concerns the new operators added to $pBPA_{drt}$ to obtain $pACP^+_{drt}$. Also, the result that $\overline{\boldsymbol{\sigma}}$ preserves $\leftrightarrow$ is given in Theorem 5.5.24.

Parallel composition. Let x, y, z and w be $\mathbb{PT}(pACP^+_{drt})$ processes such that $x \leftrightarrow y$ and $z \leftrightarrow w$. So, there exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. We define a relation R_{m} in the following way:

$R_{\mathsf{m}} = Eq(\alpha_{\mathsf{m}} \cup \beta_{\mathsf{m}} \cup \gamma_{\mathsf{m}} \cup \overline{\boldsymbol{R_1}} \cup \overline{\boldsymbol{R_2}})$,

where

$\alpha_{\mathsf{m}} = \{(p \parallel q, s \parallel t)\ :\ p, q, s, t \in \mathbb{SP}(pACP^+_{drt}), (p, s) \in \overline{\boldsymbol{R_1}}, (q, t) \in \overline{\boldsymbol{R_2}}\}$,

$\beta_{\mathsf{m}} = \{(u \between q + v \between p + u \mid v, l \between t + k \between s + l \mid k),\ :\ p, q, s, t \in \mathbb{SP}(pACP^+_{drt}),\ u, v, l, k \in \mathbb{DP}(pACP^+_{drt}),$
$(u, l) \in R_1,\ (v, k) \in R_2, (p, s) \in \overline{\boldsymbol{R_1}},\ (q, t) \in \overline{\boldsymbol{R_2}}\}$,

$\gamma_{\mathsf{m}} = \{(u \between q + u \mid v, l \between t + l \mid k),\ (v \between p + u \mid v, k \between s + l \mid k),\ (u \between q, l \between t),\ (v \between p, k \between s),\ (u \mid v, l \mid k)\ :$
$p, q, s, t \in \mathbb{SP}(pACP^+_{drt}),\ u, v, l, k \in \mathbb{DP}(pACP^+_{drt}),$
$(u, l) \in R_1,\ (v, k) \in R_2, (p, s) \in \overline{\boldsymbol{R_1}},\ (q, t) \in \overline{\boldsymbol{R_2}}\}$.

We investigate only the σ-transitions, the $\boldsymbol{D}$ predicate and the value of the PDF function μ for related processes. Let us note that:

DRTM1: α_{m}, β_{m} and γ_{m} are equivalence relations; α_{m}, $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_2}}$ contain pairs of static processes relevant to R_{m}; β_{m}, γ_{m}, $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_2}}$ contain pairs of dynamic processes relevant to R_{m};

DRTM2: if $(p \parallel q, s \parallel t) \in \alpha_{\mathsf{m}}$ and $K \in \mathbb{DP}(pACP^+_{drt})/\beta_{\mathsf{m}}$, then $p \parallel q \rightsquigarrow K$ iff $s \parallel t \rightsquigarrow K$;

DRTM3: if $p \parallel q \rightsquigarrow K$ for $K \in \mathbb{DP}(pACP^+_{drt})/R_{\mathsf{m}}$, then $K = [u \between q + v \between p + u \mid v]_{\beta_{\mathsf{m}}}$ for some u, v such that $p \rightsquigarrow u$ and $q \rightsquigarrow v$. Moreover, from the definition of β_{m} we have that $K = [u]_{R_1}\ {}^{[p]_{\overline{\boldsymbol{R_1}}}} \parallel {}^{[q]_{\overline{\boldsymbol{R_2}}}}[v]_{R_2}$;

DRTM4: since $\overline{\boldsymbol{R_1}}$, $\overline{\boldsymbol{R_2}}$ and β_{m} are all subsets of R_{m} and they are equivalence relations themselves, if $M \in \mathbb{DP}(pACP^{+}_{drt})/R_{\mathsf{m}}$, then $M = \bigcup_{i_1 \in I_1} M^1_{i_1}$, $M = \bigcup_{i_2 \in I_2} M^2_{i_2}$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I_1, I_2 and J and for some equivalence classes $M^1_{i_1},\ i_1 \in I_1$, $M^2_{i_2},\ i_2 \in I_2$ and $K_j,\ j \in J$ of $\overline{\boldsymbol{R_1}}$, $\overline{\boldsymbol{R_2}}$ and β_{m}, respectively.

PDF. Suppose that $(r, r_1) \in R_{\mathsf{m}}$ for some $r, r_1 \in \mathbb{SP}(pACP^{+}_{drt})$ and $M \in \mathbb{DP}(pACP^{+}_{drt})/R_{\mathsf{m}}$. Then

1. If $(r, r_1) \in \overline{\boldsymbol{R_k}}, k = 1, 2$, then the result can be proved easily by use of **DRTM4** and Proposition 3.3.9 *ii.* (see the proof of Theorem 3.3.36 pg. 63);
2. If $(r, r_1) \in \alpha$, then $r \equiv p \,\|\, q$ and $r_1 \equiv s \,\|\, t$ for some $p, q, s, t \in \mathbb{SP}(pACP^{+}_{drt})$ such that $(p, s) \in \overline{\boldsymbol{R_1}}$ and $(q, t) \in \overline{\boldsymbol{R_2}}$. According to **DRTM3** and **DRTM4**, $K_j = [u_j]_{R_1}{}^{[p]_{\overline{\boldsymbol{R_1}}}} \,\|\, {}^{[q]_{\overline{\boldsymbol{R_2}}}}[v_j]_{R_2}$, $p \rightsquigarrow u_j$ and $q \rightsquigarrow v_j$. Then from Proposition 5.5.13 (4.3.7 *ii.*) follows that
$$\mu(p \,\|\, q, K_j) = \mu(p \,\|\, q, [u_j]_{R_1}{}^{[p]_{\overline{\boldsymbol{R_1}}}} \,\|\, {}^{[q]_{\overline{\boldsymbol{R_2}}}}[v_j]_{R_2}) = \mu(p, [u_j]_{R_1}) \cdot \mu(q, [v_j]_{R_2})$$
$$= \mu(s, [u_j]_{R_1}) \cdot \mu(t, [v_j]_{R_2}) = \mu(s \,\|\, t, [u_j]_{R_1}{}^{[p]_{\overline{\boldsymbol{R_1}}}} \,\|\, {}^{[q]_{\overline{\boldsymbol{R_2}}}}[v_j]_{R_2}) = \mu(s \,\|\, t, K_j)$$
and using Proposition 3.3.9 *ii.* we can easily prove that $\mu(p \,\|\, q, M) = \mu(s \,\|\, t, M)$.

Let us assume that $(u \between q + v \between p + u \,|\, v, l \between t + k \between s + l \,|\, k) \in \beta_{\mathsf{m}} \subseteq R_{\mathsf{m}}$ for some $u, v, l, k \in \mathbb{DP}(pACP^{+}_{drt})$ and $p, q, s, t \in \mathbb{SP}(pACP^{+}_{drt})$ such that $(u, l) \in R_1,\ (v, k) \in R_2, (p, s) \in \overline{\boldsymbol{R_1}}$ and $(q, t) \in \overline{\boldsymbol{R_2}}$.

σ-transitions. Let us assume that $u \between q + v \between p + u \,|\, v \xrightarrow{\sigma} x$. The following cases are possible:

Case $u \between q \xrightarrow{\sigma} x_1$, $v \between p \not\xrightarrow{\sigma}$ *and* $v \,|\, u \not\xrightarrow{\sigma}$. $u \xrightarrow{\sigma} x'$, $\boldsymbol{D}(q)$, $x_1 \equiv x \equiv x' \between \overline{\boldsymbol{\sigma}}(q)$ and $v \not\xrightarrow{\sigma}$. Therefore, $l \xrightarrow{\sigma} y'$, $(x', y') \in R_1$, $\boldsymbol{D}(t)$, $k \not\xrightarrow{\sigma}$, $l \between t + k \between s + l \,|\, k \xrightarrow{\sigma} y' \between \overline{\boldsymbol{\sigma}}(t)$ and $(x' \between \overline{\boldsymbol{\sigma}}(q), y' \between \overline{\boldsymbol{\sigma}}(t)) \in R_{\mathsf{m}}$ since $(\overline{\boldsymbol{\sigma}}(q), \overline{\boldsymbol{\sigma}}(t)) \in \overline{\boldsymbol{R_2}}$;

Case $u \between q \not\xrightarrow{\sigma}$, $v \between p \xrightarrow{\sigma} x_2$ *and* $v \,|\, u \not\xrightarrow{\sigma}$. This case is similar to the previous one;

Case $u \between q \not\xrightarrow{\sigma}$, $v \between p \not\xrightarrow{\sigma}$ *and* $v \,|\, u \xrightarrow{\sigma} x_3$. $u \xrightarrow{\sigma} x'$, $v \xrightarrow{\sigma} x''$, $\neg\boldsymbol{D}(q)$, $\neg\boldsymbol{D}(p)$ and $x_3 \equiv x \equiv x' \,|\, x''$. Hence, $l \xrightarrow{\sigma} y'$, $(x', y') \in R_1$, $k \xrightarrow{\sigma} y''$, $(x'', y'') \in R_2$, $\neg\boldsymbol{D}(t)$, $\neg\boldsymbol{D}(s)$. Thus, $l \between t + k \between s + l \,|\, k \xrightarrow{\sigma} y' \,|\, y''$ and $(x' \,|\, x'', y' \,|\, y'') \in R_{\mathsf{m}}$;

Case $u \between q \xrightarrow{\sigma} x_1$, $v \between p \not\xrightarrow{\sigma}$ *and* $v \,|\, u \xrightarrow{\sigma} x_3$. Then, $u \xrightarrow{\sigma} x'$, $\boldsymbol{D}(q)$, $v \xrightarrow{\sigma} x''$, $\neg\boldsymbol{D}(p)$ and $x \equiv x_1 + x_3 \equiv x' \between \overline{\boldsymbol{\sigma}}(q) + x' \,|\, x''$. Therefore, $l \xrightarrow{\sigma} y'$, $(x', y') \in R_1$, $\boldsymbol{D}(t)$, $k \xrightarrow{\sigma} y''$, $(x'', y'') \in R_2$, $\neg\boldsymbol{D}(s)$ and $l \between t + k \between s + l \,|\, k \xrightarrow{\sigma} y' \between \overline{\boldsymbol{\sigma}}(t) + y' \,|\, y''$. Thus, $(x' \between \overline{\boldsymbol{\sigma}}(q) + x' \,|\, x'', y' \between \overline{\boldsymbol{\sigma}}(t) + y' \,|\, y'') \in R_{\mathsf{m}}$ since $(\overline{\boldsymbol{\sigma}}(q), \overline{\boldsymbol{\sigma}}(t)) \in \overline{\boldsymbol{R_2}}$;

Case $u \between q \not\xrightarrow{\sigma}$, $v \between p \xrightarrow{\sigma} x_2$ *and* $v \,|\, u \xrightarrow{\sigma} x_3$. This case is similar to the previous one.

Case $u \between q \xrightarrow{\sigma} x_1$, $v \between p \xrightarrow{\sigma} x_2$ *and* $v \,|\, u \xrightarrow{\sigma} x_3$. Then, $u \xrightarrow{\sigma} x'$, $\boldsymbol{D}(q)$, $v \xrightarrow{\sigma} x''$, $\boldsymbol{D}(p)$, $x \equiv x_1 + x_2 + x_3 \equiv x' \between \overline{\boldsymbol{\sigma}}(q) + x'' \between \overline{\boldsymbol{\sigma}}(p) + x' \,|\, x''$. Therefore, $l \xrightarrow{\sigma} y'$, $(x', y') \in R_1$, $\boldsymbol{D}(t)$, $k \xrightarrow{\sigma} y''$, $(x'', y'') \in R_2$, $\boldsymbol{D}(s)$, $l \between t + k \between s + l \,|\, k \xrightarrow{\sigma} y' \between \overline{\boldsymbol{\sigma}}(t) + y'' \between \overline{\boldsymbol{\sigma}}(s) + y' \,|\, y''$. Thus, $(x' \between \overline{\boldsymbol{\sigma}}(q) + x'' \between \overline{\boldsymbol{\sigma}}(p) + x' \,|\, x'', y' \between \overline{\boldsymbol{\sigma}}(t) + y'' \between \overline{\boldsymbol{\sigma}}(s) + y' \,|\, y'') \in R_{\mathsf{m}}$, since $(\overline{\boldsymbol{\sigma}}(q), \overline{\boldsymbol{\sigma}}(t)) \in \overline{\boldsymbol{R_2}}$ and $(\overline{\boldsymbol{\sigma}}(p), \overline{\boldsymbol{\sigma}}(s)) \in \overline{\boldsymbol{R_1}}$.

Let us assume that $(u \between q + u \,|\, v, l \between t + l \,|\, k) \in \gamma_{\mathsf{m}} \subseteq R_{\mathsf{m}}$ for some $u, v, l, k \in \mathbb{DP}(pACP^{+}_{drt})$ and $p, q, s, t \in \mathbb{SP}(pACP^{+}_{drt})$ such that $(u, l) \in R_1,\ (v, k) \in R_2, (p, s) \in \overline{\boldsymbol{R_1}}$ and $(q, t) \in \overline{\boldsymbol{R_2}}$. And let assume that $u \between q + u \,|\, v \xrightarrow{\sigma} x$. The following cases are possible:

Case $u \between q \not\xrightarrow{\sigma}$ *and* $v \mid u \xrightarrow{\sigma} x_3$. Then, $u \xrightarrow{\sigma} x'$, $v \xrightarrow{\sigma} x''$, $\neg \boldsymbol{D}(q)$ and $x_3 \equiv x \equiv x' \mid x''$. Hence, $l \xrightarrow{\sigma} y'$, $(x', y') \in R_1$, $k \xrightarrow{\sigma} y''$, $(x'', y'') \in R_2$, $\neg \boldsymbol{D}(t)$. Thus, $l \between t + l \mid k \xrightarrow{\sigma} y' \mid y''$ and $(x' \mid x'', y' \mid y'') \in R_{\mathsf{m}}$;

Case $u \between q \xrightarrow{\sigma} x_1$ *and* $v \mid u \xrightarrow{\sigma} x_3$. Then, $u \xrightarrow{\sigma} x'$, $\boldsymbol{D}(q)$, $v \xrightarrow{\sigma} x''$ and $x \equiv x_1 + x_3 \equiv x' \between \overline{\boldsymbol{\sigma}}(q) + x' \mid x''$. Therefore, $l \xrightarrow{\sigma} y'$, $(x', y') \in R_1$, $\boldsymbol{D}(t)$, $k \xrightarrow{\sigma} y''$, $(x'', y'') \in R_2$ and $l \between t + l \mid k \xrightarrow{\sigma} y' \between \overline{\boldsymbol{\sigma}}(t) + y' \mid y''$. Moreover, $(x' \between \overline{\boldsymbol{\sigma}}(q) + x' \mid x'', y' \between \overline{\boldsymbol{\sigma}}(t) + y' \mid y'') \in R_{\mathsf{m}}$.

Let us assume that $(v \between p + u \mid v, k \between s + l \mid k) \in \gamma_{\mathsf{m}} \subseteq R_{\mathsf{m}}$ for some $u, v, l, k \in \mathbb{DP}(pACP^+_{drt})$ and $p, q, s, t \in \mathbb{SP}(pACP^+_{drt})$ such that $(u, l) \in R_1$, $(v, k) \in R_2$, $(p, s) \in \overline{\boldsymbol{R_1}}$ and $(q, t) \in \overline{\boldsymbol{R_2}}$. This case is similar to the previous one.

For the cases of pairs: $(u \between q, l \between t) \in \gamma_{\mathsf{m}} \subseteq R_{\mathsf{m}}$ or $(v \between p, k \between s) \in \gamma_{\mathsf{m}} \subseteq R_{\mathsf{m}}$ or $(u \mid v, l \mid k) \in \gamma_{\mathsf{m}} \subseteq R_{\mathsf{m}}$ for $(u, l) \in R_1$, $(v, k) \in R_2$, $(p, s) \in \overline{\boldsymbol{R_1}}$ and $(q, t) \in \overline{\boldsymbol{R_2}}$ see the later proofs for the $\between$ and $\mid$ operators.

D *predicate.* From the deduction rules we obtain: $\boldsymbol{D}(p \parallel s)$ iff ($\boldsymbol{D}(p)$ and $\boldsymbol{D}(s)$) iff ($\boldsymbol{D}(q)$ and $\boldsymbol{D}(t)$) iff $\boldsymbol{D}(q \parallel t)$. And also, $\boldsymbol{D}(u \between q + v \between p + u \mid v)$ iff ($\boldsymbol{D}(u)$ and $\boldsymbol{D}(q)$) or ($\boldsymbol{D}(v)$ and $\boldsymbol{D}(p)$) or ($\boldsymbol{D}(u)$ and $\boldsymbol{D}(v)$) iff ($\boldsymbol{D}(l)$ and $\boldsymbol{D}(t)$) or ($\boldsymbol{D}(k)$ and $\boldsymbol{D}(s)$) or ($\boldsymbol{D}(l)$ and $\boldsymbol{D}(k)$) iff $\boldsymbol{D}(l \between t + k \between s + l \mid k)$.

In a similar way we can show that the $\boldsymbol{D}$ predicate preserves the γ_{m} relation.

Merge with memory. Let $x_1, x_2, x_3, x_4, y_1, y_2, y_3$ and y_4 be $\mathbb{PT}(pACP^+_{drt})$ processes such that $x_i \leftrightarrows y_i$, $i = 1, 2, 3, 4$. So, there exist probabilistic bisimulations R_1, R_2, R_3 and R_4 such that $(x_i, y_i) \in R_i$, for $i = 1, 2, 3, 4$. We define a relation R_e in the following way:

$R_e = Eq\big(\alpha_e \cup \beta_e \cup \gamma_e \cup \overline{\boldsymbol{R_{14}}} \cup \overline{\boldsymbol{R_{23}}} \cup \overline{\boldsymbol{R_{12}}} \cup \overline{\boldsymbol{R_1}} \cup \overline{\boldsymbol{R_2}} \cup \overline{\boldsymbol{R_3}} \cup \overline{\boldsymbol{R_4}}\big)$,

where

$\alpha_e = \{((p_1, z_1) \between (q_1, w_1), (p_2, z_2) \between (q_2, w_2)) \ : \ p_1, q_1, z_1, w_1, p_2, q_2, z_2, w_2 \in \mathbb{SP}(pACP^+_{drt}),$
$(p_1, p_2) \in \overline{\boldsymbol{R_1}}, (q_1, q_2) \in \overline{\boldsymbol{R_2}}, \ (z_1, z_2) \in \overline{\boldsymbol{R_3}}, \ (w_1, w_2) \in \overline{\boldsymbol{R_4}}\}$,

$\beta_e = \{(u_1 \between w_1 + v_1 \between z_1 + u_1 \mid v_1, u_2 \between w_2 + v_2 \between z_2 + u_2 \mid v_2), \ : \ z_1, w_1, z_2, w_2 \in \mathbb{SP}(pACP^+_{drt}),$
$u_1, v_1, u_2, v_2 \in \mathbb{DP}(pACP^+_{drt}), \ (u_1, u_2) \in R_1,$
$(v_1, v_2) \in R_2, (z_1, z_2) \in \overline{\boldsymbol{R_3}}, \ (w_1, w_2) \in \overline{\boldsymbol{R_4}}\}$,

$\gamma_e = \{(u_1 \between w_1 + u_1 \mid v_1, u_2 \between w_2 + u_2 \mid v_2), \ (v_1 \between z_1 + u_1 \mid v_1, v_2 \between z_2 + u_2 \mid v_2), \ (u_1 \between w_1, u_2 \between w_2),$
$(v_1 \between z_1, v_2 \between z_2), \ (u_1 \mid v_1, u_2 \mid v_2) \ :$
$z_1, w_1, z_2, w_2 \in \mathbb{SP}(pACP^+_{drt}), \ u_1, v_1, u_2, v_2 \in \mathbb{DP}(pACP^+_{drt}),$
$(u_1, u_2) \in R_1, \ (v_1, v_2) \in R_2, (z_1, z_2) \in \overline{\boldsymbol{R_3}}, \ (w_1, w_2) \in \overline{\boldsymbol{R_4}}\}$,

and $\overline{\boldsymbol{R_{14}}}$, $\overline{\boldsymbol{R_{23}}}$ and $\overline{\boldsymbol{R_{12}}}$ are defined in the same way like R_{m} if the relation $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_2}}$ are replaced by: $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_4}}$ for $\overline{\boldsymbol{R_{14}}}$, $\overline{\boldsymbol{R_2}}$ and $\overline{\boldsymbol{R_3}}$ for $\overline{\boldsymbol{R_{23}}}$ and $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_2}}$ for $\overline{\boldsymbol{R_{12}}}$.

The proof that R_e is a bisimulation is similar to the previous proof for the $\parallel$ operator.

Left merge. Let x, y, z and w be $\mathbb{PT}(pACP^+_{drt})$ processes such that $x \leftrightarrows y$ and $z \leftrightarrows w$. So, there exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup \alpha_{\mathsf{m}} \cup \beta_{\mathsf{m}} \cup \gamma_{\mathsf{m}} \cup \overline{\boldsymbol{R_1}} \cup \overline{\boldsymbol{R_2}})$,

where

$\alpha = \{(p \between q, s \between t) \ : \ p, q, s, t \in \mathbb{SP}(pACP^+_{drt}), (p, s) \in R_1, (q, t) \in \overline{\boldsymbol{R_2}}\}$,

$\beta = \{(u \between q, v \between t) \ : \ q, t \in \mathbb{SP}(pACP^+_{drt}), \ u, v \in \mathbb{DP}(pACP^+_{drt}), \ (u, v) \in R_1, (q, t) \in \overline{\boldsymbol{R_2}}\}$,

and α_{m}, β_{m} and γ_{m} are defined as before.

We investigate only the σ-transitions, the $\boldsymbol{D}$ predicate and the value of the PDF function μ for related processes. Let us note that:

DRTL1: α and β are equivalence relations; α, α_{m}, $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_2}}$ contain pairs of static processes relevant to R; β, β_{m}, γ_{m}, $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_2}}$ contain pairs of dynamic processes relevant to R;

DRTL2: if $(p \between q, s \between t) \in \alpha$ and $K \in \mathbb{DP}(pACP^+_{drt})/\beta$, then $p \between q \rightsquigarrow K$ iff $s \between t \rightsquigarrow K$;

DRTL3: if $p \between q \rightsquigarrow K$ for $K \in \mathbb{DP}(pACP^+_{drt})/R$, then $K = [u \between q]_\beta$ for some u such that $p \rightsquigarrow u$. Moreover, from the definition of β we have that $K = [u]_{R_1} \between [q]_{\overline{\boldsymbol{R_2}}}$;

DRTL4: since $\overline{\boldsymbol{R_1}}$, $\overline{\boldsymbol{R_2}}$, β_{m} and β are all subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(pACP^+_{drt})/R$, then $M = \bigcup_{i_1 \in I_1} M^1_{i_1}$, $M = \bigcup_{i_2 \in I_2} M^2_{i_2}$, $M = \bigcup_{l \in L} N_l$ and $M = \bigcup_{j \in J} K_j$ for some non-empty index sets I_1, I_2, L and J and for some equivalence classes $M^1_{i_1}$, $i_1 \in I_1$, $M^2_{i_2}$, $i_2 \in I_2$, N_l, $l \in L$ and K_j, $j \in J$ of $\overline{\boldsymbol{R_1}}$, $\overline{\boldsymbol{R_2}}$, β and β_{m}, respectively.

PDF. Suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}(pACP^+_{drt})$ and $M \in \mathbb{DP}(pACP^+_{drt})/R$. Then

1. If $(r, r_1) \in \overline{\boldsymbol{R_k}}, k = 1, 2$, then the result can be proved easily by use of **DRTL4** and Proposition 3.3.9 *ii.*;
2. If $(r, r_1) \in \alpha_{\mathsf{m}}$, then the result is proved above in the proof of the $\parallel$ operator;
3. If $(r, r_1) \in \alpha$, then $r \equiv p \between q$ and $r_1 \equiv s \between t$ for some $p, q, s, t \in \mathbb{SP}(pACP^+_{drt})$ such that $(p, s) \in \overline{\boldsymbol{R_1}}$ and $(q, t) \in \overline{\boldsymbol{R_2}}$. According to **DRTL3** and **DRTL4**, $K_j = [u_j]_{R_1} \between [q]_{\overline{\boldsymbol{R_2}}}$ and $p \rightsquigarrow u_j$. Then from Proposition 5.5.13 (4.3.7 *iv.*) follows that
$\mu(p \between q, K_j) = \mu(p \between q, [u_j]_{R_1} \between [q]_{\overline{\boldsymbol{R_2}}}) = \mu(p, [u_j]_{R_1})$
$= \mu(s, [u_j]_{R_1}) = \mu(s \between t, [u_j]_{R_1} \between [q]_{\overline{\boldsymbol{R_2}}}) = \mu(s \between t, K_j)$.
Using Proposition 3.3.9 *ii.* we can easily prove that $\mu(p \between q, M) = \mu(s \between t, M)$.

Suppose that $(u \between q, v \between t) \in \beta \subseteq R$. Then, $(u, v) \in R_1$ and $(q, t) \in R_2$.

σ-transitions. If $u \between q \xrightarrow{\sigma} x$ then $u \xrightarrow{\sigma} x'$, $\boldsymbol{D}(q)$ and $x \equiv x' \between \overline{\boldsymbol{\sigma}}(q)$. Therefore, $v \xrightarrow{\sigma} y'$, $\boldsymbol{D}(t)$ and $(x', y') \in R_1$. Thus, $v \between t \xrightarrow{\sigma} y' \between \overline{\boldsymbol{\sigma}}(t)$ and $(x' \between \overline{\boldsymbol{\sigma}}(q), y' \between \overline{\boldsymbol{\sigma}}(t)) \in \beta \subseteq R$, because $(\overline{\boldsymbol{\sigma}}(q), \overline{\boldsymbol{\sigma}}(t)) \in \overline{\boldsymbol{R_2}}$.

For σ-transitions of the pairs of β_{m} see the proof of the $\parallel$ operator.

$\boldsymbol{D}$ predicate. $\boldsymbol{D}(p \between q)$ iff ($\boldsymbol{D}(p)$ and $\boldsymbol{D}(q)$) iff ($\boldsymbol{D}(s)$ and $\boldsymbol{D}(t)$) iff $\boldsymbol{D}(s \between t)$ for any p, q, s and t such that $(p, s) \in R_1$ and $(q, t) \in \overline{\boldsymbol{R_2}}$.

Communication merge. Let x, y, z and w be $\mathbb{PT}(pACP^+_{drt})$ processes such that $x \leftrightarrow y$ and $z \leftrightarrow w$. So, there exist probabilistic bisimulations R_1 and R_2 such that $(x, y) \in R_1$ and $(z, w) \in R_2$. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup \alpha_{\mathsf{m}} \cup \beta_{\mathsf{m}} \cup \gamma_{\mathsf{m}} \cup \overline{\boldsymbol{R_1}} \cup \overline{\boldsymbol{R_2}})$,

where

$\alpha = \{(p \mid s, q \mid t) \ : \ p, q, s, t \in \mathbb{SP}(pACP^+_{drt}), (p, q) \in R_1, (s, t) \in R_2\}$,

$\beta = \{(u \mid v, l \mid k) \ : \ u, v, l, k \in \mathbb{DP}(pACP^+_{drt}), \ (u, l) \in R_1, (v, k) \in R_2\}$,

and α_{m}, β_{m} and γ_{m} are defined as before.

We investigate only the σ-transitions, the $\boldsymbol{D}$ predicate and the value of the PDF function μ for related processes. Let us note that:

DRTC1: α and β are equivalence relations; α, α_{m}, $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_2}}$ contain pairs of static processes relevant to R; β, β_{m}, γ_{m}, $\overline{\boldsymbol{R_1}}$ and $\overline{\boldsymbol{R_2}}$ contain pairs of dynamic processes relevant to R;

DRTC2: if $(p \,|\, q, s \,|\, t) \in \alpha$ and $K \in \mathbb{DP}(\textit{pACP}^+_{\textit{drt}})/\beta$, then $p \,|\, q \rightsquigarrow K$ iff $s \,|\, t \rightsquigarrow K$;

DRTC3: if $p \,|\, q \rightsquigarrow K$ for $K \in \mathbb{DP}(\textit{pACP}^+_{\textit{drt}})/\beta$, then $K = [u \,|\, v]_\beta$ for some u and v such that $p \rightsquigarrow u$ and $q \rightsquigarrow v$. Moreover, from the definition of β we have that $K = [u]_{R_1} \,|\, [v]_{R_2}$;

DRTC4: since $\overline{\boldsymbol{R_1}}$, $\overline{\boldsymbol{R_2}}$, β_{m} and β are all subsets of R and they are equivalence relations themselves, if $M \in \mathbb{DP}(\textit{pACP}^+_{\textit{drt}})/R$, then $M = \bigcup\limits_{i_1 \in I_1} M^1_{i_1}$, $M = \bigcup\limits_{i_2 \in I_2} M^2_{i_2}$, $M = \bigcup\limits_{l \in L} N_l$ and $M = \bigcup\limits_{j \in J} K_j$ for some non-empty index sets I_1, I_2, L and J and for some equivalence classes $M^1_{i_1},\ i_1 \in I_1$, $M^2_{i_2},\ i_2 \in I_2$, $N_l,\ l \in L$ and $K_j,\ j \in J$ of $\overline{\boldsymbol{R_1}}$, $\overline{\boldsymbol{R_2}}$, β and β_{m}, respectively.

PDF. Suppose that $(r, r_1) \in R$ for some $r, r_1 \in \mathbb{SP}(\textit{pACP}^+_{\textit{drt}})$ and $M \in \mathbb{DP}(\textit{pACP}^+_{\textit{drt}})/R$. Then

1. If $(r, r_1) \in \overline{\boldsymbol{R_k}}, k = 1, 2$, then the result can be proved easily by use of **DRTC4** and Proposition 3.3.9 *ii.*;
2. If $(r, r_1) \in \alpha_{\mathsf{m}}$, then the result is proved above in the proof of the $\parallel$ operator;
3. If $(r, r_1) \in \alpha$, then $r \equiv p \,|\, q$ and $r_1 \equiv s \,|\, t$ for some $p, q, s, t \in \mathbb{SP}(\textit{pACP}^+_{\textit{drt}})$ such that $(p, s) \in \overline{\boldsymbol{R_1}}$ and $(q, t) \in \overline{\boldsymbol{R_2}}$. According to **DRTC3** and **DRTC4**, $K_j = [u_j]_{R_1} \,|\, [v_j]_{R_2}$ and $p \rightsquigarrow u_j$ and $q \rightsquigarrow v_j$. Then from Proposition 5.5.13 (4.3.7*v.*) follows that
$$\begin{aligned}\mu(p \,|\, q, K_j) &= \mu(p \,|\, q, [u_j]_{R_1} \,|\, [v_j]_{R_2}) = \mu(p, [u_j]_{R_1}) \cdot \mu(q, [v_j]_{R_2}) \\ &= \mu(s, [u_j]_{R_1}) \cdot \mu(t, [v_j]_{R_2}) = \mu(s \,|\, t, [u_j]_{R_1} \,|\, [v_j]_{R_2}) = \mu(s \,|\, t, K_j).\end{aligned}$$
Using Proposition 3.3.9 *ii.* we can easily prove that $\mu(p \,|\, q, M) = \mu(s \,|\, t, M)$.

Suppose that $(u \,|\, v, l \,|\, k) \in \beta \subseteq R$. Then, $(u, l) \in R_1$ and $(v, k) \in R_2$.

σ-transitions. If $u \,|\, v \xrightarrow{\sigma} x$ then $u \xrightarrow{\sigma} x'$, $v \xrightarrow{\sigma} x''$ and $x \equiv x' \,|\, x''$. Therefore, $l \xrightarrow{\sigma} y'$, $k \xrightarrow{\sigma} y''$, for some y' and y'' such that $(x', y') \in R_1$ and $(x'', y'') \in R_2$. Thus $l \,|\, k \xrightarrow{\sigma} y' \,|\, y''$ and $(x' \,|\, x'', y' \,|\, y'') \in \beta \subseteq R$.

For the σ-transitions of the pairs of β_{m} see the proof of the $\parallel$ operator.

$\boldsymbol{D}$ predicate. $\boldsymbol{D}(p \,|\, q)$ iff ($\boldsymbol{D}(p)$ and $\boldsymbol{D}(q)$) iff ($\boldsymbol{D}(s)$ and $\boldsymbol{D}(t)$) iff $\boldsymbol{D}(s \,|\, t)$ for any p, q, s and t such that $(p, s) \in R_1$ and $(q, t) \in R_2$.

Encapsulation. Let x and y be $\mathbb{PT}(\textit{pACP}^+_{\textit{drt}})$ processes such that $x \leftrightarrows y$. So, there exists a probabilistic bisimulations R_1 such that $(x, y) \in R_1$. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup R_1)$,

where

$\alpha = \{(\partial_H(p), \partial_H(q)) \ :\ p, q \in \mathbb{SP}(\textit{pACP}^+_{\textit{drt}}), (p, q) \in R_1\}$,

$\beta = \{(\partial_H(u), \partial_H(v)) \ :\ u, v \in \mathbb{DP}(\textit{pACP}^+_{\textit{drt}}),\ (u, v) \in R_1\}$.

We only give the proof about the σ-transitions and the $\boldsymbol{D}$ predicate. The rest of the proof is very similar to the proof of Theorem 4.3.15 (the part for ∂_H operator).

Let us assume that $(\partial_H(u), \partial_H(v)) \in \beta \subseteq R$.

σ-transitions. If $\partial_H(u) \xrightarrow{\sigma} x$, then $u \xrightarrow{\sigma} x'$ and $x \equiv \partial_H(x')$. Therefore, $v \xrightarrow{\sigma} y'$ and $(x', y') \in R_1$ and $\partial_H(v) \xrightarrow{\sigma} \partial_H(y')$ and $(\partial_H(x'), \partial_H(y')) \in \beta \subseteq R$.

***D** predicate.* $\boldsymbol{D}(\partial_H(p))$ iff $\boldsymbol{D}(p)$ iff $\boldsymbol{D}(q)$ iff $\boldsymbol{D}(\partial_H(q))$ for any p and q such that $(p,q) \in R_1$. □

Proposition 5.5.27. Lemma 4.3.16 and 4.3.17 remain valid in $pACP^+_{drt}$. □

Theorem 5.5.28 (*Soundness of* $pACP^+_{drt}$). Let $\mathbf{p}$ and $\mathbf{q}$ be closed $pACP^+_{drt}$ terms. If $pACP^+_{drt} \vdash \mathbf{p} = \mathbf{q}$ then $p \leftrightarrows q$.

Proof. We only treat the axioms which are added to $pBPA_{drt}$. Also some axioms that occur in $pACP^+$ are not investigated here since the soundness of them is proved in Section 4.3 and the part about the $\boldsymbol{D}$ predicate is trivial and the part about σ transition is either trivial or it is very much like the proof of the relevant axiom in [108]. Here we reconsider only those axioms that we find non-trivial, but we give only the part for the $\boldsymbol{D}$ and the σ transitions. Thus we do not give the proof for $DRTCF$, $DRTCM2-7$, $DRTCM5-7$, $PrCM1-3$, $DRTM2-3$, $DRTD1-2,5$ and $D3-4$.

Axiom DRTM4. The relation R is defined the following way (see pg. 108):

$$R = Eq\Big(\{((p+q)\between s, p\between s + q\between s) \,:\, p,q,s \in \mathbb{SP}(pACP^+_{drt})\} \cup \{((u+v)\between s, u\between s + v\between s) \,:\, u,v \in \mathbb{DP}(pACP^+_{drt}), s \in \mathbb{SP}(pACP^+_{drt})\}\Big).$$

Suppose that $((u+v)\between s, u\between s+v\between s) \in R$ for some $u,v \in \mathbb{DP}(pACP^+_{drt})$ and $s \in \mathbb{SP}(pACP^+_{drt})$.

σ-transitions. If $(u+v)\between s \xrightarrow{\sigma} x$, then one of the following situations occurs:

- *Case* $u \xrightarrow{\sigma} y$, $v \not\xrightarrow{\sigma}$, $\boldsymbol{D}(s)$ *and* $x \equiv y\between \overline{\boldsymbol{\sigma}}(s)$. Then $u\between s \xrightarrow{\sigma} y\between \overline{\boldsymbol{\sigma}}(s)$, $v\between s \not\xrightarrow{\sigma}$. Hence, $u\between s + v\between s \xrightarrow{\sigma} y\between \overline{\boldsymbol{\sigma}}(s)$ and $(y\between \overline{\boldsymbol{\sigma}}(s), y\between \overline{\boldsymbol{\sigma}}(s)) \in R$;
- *Case* $u \not\xrightarrow{\sigma}$, $v \xrightarrow{\sigma} y$, $\boldsymbol{D}(s)$ *and* $x \equiv y\between \overline{\boldsymbol{\sigma}}(s)$. This case is similar to the previous one;
- *Case* $u \xrightarrow{\sigma} y_1$, $v \xrightarrow{\sigma} y_2$, $\boldsymbol{D}(s)$ *and* $x \equiv (y_1+y_2)\between \overline{\boldsymbol{\sigma}}(s)$. Then $u\between s \xrightarrow{\sigma} y_1\between \overline{\boldsymbol{\sigma}}(s)$, $v\between s \xrightarrow{\sigma} y_2\between \overline{\boldsymbol{\sigma}}(s)$. So, $u\between s + v\between s \xrightarrow{\sigma} y_1\between \overline{\boldsymbol{\sigma}}(s) + y_2\between \overline{\boldsymbol{\sigma}}(s)$ and $((y_1+y_2)\between \overline{\boldsymbol{\sigma}}(s), y_1\between \overline{\boldsymbol{\sigma}}(s) + y_2\between \overline{\boldsymbol{\sigma}}(s)) \in R$.

If $u\between s + u\between s \xrightarrow{\sigma} x$, then one of the following situations occurs:

- *Case* $u\between s \xrightarrow{\sigma} x$, $v\between s \not\xrightarrow{\sigma}$. Then $\boldsymbol{D}(s)$, $u \xrightarrow{\sigma} y$, $x \equiv y\between \overline{\boldsymbol{\sigma}}(s)$ and $v \not\xrightarrow{\sigma}$. Hence, $(u+v)\between s \xrightarrow{\sigma} y\between \overline{\boldsymbol{\sigma}}(s)$ and $(y\between \overline{\boldsymbol{\sigma}}(s), y\between \overline{\boldsymbol{\sigma}}(s)) \in R$;
- *Case* $u\between s \not\xrightarrow{\sigma}$, $v\between s \xrightarrow{\sigma} x$. This case is similar to the previous one;
- *Case* $u\between s \xrightarrow{\sigma} x_1$, $v\between s \xrightarrow{\sigma} x_2$. Then $\boldsymbol{D}(s)$, $u \xrightarrow{\sigma} y_1$, $v \xrightarrow{\sigma} y_2$ and $x \equiv y_1\between \overline{\boldsymbol{\sigma}}(s) + y_2\between \overline{\boldsymbol{\sigma}}(s)$. Therefore, $(u+v)\between s \xrightarrow{\sigma} (y_1+y_2)\between \overline{\boldsymbol{\sigma}}(s)$ and $((y_1+y_2)\between \overline{\boldsymbol{\sigma}}(s), y_1\between \overline{\boldsymbol{\sigma}}(s) + y_2\between \overline{\boldsymbol{\sigma}}(s)) \in R$.

***D** predicate.* $\boldsymbol{D}((p+q)\between s)$ iff ($\boldsymbol{D}(s)$ and ($\boldsymbol{D}$(p) or $\boldsymbol{D}$(q))) iff $\boldsymbol{D}(p\between s + q\between s)$ for any $p,q,s \in \mathbb{PT}(pACP^+_{drt})$.

Axiom PrCM4. In the proof of soundness of the axiom $PrCM4$ on pg. 112 we needed to prove that $(v_1+v_2) \mid w_1 \leftrightarrows v_1 \mid w_1 + v_2 \mid w_2$ for any $v_1,v_2,w_1,w_2 \in \mathbb{DP}(pACP^+)$ such that $w_1 \leftrightarrows w_2$. There we considered the action transitions of both processes. Here we need to prove that $(v_1+v_2) \mid w_1 \leftrightarrows v_1 \mid w_1 + v_2 \mid w_2$ for any $v_1,v_2,w_1,w_2 \in \mathbb{DP}(pACP^+_{drt})$ such that $w_1 \leftrightarrows w_2$ and we

will investigate only the σ-transitions, since the investigation of action transitions is similar to the one on pg. 112. Also we do not give the proof about the $\boldsymbol{D}$ predicate since it is trivial.

We define the following relation R on $\mathbb{PT}(pACP^+_{drt})$:

$$R = Eq\Big(\{\big((v_1{+}v_2)\,|\,w_1, v_1\,|\,w_1{+}v_2\,|\,w_2\big)\ :\ v_1, v_2, w_1, w_2 \in \mathbb{DP}(pACP^+_{drt})\ \&\ w_1 \leftrightarrows w_2\} \cup R_1\Big),$$

where R_1 is a bisimulation relation such that $R_1 \supseteq \{(u\,|\,z, u\,|\,z') \ :\ u, z, z' \in \mathbb{DP}(pACP^+_{drt})\ \&\ z \leftrightarrows z'$, whose existence is guaranteed by the Congruence theorem of $pACP^+_{drt}$.

σ-transitions. If $(v_1{+}v_2)\,|\,w_1 \xrightarrow{\sigma} x$, then $v_1{+}v_2 \xrightarrow{\sigma} y$ and $w_1 \xrightarrow{\sigma} z$ and $x \equiv y\,|\,z$. Since $w_1 \leftrightarrows w_2$ it follows that $w_2 \xrightarrow{\sigma} z'$ and $z \leftrightarrows z'$ (here we use Proposition 5.5.8). The following cases are possible:

- *Case $v_1 \xrightarrow{\sigma} y$ and $v_2 \not\xrightarrow{\sigma}$.* $v_1\,|\,w_1 \xrightarrow{\sigma} y\,|\,z$, $v_2\,|\,w_2 \not\xrightarrow{\sigma}$. So, $v_1\,|\,w_1 + v_2\,|\,w_2 \xrightarrow{\sigma} y\,|\,z$ and $(y\,|\,z, y\,|\,z) \in R$;
- *Case $v_1 \not\xrightarrow{\sigma}$ and $v_2 \xrightarrow{\sigma} y$.* $v_1\,|\,w_1 \not\xrightarrow{\sigma}$, $v_2\,|\,w_2 \xrightarrow{\sigma} y\,|\,z'$. Thus, $v_1\,|\,w_1 + v_2\,|\,w_2 \xrightarrow{\sigma} y\,|\,z'$ and $(y\,|\,z, y\,|\,z') \in R_1 \subseteq R$;
- *Case $v_1 \xrightarrow{\sigma} y_1$, $v_2 \xrightarrow{\sigma} y_2$ and $y \equiv y_1 + y_2$.* $v_1\,|\,w_1 \xrightarrow{\sigma} y_1\,|\,z$, $v_2\,|\,w_2 \xrightarrow{\sigma} y_2\,|\,z'$. Therefore, $v_1\,|\,w_1 + v_2\,|\,w_2 \xrightarrow{\sigma} y_1\,|\,z + y_2\,|\,z'$ and $\big((y_1 + y_2)\,|\,z, y_1\,|\,z + y_2\,|\,z'\big) \in R$.

If $v_1\,|\,w_1 + v_2\,|\,w_2 \xrightarrow{\sigma} x$, then $v_1\,|\,w_1 \xrightarrow{\sigma} x_1$, $w_1 \xrightarrow{\sigma} z$ and $x \equiv y\,|\,z$. From $w_1 \leftrightarrows w_2$ follows that $w_2 \xrightarrow{\sigma} z'$ and $z \leftrightarrows z'$ (here Proposition 5.5.8 is used). The following cases are possible:

- *Case $v_1\,|\,w_1 \xrightarrow{\sigma} x$ and $v_2\,|\,w_2 \not\xrightarrow{\sigma}$.* $v_1 \xrightarrow{\sigma} y$, $w_1 \xrightarrow{\sigma} z$, $x \equiv y\,|\,z$ and $v_2 \not\xrightarrow{\sigma}$ (since $w_1 \leftrightarrows w_2$). Thus, $(v_1 + v_2)\,|\,w_1 \xrightarrow{\sigma} y\,|\,z$;
- *Case $v_1\,|\,w_1 \not\xrightarrow{\sigma}$ and $v_2\,|\,w_2 \xrightarrow{\sigma} x$.* $v_2 \xrightarrow{\sigma} y$, $w_2 \xrightarrow{\sigma} z$, $x \equiv y\,|\,z$ and $v_1 \not\xrightarrow{\sigma}$. From $w_1 \leftrightarrows w_2$ it follows that $w_1 \xrightarrow{\sigma} z'$ and $z \leftrightarrows z'$. Thus, $(v_1 + v_2)\,|\,w_1 \xrightarrow{\sigma} y\,|\,z'$ and $(y\,|\,z, y\,|\,z') \in R_1 \subseteq R$;
- *Case $v_1\,|\,w_1 \xrightarrow{\sigma} x_1$ and $v_2\,|\,w_2 \xrightarrow{\sigma} x_2$.* $v_1 \xrightarrow{\sigma} y_1$, $w_1 \xrightarrow{\sigma} z$, $v_2 \xrightarrow{\sigma} y_2$, $w_2 \xrightarrow{\sigma} z'$, $x \equiv y_1\,|\,z + y_2\,|\,z'$ and $z \leftrightarrows z'$ Hence, $(v_1 + v_2)\,|\,w_1 \xrightarrow{\sigma} (y_1 + y_2)\,|\,z$ and $((y_1 + y_2)\,|\,z, y_1\,|\,z + y_2\,|\,z') \in R$;

Axiom PrRN1. We define a relation R in the following way:

$$R = Eq\Big(\{(\overline{\boldsymbol{\sigma}}(\nu_{rel}(p)), \underline{\underline{\delta}})\ :\ p \in \mathbb{SP}(pACP^+_{drt})\}\Big).$$

First, let us note that for any $p \in \mathbb{SP}(pACP^+_{drt})$, $\neg\boldsymbol{D}(\nu_{rel}(p))$ holds.

PDF. $\overline{\boldsymbol{\sigma}}(\nu_{rel}(p)) \rightsquigarrow \breve{\underline{\underline{\delta}}}$ and $\mu(\overline{\boldsymbol{\sigma}}(\nu_{rel}(p)), \breve{\underline{\underline{\delta}}}) = 1$. Also, $\underline{\underline{\delta}} \rightsquigarrow \breve{\underline{\underline{\delta}}}$ and $\mu(\underline{\underline{\delta}}, \breve{\underline{\underline{\delta}}}) = 1$.

$\boldsymbol{D}$ predicate. From $\neg\boldsymbol{D}(\nu_{rel}(p))$ it follows that $\neg\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\nu_{rel}(p)))$ and $\neg\boldsymbol{D}(\underline{\underline{\delta}})$.

Axiom PrRN2. We define a relation in the following way:

$$R = Eq\Big(\{(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q) + \sigma_{rel}(r)), r)\ :\ q, r \in \mathbb{SP}(pACP^+_{drt})\}\Big).$$

PDF. Let us note that $\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)+\sigma_{rel}(r)) \rightsquigarrow u$ implies $r \rightsquigarrow u$ which can be easily proved following the deduction rules. Moreover, from Proposition 5.5.20 we have that $\mathsf{rf}(\nu_{rel}(q)+\sigma_{rel}(r))=1$. Thus we have:

$\mu(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)+\sigma_{rel}(r)),u)$
$=\frac{1}{\mathsf{rf}(\nu_{rel}(q)+\sigma_{rel}(r))}\cdot\mu(\nu_{rel}(q)+\sigma_{rel}(r),\{x \,:\, \nu_{rel}(q)+\sigma_{rel}(r)\rightsquigarrow x \,\&\, x\xrightarrow{\sigma}u\})$
$=\mu(\nu_{rel}(q)+\sigma_{rel}(r),\{\nu_{rel}(v)+\sigma_{rel}(w) : \nu_{rel}(q)+\sigma_{rel}(r)\rightsquigarrow\nu_{rel}(v)+\sigma_{rel}(w)\,\&\,\nu_{rel}(v)+\sigma_{rel}(w)\xrightarrow{\sigma}u\})$
$=\mu(\nu_{rel}(q)+\sigma_{rel}(r),\{\nu_{rel}(v)+\sigma_{rel}(u) \,:\, q\rightsquigarrow v\})=\mu(\nu_{rel}(q)+\sigma_{rel}(r),\bigcup_{v:q\rightsquigarrow v}\{\nu_{rel}(v)+\sigma_{rel}(u)\})$
$=\sum_{v:q\rightsquigarrow v}\mu(\nu_{rel}(q)+\sigma_{rel}(r),\nu_{rel}(v)+\sigma_{rel}(u))$
$=\sum_{v:q\rightsquigarrow v}\mu(q,v)\cdot\mu(r,u)=\Big(\sum_{v:q\rightsquigarrow v}\mu(q,v)\Big)\cdot\mu(r,u)=\mu(r,u).$

The result $\mu(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)+\sigma_{rel}(r)),M)=\mu(r,M)$ for every R equivalence class follows from Proposition 3.3.10.

D *predicate.* If $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)+\sigma_{rel}(r)))$, then $\nu_{rel}(q)+\sigma_{rel}(r)\rightsquigarrow x$ and $x\xrightarrow{\sigma}y$ and $\boldsymbol{D}(y)$ for some $x,y\in\mathbb{DP}(pACP^{+}_{drt})$. Therefore, $q\rightsquigarrow v$, $r\rightsquigarrow y$ and $x\equiv\nu_{rel}(v)+\sigma_{rel}(y)$. To conclude, $r\rightsquigarrow y$ and $\boldsymbol{D}(y)$ and using Proposition 5.5.6 we obtain $\boldsymbol{D}(r)$.

Now assume that $\boldsymbol{D}(r)$. From Proposition 5.5.7 we obtain that there exists $u\in\mathbb{DP}(pACP^{+}_{drt})$ such that $r\rightsquigarrow u$ and $\boldsymbol{D}(u)$. Then $\sigma_{rel}(r)\rightsquigarrow\sigma_{rel}(u)$ and $\sigma_{rel}(u)\xrightarrow{\sigma}u$ as well. Having that there is a $v\in\mathbb{DP}(pACP^{+}_{drt})$ such that $q\rightsquigarrow v$ we obtain the following: $\nu_{rel}(q)+\sigma_{rel}(r)\rightsquigarrow\nu_{rel}(v)+\sigma_{rel}(u)$ and $\nu_{rel}(v)+\sigma_{rel}(u)\xrightarrow{\sigma}u$ and $\boldsymbol{D}(u)$. This yields the result $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)+\sigma_{rel}(r)))$.

Axiom PrRN3. We define the following relation:

$$R=Eq\Big(\{(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)\leftplus_\pi r),\overline{\boldsymbol{\sigma}}(r)) \,:\, q,r\in\mathbb{SP}(pACP^{+}_{drt})\}\Big).$$

PDF. Let us note that $\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)\leftplus_\pi r)\rightsquigarrow u$ iff $\overline{\boldsymbol{\sigma}}(r)\rightsquigarrow u$ and $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)\leftplus_\pi r))$ iff $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(r))$. Hence, if $\neg\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)\leftplus_\pi r))$ and $\neg\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(r))$, then $\mu(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)\leftplus_\pi r),\breve{\underline{\delta}})=1$ and $\mu(\overline{\boldsymbol{\sigma}}(r),\breve{\underline{\delta}})=1$. Otherwise, $\mathsf{rf}(\nu_{rel}(q)\leftplus_\pi r)=\pi\cdot\mathsf{rf}(\nu_{rel}(q))+(1-\pi)\cdot\mathsf{rf}(r)=(1-\pi)\mathsf{rf}(r)$. Since
$\{x \,:\, \nu_{rel}(q)\rightsquigarrow x\,\&\,x\xrightarrow{\sigma}u\}=\emptyset$ and also $\mu(\nu_{rel}(q),\{x \,:\, \nu_{rel}(q)\rightsquigarrow x\,\&\,x\xrightarrow{\sigma}u\}=0$ we obtain:

$\mu(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)\leftplus_\pi r,u))=\frac{1}{(1-\pi)\cdot\mathsf{rf}(r)}\cdot\mu(\nu_{rel}(q)\leftplus_\pi r,\{x \,:\, \nu_{rel}(q)\leftplus_\pi r\rightsquigarrow x\,\&\,x\xrightarrow{\sigma}u\})$
$=\frac{1}{(1-\pi)\cdot\mathsf{rf}(r)}\cdot\big(\pi\cdot\mu(\nu_{rel}(q),\{x:\nu_{rel}(q)\rightsquigarrow x\,\&\,x\xrightarrow{\sigma}u\})$
$+(1-\pi)\cdot\mu(r,\{x:r\rightsquigarrow x\,\&\,x\xrightarrow{\sigma}u\})\big)$
$=\frac{1}{(1-\pi)\cdot\mathsf{rf}(r)}\cdot(1-\pi)\cdot\mu(r,\{x:r\rightsquigarrow x\,\&\,x\xrightarrow{\sigma}u\})$
$=\frac{1}{\mathsf{rf}(r)}\cdot\mu(r,\{x:r\rightsquigarrow x\,\&\,x\xrightarrow{\sigma}u\})=\mu(\overline{\boldsymbol{\sigma}}(r),u).$

D *predicate.* If $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)\leftplus_\pi r))$, then there are x,y such that $\nu_{rel}(q)\leftplus_\pi r\rightsquigarrow x$ and $x\xrightarrow{\sigma}y$ and $\boldsymbol{D}(y)$. Then, $\nu_{rel}(q)\rightsquigarrow x$ or $r\rightsquigarrow x$. The first case is not possible because $x\xrightarrow{\sigma}$. So, $r\rightsquigarrow x$ and $x\xrightarrow{\sigma}y$ and $\boldsymbol{D}(y)$ which implies $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(r))$.

If $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(r))$ then there are x,y such that $r\rightsquigarrow x$ and $x\xrightarrow{\sigma}y$ and $\boldsymbol{D}(y)$. Then also $\nu_{rel}(q)\leftplus_\pi r\rightsquigarrow x$ and $x\xrightarrow{\sigma}y$ and $\boldsymbol{D}(y)$. This yields $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\nu_{rel}(q)\leftplus_\pi r))$.

Axiom PrRN4. We define the following relation:

$$R = Eq\Big(\{(\overline{\boldsymbol{\sigma}}((\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r), \overline{\boldsymbol{\sigma}}(\sigma_{rel}(q)\leftplus_\pi r)) \ : \ q,r, \in \mathbb{SP}(pACP^+_{drt})\}\Big).$$

PDF. Let us first note that $\overline{\boldsymbol{\sigma}}((\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r) \rightsquigarrow u$ iff $\overline{\boldsymbol{\sigma}}(\sigma_{rel}(q)\leftplus_\pi r) \rightsquigarrow u$. Second, let us consider the sets:
$S_1 = \{x'+x'' \ : \ \nu_{rel}(p)+\sigma_{rel}(q) \rightsquigarrow x'+x'' \ \&\ x'+x'' \xrightarrow{\sigma} u\}$ and
$S_2 = \{x' \ : \ \nu_{rel}(p) \rightsquigarrow x'\} + \{x'' \ : \ \sigma_{rel}(q) \rightsquigarrow x'' \ \&\ x'' \xrightarrow{\sigma} u\}$ [4]. The fact that these sets are equal is obvious since for all $y \in \{x' \ : \ \nu_{rel}(p) \rightsquigarrow x'\}$, $y \not\xrightarrow{\sigma}$. Having that $\mathsf{rf}(\nu_{rel}(p)+\sigma_{rel}(q)) = 1$, for the value of the PDF function we have:
$\mu(\overline{\boldsymbol{\sigma}}((\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r, u)$
$= \frac{1}{\mathsf{rf}((\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r)} \cdot \mu((\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r, \{x \ : \ (\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})$
$= \frac{1}{\pi\cdot\mathsf{rf}(\nu_{rel}(p)+\sigma_{rel}(q))+(1-\pi)\cdot\mathsf{rf}(r)} \cdot \big(\pi \cdot \mu((\nu_{rel}(p)+\sigma_{rel}(q)), \{x \ : \ (\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})$
$+(1-\pi)\cdot\mu(r, \{x \ : \ (\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})\big)$
$= \frac{1}{\pi+(1-\pi)\cdot\mathsf{rf}(r)} \cdot \big(\pi \cdot \mu((\nu_{rel}(p)+\sigma_{rel}(q)), \{x \ : \ \nu_{rel}(p)+\sigma_{rel}(q) \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})$
$+(1-\pi)\cdot\mu(r, \{x \ : \ r \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})\big)$
$= \frac{1}{\pi+(1-\pi)\cdot\mathsf{rf}(r)} \cdot \big(\pi \cdot \mu(\nu_{rel}(p)+\sigma_{rel}(q), S_1) + (1-\pi)\cdot\mu(r, \{x \ : \ r \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})\big)$
$= \frac{1}{\pi+(1-\pi)\cdot\mathsf{rf}(r)} \cdot \big(\pi \cdot \mu\big(\nu_{rel}(p)+\sigma_{rel}(q), S_2\big) + (1-\pi)\cdot\mu(r, \{x \ : \ r \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})\big)$
$= \frac{1}{\pi+(1-\pi)\cdot\mathsf{rf}(r)} \cdot \big(\pi\cdot\mu(\nu_{rel}(p), \{x' \ : \ \nu_{rel}(p) \rightsquigarrow x'\})\cdot\mu(\sigma_{rel}(q), \{x'' \ : \ \sigma_{rel}(q) \rightsquigarrow x'' \ \&\ x'' \xrightarrow{\sigma} u\})$
$+(1-\pi)\cdot\mu(r, \{x \ : \ r \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})\big)$
$= \frac{1}{\pi\cdot\mathsf{rf}(\sigma_{rel}(q))+(1-\pi)\cdot\mathsf{rf}(r)} \cdot \big(\pi \cdot \mu(\sigma_{rel}(q), \{x'' \ : \ \sigma_{rel}(q) \rightsquigarrow x'' \ \&\ x'' \xrightarrow{\sigma} u\})$
$+(1-\pi)\cdot\mu(r, \{x \ : \ r \rightsquigarrow x \ \&\ x \xrightarrow{\sigma} u\})\big)$
(since $\mathsf{rf}(\sigma_{rel}(q) = 1)$
$= \frac{1}{\mathsf{rf}(\sigma_{rel}(q)\leftplus_\pi r)} \cdot \mu(\sigma_{rel}(q)\leftplus_\pi r, \{y \ : \ \sigma_{rel}(q)\leftplus_\pi r \rightsquigarrow y \ \&\ y \xrightarrow{\sigma} u\})$
$= \mu(\overline{\boldsymbol{\sigma}}(\sigma_{rel}(q)\leftplus_\pi r), u)$.
The result follows from Proposition 3.3.10.

$\boldsymbol{D}$ *predicate.* If $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}((\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r))$, then $(\nu_{rel}(p)+\sigma_{rel}(q))\leftplus_\pi r \rightsquigarrow x$ and $x \xrightarrow{\sigma} y$ and $\boldsymbol{D}(y)$ for some $x, y \in \mathbb{DP}(pACP^+_{drt})$. There are two possibilities:

Case $r \rightsquigarrow x$. Then $\sigma_{rel}(q)\leftplus_\pi r \rightsquigarrow x$. Since $x \xrightarrow{\sigma} y$ and $\boldsymbol{D}(y)$ we obtain directly $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\sigma_{rel}(q)\leftplus_\pi r))$;

Case $\nu_{rel}(p)+\sigma_{rel}(q) \rightsquigarrow x$, $\nu_{rel}(p) \rightsquigarrow x'$, $\sigma_{rel}(q) \rightsquigarrow x''$. Then $x \equiv x'+x''$, $x' \not\xrightarrow{\sigma}$ and $x'' \xrightarrow{\sigma} y$. Thus, $\sigma_{rel}(q)\leftplus_\pi r \rightsquigarrow x''$ and $x'' \xrightarrow{\sigma} y$ and $\boldsymbol{D}(y)$ which implies $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\sigma_{rel}(q)\leftplus_\pi r))$.

If $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\sigma_{rel}(q)\leftplus_\pi r))$, then $\sigma_{rel}(q)\leftplus_\pi r \rightsquigarrow x$ and $x \xrightarrow{\sigma} y$ and $\boldsymbol{D}(y)$ for some $x, y \in \mathbb{DP}(pACP^+_{drt})$. There are two possibilities:

[4] '+' over sets is defined in Section 2.3.

Case $r \rightsquigarrow x$. Then $(\nu_{rel}(p) + \sigma_{rel}(q)) \uplus_\pi r \rightsquigarrow x$. Since $x \xrightarrow{\sigma} y$ and $\boldsymbol{D}(y)$ it follows that $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}((\nu_{rel}(p) + \sigma_{rel}(q)) \uplus_\pi r))$;

Case $\sigma_{rel}(q) \rightsquigarrow x$. Then there is a $z \in \mathbb{DP}(pACP^+_{drt})$ such that $\nu_{rel}(p) \rightsquigarrow z$ and $z \not\xrightarrow{\sigma}$. Thus, $\nu_{rel}(p) + \sigma_{rel}(q) \rightsquigarrow z + x$ and $z + x \xrightarrow{\sigma} y$. And also, $(\nu_{rel}(p) + \sigma_{rel}(q)) \uplus_\pi r \rightsquigarrow z + x$, $z + x \xrightarrow{\sigma} y$ and $\boldsymbol{D}(y)$ from which $\boldsymbol{D}(\overline{\boldsymbol{\sigma}}((\nu_{rel}(p) + \sigma_{rel}(q)) \uplus_\pi r))$.

Axiom DRTM5. We define a relation R in the following way:

$$R = Eq\Big(\{(\sigma_{rel}(p) \lfloor\!\lfloor \nu_{rel}(q), \underline{\underline{\delta}}) \ : \ p, q \in \mathbb{SP}(pACP^+_{drt})\} \cup \{(\sigma_{rel}(u) \lfloor\!\lfloor \nu_{rel}(q), \breve{\underline{\underline{\delta}}}) \ : \ u \in \mathbb{DP}(pACP^+_{drt}), q \in \mathbb{SP}(pACP^+_{drt})\}\Big).$$

PDF. Let us note that from the definition of R follows that $\forall x : \ \sigma_{rel}(p) \lfloor\!\lfloor \nu_{rel}(q) \rightsquigarrow x \Rightarrow x \in \left[\breve{\underline{\underline{\delta}}}\right]_R$. Thus,
$\mu(\sigma_{rel}(p) \lfloor\!\lfloor \nu_{rel}(q), \left[\breve{\underline{\underline{\delta}}}\right]_R) = \mu(\sigma_{rel}(p) \lfloor\!\lfloor \nu_{rel}(q), \{x : \ \sigma_{rel}(p) \lfloor\!\lfloor \nu_{rel}(q) \rightsquigarrow x\}) = 1$ and also $\mu(\underline{\underline{\delta}}, \left[\breve{\underline{\underline{\delta}}}\right]_R) = 1$.

***D** predicate.* $\neg\boldsymbol{D}(\nu_{rel}(q))$ implies $\neg\boldsymbol{D}(\sigma_{rel}(p) \lfloor\!\lfloor \nu_{rel}(q))$ and $\neg\boldsymbol{D}(\underline{\underline{\delta}})$ as well.

Axiom DRTM6. We define a relation R in the following way:

$$R = Eq\Big(\{(\sigma_{rel}(p) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r)), \sigma_{rel}(p \lfloor\!\lfloor r)) \ : \ p, q, r \in \mathbb{SP}(pACP^+_{drt})\} \cup \{(\sigma_{rel}(u) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r)), \sigma_{rel}(u \lfloor\!\lfloor r)) \ : \ u \in \mathbb{DP}(pACP^+_{drt}), q, r \in \mathbb{SP}(pACP^+_{drt})\} \cup R_1\Big),$$

where R_1 is a bisimulation relation such that $\{(u \lfloor\!\lfloor \overline{\boldsymbol{\sigma}}(\nu_{rel}(q) + \sigma_{rel}(r)), u \lfloor\!\lfloor r) \ : \ u \in \mathbb{DP}(pACP^+_{drt}), q, r \in \mathbb{SP}(pACP^+_{drt})\} \subseteq R_1$. The existence of R_1 is guaranteed by soundness of $PrRN2$ and the Congruence theorem of $pACP^+_{drt}$. Since R_1 is a bisimulation relation we do not investigate pairs belonging to R_1.

PDF. Suppose that $(\sigma_{rel}(p) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r)), \sigma_{rel}(p \lfloor\!\lfloor r)) \in R$ for some $p, q, r \in \mathbb{SP}(pACP^+_{drt})$ and $M \in \mathbb{DP}(pACP^+_{drt})/R$. The following holds: $p \rightsquigarrow u$ iff $\sigma_{rel}(p) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r)) \rightsquigarrow \sigma_{rel}(u) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r))$ iff $\sigma_{rel}(p \lfloor\!\lfloor r) \rightsquigarrow \sigma_{rel}(u \lfloor\!\lfloor r)$. Moreover, from the definition of R it follows that $\sigma_{rel}(u) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r)) \in M$ iff $\sigma_{rel}(u \lfloor\!\lfloor r) \in M$. For the values of the PDF function we have: $\mu(\sigma_{rel}(p) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r)), \sigma_{rel}(u) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r))) = \mu(\sigma_{rel}(p), \sigma_{rel}(u)) = \mu(p, u) = \mu(\sigma_{rel}(p \lfloor\!\lfloor r), \sigma_{rel}(u \lfloor\!\lfloor r))$. The result follows from Proposition 3.3.10.

σ-transitions. Suppose that $(\sigma_{rel}(u) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r)), \sigma_{rel}(u \lfloor\!\lfloor r)) \in R$ for some $u \in \mathbb{DP}(pACP^+_{drt})$ and $q, r \in \mathbb{SP}(pACP^+_{drt})$. If $\sigma_{rel}(u) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r)) \xrightarrow{\sigma} v$, then $v \equiv u \lfloor\!\lfloor \overline{\boldsymbol{\sigma}}(\nu_{rel}(q) + \sigma_{rel}(r))$. If $\sigma_{rel}(u \lfloor\!\lfloor r) \xrightarrow{\sigma} z$, then $z \equiv u \lfloor\!\lfloor r$. Moreover, $(u \lfloor\!\lfloor \overline{\boldsymbol{\sigma}}(\nu_{rel}(q) + \sigma_{rel}(r)), u \lfloor\!\lfloor r) \in R_1 \subseteq R$.

***D** predicate.* It holds that $\boldsymbol{D}(\sigma_{rel}(p))$ and $\boldsymbol{D}(\nu_{rel}(q) + \sigma_{rel}(r))$. This implies that $\boldsymbol{D}(\sigma_{rel}(p) \lfloor\!\lfloor (\nu_{rel}(q) + \sigma_{rel}(r))$ and also $\boldsymbol{D}(\sigma_{rel}(p \lfloor\!\lfloor r))$ for any $p \in \mathbb{PT}(pACP^+_{drt})$.

Axiom PrDRTM7. We define a relation R in the following way:

$$\begin{aligned} R = Eq\Big(& \{(\sigma_{rel}(p) \between (\nu_{rel}(q) \leftplus_\pi r), \sigma_{rel}(p) \between r) \ : \ p,q,r \in \mathbb{SP}(pACP^+_{drt})\} \\ \cup \ & \{(\sigma_{rel}(u) \between (\nu_{rel}(q) \leftplus_\pi r), \sigma_{rel}(u) \between r) \ : \ u \in \mathbb{DP}(pACP^+_{drt}), q,r \in \mathbb{SP}(pACP^+_{drt})\} \\ \cup \ & R_1\Big), \end{aligned}$$

where R_1 is a bisimulation relation such that $\{(u \between \overline{\boldsymbol{\sigma}}(\nu_{rel}(q) \leftplus_\pi r), u \between \overline{\boldsymbol{\sigma}}(r)) \ : \ u \in \mathbb{DP}(pACP^+_{drt}), q,r \in \mathbb{SP}(pACP^+_{drt})\} \subseteq R_1$. The existence of R_1 is guaranteed by soundness of $PrRN3$ and the Congruence theorem of $pACP^+_{drt}$. Since R_1 as a bisimulation relation we do not investigate pairs belonging in R_1.

PDF. Suppose that $(\sigma_{rel}(p) \between (\nu_{rel}(q) \leftplus_\pi r), \sigma_{rel}(p) \between r) \in R$ for some $p,q,r \in \mathbb{SP}(pACP^+_{drt})$ and $M \in \mathbb{DP}(pACP^+_{drt})/R$. The following holds: $p \rightsquigarrow u$ iff $\sigma_{rel}(p) \between (\nu_{rel}(q) \leftplus_\pi r) \rightsquigarrow \sigma_{rel}(u) \between (\nu_{rel}(q) \leftplus_\pi r)$ iff $\sigma_{rel}(p) \between r \rightsquigarrow \sigma_{rel}(u) \between r$. Moreover, from the definition of R it follows that $\sigma_{rel}(u) \between (\nu_{rel}(q) \leftplus_\pi r) \in M$ iff $\sigma_{rel}(u) \between r \in M$. For the values of the PDF function we have:
$\mu(\sigma_{rel}(p) \between (\nu_{rel}(q) \leftplus_\pi r), \sigma_{rel}(u) \between (\nu_{rel}(q) \leftplus_\pi r)) = \mu(\sigma_{rel}(p), \sigma_{rel}(u)) = \mu(p,u)$
$= \mu(\sigma_{rel}(p) \between r, \sigma_{rel}(u) \between r)$. The result $\mu(\sigma_{rel}(p) \between (\nu_{rel}(q) \leftplus_\pi r), M) = \mu(\sigma_{rel}(p) \between r, M)$ follows from Proposition 3.3.10.

σ-transitions. Suppose that $(\sigma_{rel}(u) \between (\nu_{rel}(q) \leftplus_\pi r), \sigma_{rel}(u) \between r) \in R$ for some $u \in \mathbb{DP}(pACP^+_{drt})$ and $q,r \in \mathbb{SP}(pACP^+_{drt})$. If $\sigma_{rel}(u) \between (\nu_{rel}(q) \leftplus_\pi r) \xrightarrow{\sigma} v$, then $v \equiv u \between \overline{\boldsymbol{\sigma}}(\nu_{rel}(q) \leftplus_\pi r)$. If $\sigma_{rel}(u) \between r \xrightarrow{\sigma} z$, then $z \equiv u \between \overline{\boldsymbol{\sigma}}(r)$. The conclusion follows from the definition of R, that is, $(u \between \overline{\boldsymbol{\sigma}}(\nu_{rel}(q) \leftplus_\pi r), u \between \overline{\boldsymbol{\sigma}}(r)) \in R_1 \subseteq R$.

***D* predicate.** For any $p \in \mathbb{PT}(pACP^+_{drt})$ it holds that $\boldsymbol{D}(\sigma_{rel}(p))$ and $\neg \boldsymbol{D}(\nu_{rel}(q))$. Therefore, $\boldsymbol{D}(\sigma_{rel}(p) \between (\nu_{rel}(q) \leftplus_\pi r))$ iff $\boldsymbol{D}(r)$ iff $\boldsymbol{D}(\sigma_{rel}(p) \between r)$.

Axiom PrDRTM8. We define a relation R in the following way:

$$\begin{aligned} R = Eq\Big(& \{\big(\sigma_{rel}(p) \between (\nu_{rel}(q) + \sigma_{rel}(r)) \leftplus_\pi s), \sigma_{rel}(p) \between (\sigma_{rel}(r) \leftplus_\pi s)\big) : \\ & \qquad p,q,r,s \in \mathbb{SP}(pACP^+_{drt})\} \\ \cup \ & \{\big(\sigma_{rel}(u) \between (\nu_{rel}(q) + \sigma_{rel}(r)) \leftplus_\pi s), \sigma_{rel}(u) \between (\sigma_{rel}(r) \leftplus_\pi s)\big) \ : \ u \in \mathbb{DP}(pACP^+_{drt}), \\ & \qquad q,r,s \in \mathbb{SP}(pACP^+_{drt})\} \\ \cup \ & R_1\Big), \end{aligned}$$

where R_1 is a bisimulation relation such that $\{\big(u \between \overline{\boldsymbol{\sigma}}((\nu_{rel}(q) + \sigma_{rel}(r)) \leftplus_\pi s), u \between \overline{\boldsymbol{\sigma}}(\sigma_{rel}(r) \leftplus_\pi s)\big) \ : \ u \in \mathbb{DP}(pACP^+_{drt}), q,r,s \in \mathbb{SP}(pACP^+_{drt})\} \subseteq R_1$. The existence of R_1 is guaranteed by soundness of $PrRN4$ and the Congruence theorem of $pACP^+_{drt}$. Since R_1 as a bisimulation relation we do not investigate pairs belonging to R_1.

PDF. Suppose that $\big(\sigma_{rel}(p) \between ((\nu_{rel}(q) + \sigma_{rel}(r)) \leftplus_\pi s), \sigma_{rel}(p) \between (\sigma_{rel}(r) \leftplus_\pi s)\big) \in R$ for some $p,q,r,s \in \mathbb{SP}(pACP^+_{drt})$ and $M \in \mathbb{DP}(pACP^+_{drt})/R$. The following holds: $p \rightsquigarrow u$ iff $\sigma_{rel}(p) \between ((\nu_{rel}(q) + \sigma_{rel}(r)) \leftplus_\pi s) \rightsquigarrow \sigma_{rel}(u) \between ((\nu_{rel}(q) + \sigma_{rel}(r)) \leftplus_\pi s)$ iff $\sigma_{rel}(p) \between (\sigma_{rel}(r) \leftplus_\pi s) \rightsquigarrow \sigma_{rel}(u) \between (\sigma_{rel}(r) \leftplus_\pi s)$. Moreover, from the definition of R it follows that $\sigma_{rel}(u) \between ((\nu_{rel}(q) + \sigma_{rel}(r)) \leftplus_\pi s) \in M$ iff $\sigma_{rel}(u) \between (\sigma_{rel}(r) \leftplus_\pi s) \in M$. For the values of the PDF function we have:

$\mu(\sigma_{rel}(p)\between((\nu_{rel}(q)+\sigma_{rel}(r))\leftplus_\pi s),\sigma_{rel}(u)\between((\nu_{rel}(q)+\sigma_{rel}(r))\leftplus_\pi s))=\mu(\sigma_{rel}(p),\sigma_{rel}(u))=\mu(p,u)=\mu\big(\sigma_{rel}(p)\between(\sigma_{rel}(r)\leftplus_\pi s),\sigma_{rel}(u)\between(\sigma_{rel}(r)\leftplus_\pi s)\big)$ and the result follows from Proposition 3.3.10.

σ-transitions. Suppose that $(\sigma_{rel}(u)\between((\nu_{rel}(q)+\sigma_{rel}(r))\leftplus_\pi s),\sigma_{rel}(u)\between(\sigma_{rel}(r)\leftplus_\pi s))\in R$ for some $u\in\mathbb{DP}(pACP^+_{drt})$ and $q,r,s\in\mathbb{SP}(pACP^+_{drt})$. If $\sigma_{rel}(u)\between((\nu_{rel}(q)+\sigma_{rel}(r))\leftplus_\pi s)\xrightarrow{\sigma}v$, then $v\equiv u\between\overline{\boldsymbol{\sigma}}((\nu_{rel}(q)+\sigma_{rel}(r))\leftplus_\pi s)$. If $\sigma_{rel}(u)\between(\sigma_{rel}(r)\leftplus_\pi s)\xrightarrow{\sigma}z$, then $z\equiv u\between\overline{\boldsymbol{\sigma}}(\sigma_{rel}(r)\leftplus_\pi s)$. The conclusion follows from the definition of R, that is, $\big(u\between\overline{\boldsymbol{\sigma}}((\nu_{rel}(q)+\sigma_{rel}(r))\leftplus_\pi s),u\between\overline{\boldsymbol{\sigma}}(\sigma_{rel}(r)\leftplus_\pi s)\big)\in R_1\subseteq R$.

***D* predicate.** For any $p\in\mathbb{PT}(pACP^+_{drt})$ it holds that $\boldsymbol{D}(\sigma_{rel}(p))$ and $\boldsymbol{D}(\nu_{rel}(q)+\sigma_{rel}(r))$ and $\boldsymbol{D}(\sigma_{rel}(r))$. Therefore, $\boldsymbol{D}\big(\sigma_{rel}(p)\between((\nu_{rel}(q)+\sigma_{rel}(r))\leftplus_\pi s)\big)$ and $\boldsymbol{D}(\sigma_{rel}(p)\between(\sigma_{rel}(r)\leftplus_\pi s))$.

Axiom PrDRTMM4. Let $p'',q''\in\mathbb{SP}(pACP^+_{drt})$ such that $p''\leftrightarrows p''+p''$, $q''\leftrightarrows q''+q''$ and $\mathcal{RP}(p'')=\{x:p''\rightsquigarrow x\}$ and $\mathcal{RP}(q'')=\{y:q''\rightsquigarrow y\}$. By Lemma 5.5.27 (4.3.17*ii.*) we have that for every $x_1,x_2\in\mathcal{RP}(p'')$, $x_1\leftrightarrows x_2$ and $\mu(p'',\mathcal{RP}(p''))=1$. And also for every $y_1,y_2\in\mathcal{RP}(q'')$, $y_1\leftrightarrows y_2$ and $\mu(q'',\mathcal{RP}(q''))=1$. We will prove that for arbitrary $p',q',p'',q'',z,w\in\mathbb{SP}(pACP^+_{drt})$,
$((\nu_{rel}(p')+\sigma_{rel}(p''),z)\between(\nu_{rel}(q')+\sigma_{rel}(q''),w)\leftrightarrows$

$$(\nu_{rel}(p),z)\between(\nu_{rel}(q'),w)+\big(\sigma_{rel}(p'')\between w+\sigma_{rel}(q'')\between z+\sigma_{rel}(p'')\mid\sigma_{rel}(q'')\big).$$

Probabilistic transitions. If $((\nu_{rel}(p')+\sigma_{rel}(p''),z)\between(\nu_{rel}(q')+\sigma_{rel}(q''),w)\rightsquigarrow U$, then
$U\equiv((\nu_{rel}(x')+\sigma_{rel}(x''))\between w+(\nu_{rel}(y')+\sigma_{rel}(y''))\between z+(\nu_{rel}(x')+\sigma_{rel}(x''))\mid(\nu_{rel}(y')+\sigma_{rel}(y''))$,
and $p'\rightsquigarrow x'$, $q'\rightsquigarrow y'$, $x''\in\mathcal{RP}(p'')$ and $y''\in\mathcal{RP}(q'')$. But then,
$(\nu_{rel}(p'),z)\between(\nu_{rel}(q'),w)+\big(\sigma_{rel}(p'')\between w+\sigma_{rel}(q'')\between z+\sigma_{rel}(p'')\mid\sigma_{rel}(q'')\big)\rightsquigarrow V$,
for $V\equiv(\nu_{rel}(x')\between w+\nu_{rel}(y')\between z+\nu_{rel}(x')\mid\nu_{rel}(y'))+\big(\sigma_{rel}(x'')\between w+\sigma_{rel}(y'')\between z+\sigma_{rel}(x'')\mid\sigma_{rel}(y'')\big)$ and we need to prove that
$U\leftrightarrows V$. (1)
If $(\nu_{rel}(p'),z)\between(\nu_{rel}(q'),w)+\big(\sigma_{rel}(p'')\between w+\sigma_{rel}(q'')\between z+\sigma_{rel}(p'')\mid\sigma_{rel}(q'')\big)\rightsquigarrow V_1$,
then $V_1\equiv(\nu_{rel}(x')\between w+\nu_{rel}(y')\between z+\nu_{rel}(x')\mid\nu_{rel}(y'))+\big(\sigma_{rel}(x_1'')\between w+\sigma_{rel}(y_1'')\between z+\sigma_{rel}(x_2'')\mid\sigma_{rel}(y_2'')\big)$
for $p'\rightsquigarrow x'$, $q'\rightsquigarrow y'$, $x_1'',x_2''\in\mathcal{RP}(p'')$ and $y_1'',y_2''\in\mathcal{RP}(q'')$. And then,
$((\nu_{rel}(p')+\sigma_{rel}(p''),z)\between(\nu_{rel}(q')+\sigma_{rel}(q''),w)\rightsquigarrow U_1$ for
$U_1\equiv((\nu_{rel}(x')+\sigma_{rel}(x_1''))\between w+(\nu_{rel}(y)+\sigma_{rel}(y_1''))\between z+(\nu_{rel}(x')+\sigma_{rel}(x_1''))\mid(\nu_{rel}(y')+\sigma_{rel}(y_1''))$.
We need to prove that $U_1\leftrightarrows V_1$. Because (1) is a subcase of this one, it is sufficient to prove that $U_1\leftrightarrows V_1$ for U_1 and V_1 as given above.

σ-transitions. If $((\nu_{rel}(x')+\sigma_{rel}(x''))\between w+(\nu_{rel}(y')+\sigma_{rel}(y''))\between z+(\nu_{rel}(x')+\sigma_{rel}(x''))\mid(\nu_{rel}(y')+\sigma_{rel}(y''))\xrightarrow{\sigma}u$, then the following cases are possible:

Case $(\nu_{rel}(x')+\sigma_{rel}(x_1''))\between w\not\xrightarrow{\sigma}$, $(\nu_{rel}(y')+\sigma_{rel}(y_1''))\between z\not\xrightarrow{\sigma}$ *and* $(\nu_{rel}(x')+\sigma_{rel}(x_1''))\mid(\nu_{rel}(y')+\sigma_{rel}(y_1''))\xrightarrow{\sigma}u$.
$\neg\boldsymbol{D}(z)$, $\neg\boldsymbol{D}(w)$ and $u\equiv x_1''\mid y_1''$. Then, $\sigma_{rel}(x_1'')\between w\not\xrightarrow{\sigma}$, $\sigma_{rel}(y_1'')\between z\not\xrightarrow{\sigma}$ and $\sigma_{rel}(x_2'')\mid\sigma_{rel}(y_2'')\xrightarrow{\sigma}x_2''\mid y_2''$. Finally, $x_1''\mid y_1''\leftrightarrows x_2''\mid y_2''$ due to the Congruence theorem;

Case $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \between w \xrightarrow{\sigma} u_1$, $(\nu_{rel}(y') + \sigma_{rel}(y''_1)) \between z \not\xrightarrow{\mathcal{J}}$ *and* $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \mid (\nu_{rel}(y') + \sigma_{rel}(y''_1)) \xrightarrow{\sigma} u_3$.
$\neg \boldsymbol{D}(z)$ and $u \equiv (x''_1 \between \overline{\boldsymbol{\sigma}}(w)) + x''_1 \mid y''_1$. This yields $\sigma_{rel}(x''_1) \between w \xrightarrow{\sigma} x''_1 \between \overline{\boldsymbol{\sigma}}(w)$, $\sigma_{rel}(y''_1) \between z \not\xrightarrow{\mathcal{J}}$ and $\sigma_{rel}(x''_2) \mid \sigma_{rel}(y''_2) \xrightarrow{\sigma} x''_2 \mid y''_2$. Moreover, $x''_1 \between \overline{\boldsymbol{\sigma}}(w) + x''_1 \mid y''_1 \leftrightarrows x''_1 \between \overline{\boldsymbol{\sigma}}(w) + x''_2 \mid y''_2$ due to the Congruence theorem;

Case $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \between w \not\xrightarrow{\mathcal{J}}$, $(\nu_{rel}(y') + \sigma_{rel}(y''_1)) \between z \xrightarrow{\sigma} u_2$ *and* $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \mid (\nu_{rel}(y') + \sigma_{rel}(y''_1)) \xrightarrow{\sigma} u_3$.
This case is similar to the previous one;

Case $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \between w \xrightarrow{\sigma} u_1$, $(\nu_{rel}(y') + \sigma_{rel}(y''_1)) \between z \xrightarrow{\sigma} u_2$ *and* $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \mid (\nu_{rel}(y') + \sigma_{rel}(y''_1)) \xrightarrow{\sigma} u_3$.
$u \equiv x''_1 \between \overline{\boldsymbol{\sigma}}(w) + y''_1 \between \overline{\boldsymbol{\sigma}}(w) + x''_1 \mid y''_1$. Then, $\sigma_{rel}(x''_1) \between w \xrightarrow{\sigma} x''_1 \between \overline{\boldsymbol{\sigma}}(w)$, $\sigma_{rel}(y''_1) \between z \xrightarrow{\sigma} y''_1 \between \overline{\boldsymbol{\sigma}}(z)$ and $\sigma_{rel}(x''_2) \mid \sigma_{rel}(y''_2) \xrightarrow{\sigma} x''_2 \mid y''_2$. Moreover, $x''_1 \between \overline{\boldsymbol{\sigma}}(w) + y''_1 \between \overline{\boldsymbol{\sigma}}(w) + x''_1 \mid y''_1 \leftrightarrows x''_1 \between \overline{\boldsymbol{\sigma}}(w) + y''_1 \between \overline{\boldsymbol{\sigma}}(w) + x''_2 \mid y''_2$ due to the Congruence theorem.

If $(\nu_{rel}(x') \between w + \nu_{rel}(y') \between z + \nu_{rel}(x') \mid \nu_{rel}(y')) + \big(\sigma_{rel}(x''_1) \between w + \sigma_{rel}(y''_1) \between z + \sigma_{rel}(x''_2) \mid \sigma_{rel}(y''_2)\big) \xrightarrow{\sigma} v$ then the following cases are possible:

Case $\sigma_{rel}(x''_1) \between w \not\xrightarrow{\mathcal{J}}$, $\sigma_{rel}(y''_1) \between z \not\xrightarrow{\mathcal{J}}$ *and*$\sigma_{rel}(x''_2) \mid \sigma_{rel}(y''_2) \xrightarrow{\sigma} v$. $\neg \boldsymbol{D}(z)$, $\neg \boldsymbol{D}(w)$ and $v \equiv x''_2 \mid y''_2$. Then, $\nu_{rel}(x') + \sigma_{rel}(x''_1) \between w \not\xrightarrow{\mathcal{J}}$, $\nu_{rel}(y') + \sigma_{rel}(y''_1) \between z \not\xrightarrow{\mathcal{J}}$ and $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \mid (\nu_{rel}(y') + \sigma_{rel}(y''_1)) \xrightarrow{\sigma} x''_1 \mid y''_1$. Moreover, $x''_2 \mid y''_2 \leftrightarrows x''_1 \mid y''_1$ due to the Congruence theorem;

Case $\sigma_{rel}(x''_1) \between w \xrightarrow{\sigma} v_1$, $\sigma_{rel}(y''_1) \between z \not\xrightarrow{\mathcal{J}}$ *and* $\sigma_{rel}(x''_2) \mid \sigma_{rel}(y''_2) \xrightarrow{\sigma} v_3$. $\neg \boldsymbol{D}(z)$ and $v \equiv x''_1 \between \overline{\boldsymbol{\sigma}}(w) + x''_2 \mid y''_2$. This yields $\nu_{rel}(x') + \sigma_{rel}(x''_1) \between w \xrightarrow{\sigma} x''_1 \between \overline{\boldsymbol{\sigma}}(w)$, $\nu_{rel}(y') + \sigma_{rel}(y''_1) \between z \not\xrightarrow{\mathcal{J}}$ and $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \mid (\nu_{rel}(y') + \sigma_{rel}(y''_1)) \xrightarrow{\sigma} x''_1 \mid y''_1$. Finally, $x''_1 \between \overline{\boldsymbol{\sigma}}(w) + x''_2 \mid y''_2 \leftrightarrows x''_1 \between \overline{\boldsymbol{\sigma}}(w) + x''_1 \mid y''_1$ due to the Congruence theorem;

Case $\sigma_{rel}(x''_1) \between w \not\xrightarrow{\mathcal{J}}$, $\sigma_{rel}(y''_1) \between z \xrightarrow{\sigma} v_2$ *and* $\sigma_{rel}(x''_2) \mid \sigma_{rel}(y''_2) \xrightarrow{\sigma} v_3$. This case is similar to the previous one;

Case $\sigma_{rel}(x''_1) \between w \xrightarrow{\sigma} v_1$, $\sigma_{rel}(y''_1) \between z \xrightarrow{\sigma} v_2$ *and* $\sigma_{rel}(x''_2) \mid \sigma_{rel}(y''_2) \xrightarrow{\sigma} v_3$. $v \equiv x''_1 \between \overline{\boldsymbol{\sigma}}(w) + y''_1 \between \overline{\boldsymbol{\sigma}}(z) + x''_2 \mid y''_2$. It implies $\nu_{rel}(x') + \sigma_{rel}(x''_1) \between w \xrightarrow{\sigma} x''_1 \between \overline{\boldsymbol{\sigma}}(w)$, $\nu_{rel}(y') + \sigma_{rel}(y''_1) \between z \xrightarrow{\sigma} y''_1 \between \overline{\boldsymbol{\sigma}}(z)$ and $(\nu_{rel}(x') + \sigma_{rel}(x''_1)) \mid (\nu_{rel}(y') + \sigma_{rel}(y''_1)) \xrightarrow{\sigma} x''_1 \mid y''_1$. To conclude $x''_1 \between \overline{\boldsymbol{\sigma}}(w) + y''_1 \between \overline{\boldsymbol{\sigma}}(z) + x''_2 \mid y''_2 \leftrightarrows$
$x''_1 \between \overline{\boldsymbol{\sigma}}(w) + y''_1 \between \overline{\boldsymbol{\sigma}}(z) + x''_1 \mid y''_1$ due to the Congruence theorem.

PDF. Now let us suppose that $M \in \mathbb{DP}(pACP^+_{drt})/\leftrightarrows$. From the discussion above we conclude that
$p \equiv ((\nu_{rel}(p') + \sigma_{rel}(p''), z) \between (\nu_{rel}(q') + \sigma_{rel}(q''), w) \rightsquigarrow M$ iff
$q \equiv (\nu_{rel}(p'), z) \between (\nu_{rel}(q'), w) + \big(\sigma_{rel}(p'') \between w + \sigma_{rel}(q'') \between z + \sigma_{rel}(p'') \mid \sigma_{rel}(q'')\big) \rightsquigarrow M$.
Also,
$((\nu_{rel}(x')+\sigma_{rel}(x''_1)) \between w+(\nu_{rel}(y')+\sigma_{rel}(y''_1)) \between z+(\nu_{rel}(x')+\sigma_{rel}(x''_1)) \mid (\nu_{rel}(y')+\sigma_{rel}(y''_1)) \in M$, iff
$(\nu_{rel}(x') \between w + \nu_{rel}(y') \between z + \nu_{rel}(x') \mid \nu_{rel}(y')) + \big(\sigma_{rel}(x''_1) \between w + \sigma_{rel}(y''_1) \between z + \sigma_{rel}(x''_2) \mid \sigma_{rel}(y''_2)\big) \in M$
for $p' \rightsquigarrow x'$, $q' \rightsquigarrow y'$, $x''_1, x''_2 \in \mathcal{RP}(p'')$ and $y''_1, y''_2 \in \mathcal{RP}(q'')$. Moreover, the subset of reachable elements from p in M is contained in the set:

$K = \big(\nu_{rel}([x']_{\leftrightarrows}) + \sigma_{rel}(\mathcal{RP}(p''))^z \,\|^w \big(\nu_{rel}([y']_{\leftrightarrows}) + \sigma_{rel}(\mathcal{RP}(q'')\big) \subset M$. The subset of reachable elements from q in M is contained in the set:
$N = \nu_{rel}([x']_{\leftrightarrows})^z \,\|^w \nu_{rel}([y']_{\leftrightarrows}) + \big(\sigma_{rel}(\mathcal{RP}(p''))\between w + \sigma_{rel}(\mathcal{RP}(q''))\between z + \sigma_{rel}(\mathcal{RP}(p'')) \,|\, \sigma_{rel}(\mathcal{RP}(q''))\big) \subset M$.
Having that $\mu(p'', \mathcal{RP}(p'')) = 1$ and $\mu(q'', \mathcal{RP}(q'')) = 1$ we obtain:
$$\begin{aligned}
&\mu\big(((\nu_{rel}(p') + \sigma_{rel}(p''), z) \between (\nu_{rel}(q') + \sigma_{rel}(q''), w), M\big)\\
&\quad = \mu\big(((\nu_{rel}(p') + \sigma_{rel}(p''), z) \between (\nu_{rel}(q') + \sigma_{rel}(q''), w), K\big)\\
&\quad = \mu(p', [x']_{\leftrightarrows}) \cdot \mu(q', [y']_{\leftrightarrows}) \cdot \mu(p'', \mathcal{RP}(p'')) \cdot \mu(q'', \mathcal{RP}(q''))\\
&\quad = \mu(p', [x']_{\leftrightarrows}) \cdot \mu(q', [y']_{\leftrightarrows}).
\end{aligned}$$
And also,
$$\begin{aligned}
&\mu\Big((\nu_{rel}(p'), z) \between (\nu_{rel}(q'), w) + \big(\sigma_{rel}(p'')\between w + \sigma_{rel}(q'')\between z + \sigma_{rel}(p'') \,|\, \sigma_{rel}(q'')\big), M\Big)\\
&\quad = \mu\Big((\nu_{rel}(p'), z) \between (\nu_{rel}(q'), w) + \big(\sigma_{rel}(p'')\between w + \sigma_{rel}(q'')\between z + \sigma_{rel}(p'') \,|\, \sigma_{rel}(q'')\big), N\Big)\\
&\quad = \mu(p', [x']_{\leftrightarrows}) \cdot \mu(q', [y']_{\leftrightarrows}) \cdot \mu(p'', \mathcal{RP}(p'')) \cdot \mu(q'', \mathcal{RP}(q'')) \cdot \mu(p'', \mathcal{RP}(p'')) \cdot \mu(q'', \mathcal{RP}(q''))\\
&\quad = \mu(p', [x']_{\leftrightarrows}) \cdot \mu(q', [y']_{\leftrightarrows}).
\end{aligned}$$

***D** predicate.* From $\boldsymbol{D}(\sigma_{rel}(p''))$ and $\boldsymbol{D}(\sigma_{rel}(q''))$ it follows that $\boldsymbol{D}\big(((\nu_{rel}(p') + \sigma_{rel}(p''), z) \between (\nu_{rel}(q') + \sigma_{rel}(q''), w)\big)$. Also since $\boldsymbol{D}(\sigma_{rel}(p'') \,|\, \sigma_{rel}(q''))$ we have $\boldsymbol{D}\big((\nu_{rel}(p'), z) \between (\nu_{rel}(q'), w) + (\sigma_{rel}(p'')\between w + \sigma_{rel}(q'')\between z + \sigma_{rel}(p'') \,|\, \sigma_{rel}(q''))\big)$ as well. Then, since $\boldsymbol{D}\big((\nu_{rel}(x') + \sigma_{rel}(x_1'')) \,|\, (\nu_{rel}(y') + \sigma_{rel}(y_1''))\big)$ we obtain $\boldsymbol{D}\big((\nu_{rel}(x') + \sigma_{rel}(x_1''))\between w + (\nu_{rel}(y') + \sigma_{rel}(y_1''))\between z + (\nu_{rel}(x') + \sigma_{rel}(x_1'')) \,|\, (\nu_{rel}(y') + \sigma_{rel}(y_1''))\big)$. And $\boldsymbol{D}\Big((\nu_{rel}(x')\between w + \nu_{rel}(y')\between z + \nu_{rel}(x') \,|\, \nu_{rel}(y')) + \big(\sigma_{rel}(x_1'')\between w + \sigma_{rel}(y_1'')\between z + \sigma_{rel}(x_2'') \,|\, \sigma_{rel}(y_2''))\Big)$ since $\boldsymbol{D}(\sigma_{rel}(x_2'') \,|\, \sigma_{rel}(y_2''))$.

Axiom PrDRTMM5. Let $p, q \in \mathbb{SP}(pACP^+_{drt})$ such that $p \leftrightarrows p + p$, $q \leftrightarrows q + q$ and $\mathcal{RP}(p) = \{x : p \rightsquigarrow x\}$, $\mathcal{RP}(q) = \{y : q \rightsquigarrow y\}$. From Lemma 5.5.27 (4.3.17 *ii.*) we have that for every $x_1, x_2 \in \mathcal{RP}(p)$, $x_1 \leftrightarrows x_2$ and $\mu(p, \mathcal{RP}(p)) = 1$. And also for every $y_1, y_2 \in \mathcal{RP}(q)$, $y_1 \leftrightarrows y_2$ and $\mu(q, \mathcal{RP}(q)) = 1$. We will prove that for arbitrary $p, q \in \mathbb{SP}(pACP^+_{drt})$, $(\nu_{rel}(p), z) \between (\nu_{rel}(q), w) \leftrightarrows \nu_{rel}(p)\between z + \nu_{rel}(q)\between w + \nu_{rel}(p) \,|\, \nu_{rel}(q)$.

Probabilistic transitions. If $(\nu_{rel}(p), z) \between (\nu_{rel}(q), w) \rightsquigarrow u$, then $u \equiv \nu_{rel}(x)\between w + \nu_{rel}(y)\between z + \nu_{rel}(x) \,|\, \nu_{rel}(y)$, for some $x \in \mathcal{RP}(p)$ and $y \in \mathcal{RP}(q)$. Then, $\nu_{rel}(p)\between z + \nu_{rel}(q)\between w + \nu_{rel}(p) \,|\, \nu_{rel}(q) \rightsquigarrow v$, for $v \equiv \nu_{rel}(x)\between w + \nu_{rel}(y)\between z + \nu_{rel}(x) \,|\, \nu_{rel}(y)$ and $u \leftrightarrows v$.
If $\nu_{rel}(p)\between z + \nu_{rel}(q)\between w + \nu_{rel}(p) \,|\, \nu_{rel}(q) \rightsquigarrow v_1$, then $v_1 \equiv \nu_{rel}(x)\between w + \nu_{rel}(y)\between z + \nu_{rel}(x') \,|\, \nu_{rel}(y')$ for some $x, x' \in \mathcal{RP}(p)$ and $y, y' \in \mathcal{RP}(q)$. And then, $(\nu_{rel}(p), z) \between (\nu_{rel}(q), w) \rightsquigarrow u_1$ for $u_1 \equiv \nu_{rel}(x)\between w + \nu_{rel}(y)\between z + \nu_{rel}(x) \,|\, \nu_{rel}(y)$ and $v_1 \leftrightarrows u_1$ according to the Congruence theorem of $pACP^+_{drt}$.

PDF. Now let us suppose that $M \in \mathbb{DP}(pACP^+_{drt})/\leftrightarrows$. From the discussion above we conclude that
$(\nu_{rel}(p), z) \between (\nu_{rel}(q), w) \rightsquigarrow M$ iff $\nu_{rel}(p)\between w + \nu_{rel}(q)\between z + \nu_{rel}(p) \,|\, \nu_{rel}(q) \rightsquigarrow M$ and $\nu_{rel}(x)\between w + \nu_{rel}(y)\between z + \nu_{rel}(x') \,|\, \nu_{rel}(y') \in M$, iff
$\nu_{rel}(x)\between w + \nu_{rel}(y)\between z + \nu_{rel}(x) \,|\, \nu_{rel}(y) \in M$
for $x, x' \in \mathcal{RP}(p)$ and $y, y' \in \mathcal{RP}(q)$. Then,

$$\begin{aligned}
&\mu\big((\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(q),w),M\big)\\
&\quad=\mu\big((\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(q),w),\{\nu_{rel}(x)\between w+\nu_{rel}(y)\between z+\nu_{rel}(x)\,|\,\nu_{rel}(y)\ :\\
&\qquad\qquad x\in\mathcal{RP}(p)\ \&\ y\in\mathcal{RP}(q)\}\big)\\
&\quad=\mu\big((\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(q),w),\nu_{rel}(\mathcal{RP}(p))^{z}\,]\![^{w}\nu_{rel}(\mathcal{RP}(q))\big)\\
&\quad=\mu(p,\mathcal{RP}(p))\cdot\mu(q,\mathcal{RP}(q))=1\text{ and}\\
&\mu(\nu_{rel}(p)\between w+\nu_{rel}(q)\between z+\nu_{rel}(p)\,|\,\nu_{rel}(q),M)\\
&\quad=\mu(\nu_{rel}(p)\between w+\nu_{rel}(q)\between z+\nu_{rel}(p)\,|\,\nu_{rel}(q),\{\nu_{rel}(x)\between w+\nu_{rel}(y)\between z+\nu_{rel}(x')\,|\,\nu_{rel}(y')\ :\\
&\qquad\qquad x,x'\in\mathcal{RP}(p)\ \&\ y,y'\in\mathcal{RP}(q)\})\\
&\quad=\mu(p,\mathcal{RP}(p))\cdot\mu(q,\mathcal{RP}(q))\cdot\mu(p,\mathcal{RP}(p))\cdot\mu(q,\mathcal{RP}(q))=1.
\end{aligned}$$

***D** predicate.* Both $\neg\boldsymbol{D}\big((\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(q),w)\big)$ and $\neg\boldsymbol{D}\big(\nu_{rel}(p)\between w+\nu_{rel}(q)\between z+\nu_{rel}(p)\,|\,\nu_{rel}(q)\big)$ since $\neg\boldsymbol{D}(\nu_{rel}(p))$ and $\neg\boldsymbol{D}(\nu_{rel}(q))$.

Axiom PrDRTMM6. We define a relation R in the following way:

$$\begin{aligned}
R=Eq\Big(\quad&\{\big((\nu_{rel}(p)+\sigma_{rel}(q),z)\,]\![\,(\nu_{rel}(r),w),(\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(r),w)+\sigma_{rel}(q)\between w\big)\\
&\qquad:\ p,q,r,z,w\in\mathbb{SP}(\textit{pACP}^{+}_{drt})\}\\
\cup\ &\{\big((\nu_{rel}(u)+\sigma_{rel}(v))\between w+\nu_{rel}(t)\between z+(\nu_{rel}(u)+\sigma_{rel}(v))\,|\,\nu_{rel}(t),\\
&\qquad\nu_{rel}(u)\between w+\nu_{rel}(t)\between z+\nu_{rel}(u)\,|\,\nu_{rel}(t)+\sigma_{rel}(v)\between w\big)\\
&\qquad:\ u,v,t\in\mathbb{DP}(\textit{pACP}^{+}_{drt}),z,w\in\mathbb{SP}(\textit{pACP}^{+}_{drt})\}\Big),
\end{aligned}$$

Let us note that $p\rightsquigarrow x,q\rightsquigarrow y,r\rightsquigarrow t$ iff

$(\nu_{rel}(p)+\sigma_{rel}(q),z)\,]\![\,(\nu_{rel}(r),w)\rightsquigarrow(\nu_{rel}(x)+\sigma_{rel}(y))\between w+\nu_{rel}(t)\between z+(\nu_{rel}(x)+\sigma_{rel}(y))\,|\,\nu_{rel}(t)$ iff

$(\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(r),w)+\sigma_{rel}(q)\between w\rightsquigarrow\nu_{rel}(x)\between w+\nu_{rel}(t)\between z+\nu_{rel}(x)\,|\,\nu_{rel}(t)+\sigma_{rel}(y)\between w$. And if $M\in\mathbb{DP}(\textit{pACP}^{+}_{drt})$, then $(\nu_{rel}(x)+\sigma_{rel}(y))\between w+\nu_{rel}(t)\between z+(\nu_{rel}(x)+\sigma_{rel}(y))\,|\,\nu_{rel}(t)\in M$ iff $\nu_{rel}(x)\between w+\nu_{rel}(t)\between z+\nu_{rel}(x)\,|\,\nu_{rel}(t)+\sigma_{rel}(v)\between w\in M$.

PDF. The following equalities are valid:

$$\begin{aligned}
&\mu\big(\nu_{rel}(p)+\sigma_{rel}(q),z)\,]\![\,(\nu_{rel}(r),w),(\nu_{rel}(x)+\sigma_{rel}(y))\between w\\
&\qquad\qquad+\nu_{rel}(t)\between z+(\nu_{rel}(x)+\sigma_{rel}(y))\,|\,\nu_{rel}(t)\big)\\
&\quad=\mu\big(\nu_{rel}(p)+\sigma_{rel}(q),\nu_{rel}(x)+\sigma_{rel}(y)\big)\cdot\mu(\nu_{rel}(r),\nu_{rel}(t))\\
&\quad=\mu(p,x)\cdot\mu(q,y)\cdot\mu(r,t)\text{ and}\\
&\mu\big((\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(r),w)+\sigma_{rel}(q)\between w,\nu_{rel}(x)\between w\\
&\qquad\qquad+\nu_{rel}(t)\between z+\nu_{rel}(x)\,|\,\nu_{rel}(t)+\sigma_{rel}(y)\between w\big)\\
&\quad=\mu\big((\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(r),w),\nu_{rel}(x)\between w\\
&\qquad\qquad+\nu_{rel}(t)\between z+\nu_{rel}(x)\,|\,\nu_{rel}(t)\big)\cdot\mu(\sigma_{rel}(q)\between w,\sigma_{rel}(y)\between w)\\
&\quad=\mu(\nu_{rel}(p),\nu_{rel}(x))\cdot\mu(\nu_{rel}(r),\nu_{rel}(t))\cdot\mu(\sigma_{rel}(q),\sigma_{rel}(y))\\
&\quad=\mu(p,x)\cdot\mu(r,t)\cdot\mu(q,y).
\end{aligned}$$

The result follows from Proposition 3.3.10.

σ-transitions. We observe that only the following transitions are possible only if $\boldsymbol{D}(w)$:
$(\nu_{rel}(x)+\sigma_{rel}(y))\between w+\nu_{rel}(t)\between z+(\nu_{rel}(x)+\sigma_{rel}(y))\,|\,\nu_{rel}(t)\xrightarrow{\sigma}y\between\overline{\boldsymbol{\sigma}}(w)$ and $\nu_{rel}(x)\between w+\nu_{rel}(t)\between z+\nu_{rel}(x)\,|\,\nu_{rel}(t)+\sigma_{rel}(y)\between w\xrightarrow{\sigma}y\between\overline{\boldsymbol{\sigma}}(w)$ and $(y\between\overline{\boldsymbol{\sigma}}(w),y\between\overline{\boldsymbol{\sigma}}(w))\in R$.

***D** predicate.* $\boldsymbol{D}\big(\nu_{rel}(p)+\sigma_{rel}(q),z)\,]\![\,(\nu_{rel}(r),w)\big)$ iff $\boldsymbol{D}(w)$ and $\boldsymbol{D}(z)$ iff $\boldsymbol{D}((\nu_{rel}(p),z)\,]\![\,(\nu_{rel}(r),w)+\sigma_{rel}(q)\between w)$. And also, $\boldsymbol{D}\big((\nu_{rel}(u)+\sigma_{rel}(v))\between w+$

$\nu_{rel}(t) \between z + (\nu_{rel}(u) + \sigma_{rel}(v)) \mid \nu_{rel}(t)\big)$ iff $\boldsymbol{D}(w)$ iff $\boldsymbol{D}\big(\nu_{rel}(u) \between w + \nu_{rel}(t) \between z + \nu_{rel}(u) \mid \nu_{rel}(t) + \sigma_{rel}(v) \between w\big)$.

Axiom PrDRTMM7. We define a relation R in the following way:

$$\begin{aligned} R = Eq\Big(& \{\big((\nu_{rel}(p), z) \between (\nu_{rel}(q) + \sigma_{rel}(r), w), (\nu_{rel}(p), z) \between (\nu_{rel}(r), w) + \sigma_{rel}(q) \between z\big) \\ & : p, q, r, z, w \in \mathbb{SP}(pACP^+_{drt})\} \\ \cup \ & \{\big(\nu_{rel}(u) \between w + (\nu_{rel}(v) + \sigma_{rel}(t)) \between z + \nu_{rel}(u) \mid (\nu_{rel}(v) + \sigma_{rel}(t)), \\ & \nu_{rel}(u) \between w + \nu_{rel}(v) \between z + \nu_{rel}(u) \mid \nu_{rel}(v) + \sigma_{rel}(v) \between w\big) \\ & : u, v, t \in \mathbb{DP}(pACP^+_{drt}), z, w \in \mathbb{SP}(pACP^+_{drt})\}\Big). \end{aligned}$$

The proof goes in a similar way like the proof of the axiom PrDRTMM6.

□

Completeness of $pACP^+_{drt}$

Next, we prove the completeness property of $pACP^+_{drt}$. As we did in Section 4.3.1 we do not use the direct method but we obtain the completeness property by showing that $\mathbf{T}_{pACP^+_{drt}}$ is a conservative operational extension of $\mathbf{T}_{pBPA_{drt}}$. First we will show that we cannot use the method of stratification because $\mathbf{T}_{pACP^+_{drt}}$ *is not stratifiable*. Since the method of stratification is not applicable on $\mathbf{T}_{pACP^+_{drt}}$ we employ the technique of reduction which was briefly introduced in Section 2.3. By this we will show that: 1. the deduction system $\mathbf{T}_{pACP^+_{drt}}$ is meaningful, 2. $\mathbf{T}_{pACP^+_{drt}}$ is a operational conservative extension of $\mathbf{T}_{pBPA_{drt}}$, and 3. $pACP^+_{drt}$ is complete axiomatization with respect to the model $\mathcal{M}_{pACP^+_{drt}}$.

Proposition 5.5.29. $\mathbf{T}_{pACP^+_{drt}}$ is not stratifiable.

Proof. Assume that S is a stratification on $\mathbf{T}_{pACP^+_{drt}}$. Then, for any closed substitution of a deduction rule d, if $\phi \in pprem(d)$ and $\psi \in nprem(d)$ then $S(\phi) \leq S(conc(d))$ and $S(\psi) < S(conc(d))$. Now, take the instances of rules:

$$\frac{\neg \boldsymbol{D}(\overline{\boldsymbol{\sigma}}(c))}{\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(c)) \rightsquigarrow \breve{\underline{\underline{\delta}}}} \text{ (R54)}$$

$$\frac{\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(c)) \rightsquigarrow \breve{\underline{\underline{\delta}}}, \breve{\underline{\underline{\delta}}} \xrightarrow{\sigma} t, \boldsymbol{D}(t)}{\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(c))))} \text{ (R51)}$$

$$\frac{c \rightsquigarrow s, s \xrightarrow{\sigma} \overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(c))), \boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(c))))}{\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(c))} \text{ (R51)}$$

Therefore, for S should hold:

$$S(\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(c))) \overset{R54}{<} S(\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(c)) \rightsquigarrow \breve{\underline{\underline{\delta}}}) \overset{R51}{\leq} S(\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(\overline{\boldsymbol{\sigma}}(c))))) \overset{R51}{\leq} S(\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(c))).$$

It is clear that S cannot satisfy this inequality. □

Remark 5.5.30. One can notice that the problem to define a stratification arises from the condition that all possible (unrestricted) substitutions of the rules have to be checked. If we could freely use the observation, made previous, about alternation of $\mathbb{SP}(pACP^+_{drt})$ and $\mathbb{DP}(pACP^+_{drt})$ processes in the transitions, as stated in Remark 5.3.23, then we will be able to define a map which satisfies the properties required for stratification. However, this is not allowed because by doing so we will restrict ourselves to those instances of the deduction rules which the restriction of Remark 5.3.23 allows.

Now, we present results for $\mathbf{T}_{pACP^+_{drt}}$ which bring us to the desired conclusion: $\mathbf{T}_{pACP^+_{drt}}$ is a conservative extension of $\mathbf{T}_{pBPA_{drt}}$. It will be done in a few steps: 1. we reduce $\mathbf{T}_{pACP^+_{drt}}$ to a system $Red^1(\mathbf{T}_{pACP^+_{drt}})$, 2. we define a function M on the set of closed terms over $\Sigma_{pACP^+_{drt}}$ and using it we will prove a property for transitions in the reduced system which will show useful in the next step, 3. using the function M and the property proved in the previous step we define an ordering of the literals in $\mathbf{T}_{pACP^+_{drt}}$, 4. finally, on the basis of the previous steps we are able to define a stratification for $Red^1(\mathbf{T}_{pACP^+_{drt}})$ which provides us with sufficient results to make the final conclusion.

Definition 5.5.31. $Red^1(\mathbf{T}_{pACP^+_{drt}}) = (\breve{\Sigma}_{pACP^+_{drt}}, Reduce(\mathbf{DR}_{pACP^+_{drt}}))$ is a reduction of $\mathbf{T}_{pACP^+_{drt}}$ as defined in Definition 2.3.14.

Definition 5.5.32. A map $M : \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}}) \to \omega^2$, from the set of closed terms over the signature $\breve{\Sigma}_{pACP^+_{drt}}$ to the ordinal ω^2, is defined in the following way:

1. $M(\underline{\underline{a}}) = M(\underline{\underline{\breve{a}}}) = 0$, for $a \in A_\delta$;
2. $M(a) = M(\breve{a}) = \omega$, for $a \in A_\delta$;
3. $M(\nu_{rel}(t)) = M(\partial_H(t)) = M(\overline{\boldsymbol{\sigma}}(t)) = M(t)$, for $t \in \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}})$;
4. $M(\sigma_{rel}(t)) = M(t) + 1$, for $t \in \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}})$;
5. $M(t + s) = M(t \leftplus_\pi s) = M(t \parallel s) = M(t \lfloor\!\lfloor s) = M(t \mid s) = \max\{M(t), M(s)\}$, for $t, s \in \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}})$;
6. $M(t \cdot s) = M(t) + M(s)$, for $t, s \in \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}})$;
7. $M((t, z) \between (s, w)) = \max\{M(t), M(s), M(z), M(w)\}$, for $t, s, z, w \in \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}})$;

It is obvious that M does not count the number of time steps that a process can perform. Actually, it gives the number of time steps that the process might perform if it is not forced to deadlock as soon as a time conflict occurs. (Here we mean situations as: $\nu_{rel}(\sigma_{rel}(t)) = \underline{\underline{\delta}}$, $\sigma_{rel}(t) \lfloor\!\lfloor \nu_{rel}(s) = \underline{\underline{\delta}}$ or $\nu_{rel}(t) \mid \sigma_{rel}(s) = \underline{\underline{\delta}}$.)

Lemma 5.5.33. If $t, u \in \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}})$, then if $t \rightsquigarrow u \in \longrightarrow_{Pos(\mathbf{T}_{pACP^+_{drt}})}$ or $t \xrightarrow{a} u \in \longrightarrow_{Pos(\mathbf{T}_{pACP^+_{drt}})}$ or $t \rightsquigarrow u \in \longrightarrow_{Pos(\mathbf{T}_{pACP^+_{drt}})}$, then $M(t) \geq M(u)$.

Proof. Note that $Pos(\mathbf{T}_{pACP^+_{drt}})$ contains all closed instances of the rules from $\mathbf{T}_{pACP^+_{drt}}$ but without negative premises. Hence, we need to check if the conclusion of each rule satisfies the condition under the assumption that all positive premises in that rules do it as well. For most rules the proof is trivial, so we give only the most interesting cases. Assume that $t, s, u, v, z, w \in \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}})$.

R1.1-R1.8 for each of these rules the check is trivial;

R3. $M(t) \leq M(t) + M(s) = M(t \cdot s)$;

R13. if $M(u) \leq M(t)$, then $M(u \cdot s) = M(u) + M(s) \leq M(t) + M(s) = M(t \cdot s)$;

R16. if $M(u) \leq M(t)$ and $M(v) \leq M(s)$, then
$M(u \between s + v \between t + u \mid v) = \max\{\max\{M(u), M(s)\}, \max\{M(v), M(t)\}, \max\{M(u), M(v)\}\}$
$\leq \max\{\max\{M(t), M(s)\}, \max\{M(s), M(t)\}, \max\{M(t), M(s)\}\}$
$= \max\{M(t), M(s)\} = M(t \parallel s)$;

R17. if $M(u) \leq M(t)$ and $M(v) \leq M(s)$, then
$M(u \between w + v \between z + u \mid v) = \max\{\max\{M(u), M(w)\}, \max\{M(v), M(z)\}, \max\{M(u), M(v)\}\}$
$\leq \max\{\max\{M(t), M(w)\}, \max\{M(s), M(z)\}, \max\{M(t), M(s)\}\}$
$= \max\{M(t), M(s), M(z), M(w)\} = M((t, z) \between\!\between (s, w))$;

R21. if $M(u) \leq M(t)$, then $M(\sigma_{rel}(u)) = M(u) + 1 \leq M(t) + 1 = M(\sigma_{rel}(t))$;

R35. if $M(u) \leq M(t)$, then $M(u \between s) = \max\{M(u), M(s)\} \leq \max\{M(t), M(s)\} = \max\{M(t), M(\overline{\sigma}(s))\} = M(t \between \overline{\sigma}(s))$;

R43. if $M(u) \leq M(t)$, then $M(u \between s) = \max\{M(u), M(s)\} \leq \max\{M(t), M(s)\} = \max\{M(t), M(\overline{\sigma}(s))\} = M(t \between \overline{\sigma}(s))$;

R25. $M(t) \leq M(t) + 1 = M(\sigma_{rel}(t))$. (Note that any instantiation of this rule in $Pos(\mathbf{T}_{pACP^+_{drt}})$ has the form: $\sigma_{rel}(t) \xrightarrow{\sigma} t$, since the negative premise is removed.)

R26. if $M(u) \leq M(t)$, then $M(u) \leq M(t) \leq \max\{M(t), M(s)\} = M(t + s)$. (Also, the negative premise is omitted.)

R34. $M(\breve{\delta}) = 0 \leq M(\overline{\sigma}(t))$.

□

Definition 5.5.34. On the basis of the function M we define a pre-order on the set of literals in the following way:

1. $(t \xrightarrow{\sigma} u) \leq (t' \xrightarrow{\sigma} u')$ iff $\begin{cases} M(t) < M(t') \\ M(t) = M(t') \,\&\, n_+(t) \leq n_+(t') \end{cases}$
2. $(\boldsymbol{D}(t)) \leq (t' \rightsquigarrow u')$ iff $\begin{cases} M(t) < M(t') \\ M(t) = M(t') \,\&\, n_{\overline{\sigma}}(t) \leq n_{\overline{\sigma}}(t') \end{cases}$
3. if $R \not\xrightarrow{\sigma}$ or $R' \not\xrightarrow{\sigma}$, then $(tRu) \leq (t'R'u')$ iff $M(t) \leq M(t')$;
4. if $P \neq \boldsymbol{D}$ and $R' \not\rightsquigarrow$, then $Pt \leq (t'R'u')$ iff $M(t) \leq M(t')$;
5. for any $R \in \{\rightsquigarrow, \xrightarrow{a}, \xrightarrow{\sigma}\}$ and $P, P' \in \{\boldsymbol{D}, \xrightarrow{a} \surd\}$,
$(tRu) \leq (P't')$ iff $M(t) \leq M(t')$ and
$(Pt) \leq (P't')$ iff $M(t) \leq M(t')$,

where $n_+(t)$ and $n_{\overline{\sigma}}(t)$ denote the number of $+$ and $\overline{\sigma}$ operators in t respectively.

This pre-order induces an equivalence relation on the set of literals as:

$$\phi \approx \psi \text{ iff } \phi \leq \psi \text{ and } \psi \leq \phi.$$

For some ordinal α we define implicitly a function $S : \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}}) \to \alpha$ as: for literals ϕ and ψ

1. if $\phi \approx \psi$, then $S(\phi) = S(\psi)$;
2. if $\phi \leq \psi$ and $\phi \not\approx \psi$, then $S(\phi) < S(\psi)$.

Lemma 5.5.35. S is a stratification of $Red^1(\mathbf{T}_{pACP^+_{drt}})$.

Proof. We need to investigate all rule (more precisely all instances of the rules), but we just present the most interesting cases and for the rest the proof is trivial. Let $t, s, u, v, z, w \in \mathbb{C}(\breve{\Sigma}_{pACP^+_{drt}})$.

R13. Since $M(t) \leq M(t \cdot s)$ follows that $t \rightsquigarrow u \leq t \cdot s \rightsquigarrow u \cdot s$ and also $S(t \rightsquigarrow u) \leq S(t \cdot s \rightsquigarrow u \cdot s)$;

R26. Since $M(t) \leq M(t \cdot s) = M(t) + M(s)$ follows that $t \xrightarrow{\sigma} u \leq t \cdot s \xrightarrow{\sigma} u \cdot s$. Now,

1. if $M(t) < M(t \cdot s)$, then $\neg\big((t \cdot s \xrightarrow{\sigma} u \cdot s) \leq (t \xrightarrow{\sigma} u)\big)$, from which $S(t \xrightarrow{\sigma} u)) < S(t \cdot s \xrightarrow{\sigma} u \cdot s)$;
2. if $M(t) = M(t \cdot s)$, then since by the definition $n_+(t) = n_+(t \cdot s)$, $(t \xrightarrow{\sigma} u) \leq t \cdot s \xrightarrow{\sigma} u \cdot s$, but also $(t \cdot s \xrightarrow{\sigma} u \cdot s) \leq (t \xrightarrow{\sigma} u)$, from which $S(t \xrightarrow{\sigma} u)) = S(t \cdot s \xrightarrow{\sigma} u \cdot s)$;

R27. Since $M(t) \leq M(t + s) = \max\{M(t), M(s)\}$ follows that $t \xrightarrow{\sigma} u \leq t + s \xrightarrow{\sigma} u + v$. Moreover from $n_+(t) < n_+(t + s)$ follows that $S(t \xrightarrow{\sigma} u) < S(t + s \xrightarrow{\sigma} u + v)$;

R33. From Lemma 5.5.33 $Red^1(\mathbf{T}_{pACP^+_{drt}})$ contains only the instances of this rule for which $M(v) \leq M(u) \leq M(t)$ (where $t \rightsquigarrow u$ and $u \xrightarrow{\sigma} v$ are the premises of the rule). Hence, $(t \rightsquigarrow u) \approx (\overline{\boldsymbol{\sigma}}(t) \rightsquigarrow v)$ and $(u \xrightarrow{\sigma} v) \leq (\overline{\boldsymbol{\sigma}}(t) \rightsquigarrow v)$ from which $S(t \rightsquigarrow u) \leq S(\overline{\boldsymbol{\sigma}}(t) \rightsquigarrow v)$ and $S(u \xrightarrow{\sigma} v) \leq S(\overline{\boldsymbol{\sigma}}(t) \rightsquigarrow v)$;

R43. In a similar way as above from Lemma 5.5.33 follows that $Red^1(\mathbf{T}_{pACP^+_{drt}})$ contains only the instances of this rule for which $M(v) \leq M(u) \leq M(t)$ (where $t \rightsquigarrow u$ and $u \xrightarrow{\sigma} v$ are the premises of the rule). Hence, $(t \rightsquigarrow u) \approx (\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(t)))$ (because $M(t) = M(\overline{\boldsymbol{\sigma}}(t))$), $(u \xrightarrow{\sigma} v) \leq (\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(t)))$ (because $M(u) \leq M(\overline{\boldsymbol{\sigma}}(t))$ and $(\boldsymbol{D}(v)) \leq (\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(t)))$ (because $M(v) \leq M(\overline{\boldsymbol{\sigma}}(t))$). Thus, $S(t \rightsquigarrow u) \leq S(\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(t)))$, $S(u \xrightarrow{\sigma} v) \leq S(\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(t)))$ and $S(\boldsymbol{D}(v)) \leq S(\boldsymbol{D}(\overline{\boldsymbol{\sigma}}(t)))$;

R25. Since $M(t) < M(\sigma_{rel}(t)) = M(t) + 1$ follows that $(t \rightsquigarrow u) \leq \sigma_{rel}(t) \xrightarrow{\sigma} t$ (notice that u is an arbitrary closed term) and $\neg\big(\sigma_{rel}(t) \xrightarrow{\sigma} t \leq (t \rightsquigarrow u)\big)$. Therefore, $S(t \rightsquigarrow u) < S(\sigma_{rel}(t) \xrightarrow{\sigma} t)$;

R26. For the positive premise the proof is easy. We only prove the case for the negative premise $s \xrightarrow{\sigma}\!\!\!\!\!/\;$. Because $M(s) \leq M(t + s)$ follows that $(s \xrightarrow{\sigma} v) \leq (t + s \xrightarrow{\sigma} u)$ for an arbitrary closed term v. Moreover, since $n_+(s) < n_+(t + s)$ it is obvious that $\neg\big((t + s \xrightarrow{\sigma} u) \leq (s \rightsquigarrow v)\big)$. Therefore, $S(s \xrightarrow{\sigma} v) < S(t + s \xrightarrow{\sigma} u)$;

R34. Since $M(t) = M(\overline{\boldsymbol{\sigma}}(t))$ and $n_{\overline{\boldsymbol{\sigma}}}(p) < n_{\overline{\boldsymbol{\sigma}}}(\overline{\boldsymbol{\sigma}}(p))$ follows that $(\boldsymbol{D}(t)) \leq (\overline{\boldsymbol{\sigma}}(t) \rightsquigarrow \breve{\underline{\delta}})$ but $\neg\big((\overline{\boldsymbol{\sigma}}(t) \rightsquigarrow \breve{\underline{\delta}}) \leq (\boldsymbol{D}(t))\big)$. Therefore, $S((\boldsymbol{D}(t))) < S(\overline{\boldsymbol{\sigma}}(t) \rightsquigarrow \breve{\underline{\delta}})$.

□

By Lemma 2.3.16 we conclude that:

Lemma 5.5.36. $Red^{\alpha+1}((\mathbf{T}_{pACP^+_{drt}})$ contains only rules with positive premises and $\longrightarrow_{Red^1(\mathbf{T}_{pACP^+_{drt}})}$ is associated with $\mathbf{T}_{pACP^+_{drt}}$. □

In other words the lemma says that the deduction system of $pACP^+_{drt}$ is meaningful since the relation that the system defines exists and it is unique. Furthermore, by Theorem 2.3.17 using the result in Lemma 5.5.36 we obtain:

Lemma 5.5.37. $\mathbf{T}_{pACP^+_{drt}}$ is an operational conservative extension of $\mathbf{T}_{pBPA_{drt}}$. □

From this point we follows the same steps as in Section 4.3.1.

Lemma 5.5.38. The term-deduction system $\mathbf{T}_{pACP^+_{drt}}$ is an operationally conservative extension up to the probabilistic bisimulation of the term-deduction system $\mathbf{T}_{pBPA_{drt}}$.

Proof. The conclusion is obtained from Lemma 5.5.37 in the same way as the conclusion of Lemma 4.3.20 is derived from Lemma 4.3.19. □

Lemma 5.5.39. (Conservativity of $pACP^+_{drt}$ with respect to $pBPA_{drt}$) $pACP^+_{drt}$ is an equationally conservative extension of $pBPA_{drt}$, that is, if t and s are closed $pBPA_{drt}$ terms, then $pBPA_{drt} \vdash t = s \Leftrightarrow pACP^+_{drt} \vdash t = s$.

Proof. According to the used method we need to verify that:

- $\mathbf{T}_{pACP^+_{drt}}$ is an operationally conservative extension of $\mathbf{T}_{pBPA_{drt}}$ up to probabilistic bisimulation (see Lemma 5.5.38);
- $pBPA_{drt}$ is a complete axiomatization with respect to the bisimulation model (see Theorem 5.3.36);
- $\mathbf{T}_{pACP^+_{drt}}$ with respect to the probabilistic bisimulation equivalence induces a model of $pACP^+_{drt}$ (see Theorem 5.5.28).

□

And finally we conclude that:

Theorem 5.5.40 (*Completeness theorem for* $pACP^+_{drt}$). If t and s are closed $pACP^+_{drt}$ terms, then $\mathcal{M}_{pACP^+_{drt}} \vdash t \leftrightarrows s \Rightarrow pACP^+_{drt} \vdash t = s$.

Proof. Completeness follows immediately from the following results:

- $pACP^+_{drt}$ has the elimination property for $pBPA_{drt}$ (see Theorem 5.4.6);
- $pACP^+_{drt}$ is an equationally conservative extension of $pBPA$ (see Lemma 5.5.39).

□

Chapter 6

Abstraction

6.1 Introduction

In this chapter, we turn our attention to the problem of verification of probabilistic systems. Informally, the procedure of verification of concurrent systems in a process algebraic framework covers the following steps: 1. model the desired behaviour of the system including certain requirements (specification S); 2. model the system behaviour (implementation I); 3. transform the implementation by use of hiding the internal activities, fairness assumption, encapsulation and other feasible methods and check if it meets the specification from the previous phase. The first two phases reduce to the concept of specification of the system behaviour, the main subject of the previous chapters of this thesis. The third problem has always been of large interest and has triggered a lot of attention in the field of formal methods. Translated into the (process) algebra language it means that certain operators need to be defined together with a set of axioms or conditional axioms that help to derive equality between specification S and some transformation of the implementation I' ($PA \vdash S = I'$). Semantically, an appropriate equivalence relation should be defined that relates desired processes and corresponds to "$=$" in the axiomatization. Fortunately, these questions are satisfactorily answered in the area of (non-deterministic non-probabilistic) concurrent systems, just a couple of examples: [37, 105, 13] and many models have been proposed as results of a long history of research, particularly on different equivalence relations (weak, branching, semi-branching, 2/3 nested bisimulation, η bisimulation, delay bisimulation, normed simulation, trace equivalence) [89, 59, 90, 21, 63, 27, 57, 61]. Since probabilistic systems appear as an extension of non-deterministic systems, the attempt to treat the problem of verification of probabilistic systems following the line of verification techniques for the non-probabilistic case becomes very natural. Several equivalence relations that abstract away from internal steps in probabilistic systems with the origins in the existing equivalence relations for non-probabilistic case have been proposed [80, 29, 100, 95, 30, 103]. Of course, they have to be enriched by a mechanism that captures probabilistic behaviour, as this was the case with the probabilistic variant of strong bisimulation in Definition 3.3.11. Thus, besides that two related processes mimic each other on observable actions they can perform, basically they are required to have the same probabilities of reaching a certain set of processes. These definitions (except [80] that we discuss later) have the following in common: all sub-processes reachable from the original processes have to be investigated, checked w.r.t. their reachability probabilities and related on a basis of the obtained information.

We go beyond this restriction and start from a weaker assumption: not all sub-processes have to be taken into account and checked as to their probabilities. Put differently, for given processes that should be decided whether they are related or not, we propose a criterion by which a set of sub-processes is selected and probabilities are investigated only on the elements of this set. For the rest

of the sub-processes only their branching structure is investigated but not the probability measure. The definition we present here is based on branching bisimulation and the criterion mentioned is defined only for fully probabilistic processes. The proposed equivalence relation on fully probabilistic systems basically is a weaker variant of the probabilistic equivalence relation defined in [29]. We will justify our notion of equivalence by means of a couple of examples. Although we did not investigate it, we believe that a similar criterion can be established on the other probabilistic equivalence relations as the ones in [100, 95].

In the sequel we shortly present the basic concept of abstraction as mainly taken in process algebras *BPA* and *ACP* and the concept of branching bisimulation. Later we will present an axiomatization of probabilistic process algebra with abstraction together with a set of verification rules that are added to model the fairness assumption. A larger part of the chapter covers the definition of the probabilistic branching bisimulation and the preparatory steps towards its introduction as well as results concerning the compositional aspects of this relation. Finally, we show that this equivalence relation is decidable for regular processes (processes with finitely many sub-processes) and present an algorithm that decides whether two given probabilistic systems are equivalent.

6.2 Abstraction in non-probabilistic process algebra

The issue of abstraction in *BPA* (*ACP*) is brought in by the constant τ and the unary operator τ_I for $I \subseteq A$. The τ action means an internal activity of one process; an observer cannot "see" the silent τ action. We write A_τ for $A \cup \{\tau\}$. The abstraction operator τ_I

is a renaming operator that renames all actions from I into τ. The set I contains all actions that we want to abstract from. Informally, all actions that can be performed by components of the system and are "invisible" for the outside world (environment) are contained in the set I. On the contrary, the actions from $A \setminus I$ are considered observable, external and visible to the outside world. The laws for the τ constant are given in Table 6.1 and the axioms for the τ_I operator are shown in Table 6.2.

$x \cdot \tau$	$=$	x	$B1$
$x \cdot (\tau \cdot (y + z) + y)$	$=$	$x \cdot (y + z)$	$B2$

Table 6.1: $\tau-$axioms.

$\tau_I(a)$	$=$	a	$(a \notin I)$	$TI1$
$\tau_I(a)$	$=$	τ	$(a \in I)$	$TI2$
$\tau_I(x + y)$	$=$	$\tau_I(x) + \tau_I(y)$		$TI3$
$\tau_I(x \cdot y)$	$=$	$\tau_I(x) \cdot \tau_I(y)$		$TI4$

Table 6.2: Axioms for the abstraction operator.

In order to prove the correctness of a given specification of one concurrent system fairness assumptions about the resolution of the non-deterministic choices are necessary. Algebraically such fairness assumption is described through the use of Koomen's Fairness Abstraction Rules (KFAR) (e.g. [36, 13]). The KFARs express exactly the idea that, due to some fairness mechanism, abstraction from internal steps will yield an external step after finitely many repetitions. In Table 6.3 the formulation of the rule $KFAR_n^b$ is shown, where the parameter $n \geq 1$ indicates the length of an internal cycle and the superscript b indicates that this variant of $KFAR$ holds in case of branching bisimulation.

$$
\begin{array}{lcl}
X_1 & = & i_1 \cdot X_2 + Y_1 \\
X_2 & = & i_2 \cdot X_3 + Y_2 \\
\ldots & & \\
\ldots & & \\
X_{n-1} & = & i_{n-1} \cdot X_n + Y_{n-1} \\
X_n & = & i_n \cdot X_1 + Y_n, \\
 & & I \cup \{\tau\} \supseteq \{i_1, i_2, \ldots, i_n\} \neq \{\tau\}
\end{array}
$$

$$\tau \cdot \tau_I(X_1) = \tau \cdot (\tau_I(Y_1) + \tau_I(Y_2) + \ldots + \tau_I(Y_{n-1}) + \tau_I(Y_n))$$

Table 6.3: Fairness rules $KFAR^b_n, n \geq 1, I \subseteq A$.

6.2.1 Branching bisimulation on process graphs

Different equivalence relations that abstract away internal steps have been defined, among which branching and weak bisimulation are most popular. (Strong bisimulation does not treat internal actions differently than any other action.) Here we present so-called *branching bisimulation* introduced in ([59]) because it is tightly related to the relation on probabilistic systems introduced later. (See also [58] where the author discusses the reasons why branching bisimulation is preferable over weak bisimulation.) When working with abstraction and branching bisimulation we prefer a process graph model rather than the term model used in the previous chapters. In our opinion the definition and presentation particularly on terminating processes is technically more clear here than in the term model. (See [53] for a term model of ACP_τ.)

Definition 6.2.1. A *process graph* g is a triple $(S, \rightarrow, root)$ consisting of:
- a set of states S with a designated termination state NIL,
- $root \in S$,
- a relation $\rightarrow \subseteq S \times A_\tau \times S$.

For technical reasons we do not distinguish between successful and unsuccessful termination as it is common for ACP. We only have one termination state denoted NIL.

Definition 6.2.2. Let g and h be process graphs and R be a symmetric relation between states of g and h. R is a *branching bisimulation* between g and h if:

1. the roots of g and h are related by R;
2. if $s \xrightarrow{a} s'$ for $a \in A_\tau$ and $(s,t) \in R$ then either:
   2.1 $a \equiv \tau$ and $(s',t) \in R$ or
   2.2 there exists a path $t \xRightarrow{\tau^*} t_1 \xrightarrow{a} t'$, such that $(s,t_1) \in R$ and $(s',t') \in R$;

Moreover, if

3. if $root(g) \xrightarrow{a} s'$ for $a \in A_\tau$, then there is t' with $root(h) \xrightarrow{a} t'$ and $(s',t') \in R$;
4. if $root(h) \xrightarrow{a} t'$ for $a \in A_\tau$, then there is s' with $root(g) \xrightarrow{a} s'$ and $(t',s') \in R$,

then R is called a *rooted branching bisimulation* between g and h. Constraints 3 and 4 are known as the root condition.

g and h are (*rooted*) *branching bisimilar*, $g \leftrightarrow_b h$ ($g \leftrightarrow_{rb} h$) if there exists a (rooted) branching bisimulation R that relates $root(g)$ and $root(h)$.

The main characteristic of the branching bisimulation is stated in 2.2. It says that an action transition $\xrightarrow{a}$ in g can be mimicked by action transition $\xrightarrow{a}$ in h preceded by a sequence of τ transitions that do not leave the current equivalence class. Axiom $B2$ in Table 6.1 expresses the same strategy. In the case of weak bisimulation there is no constraint on intermediate states before and after performing the observable action transition.

The purpose of the root condition and the rooted branching bisimulation is to achieve a congruence relation and therefore compositional semantics, because branching bisimulation is not preserved by the alternative composition operator. For the details about the axiomatization and construction of the model of *BPA*$_\tau$ and *ACP*$_\tau$ see [27, 53, 13].

6.3 Probabilities, abstraction and fairness

In the previous section we argued that for verification of certain properties of concurrent systems the fairness assumption about non-deterministic choice is essential. Otherwise many properties simply cannot be established. In the presence of probabilities, a fairness assumption for probabilistic choice is superfluous as it is implicitly expressed by assigning non-zero probabilities to every alternative in the probabilistic choice. For comparison, the assumption that the internal action τ cannot be executed infinitely many times if it is an alternative in a non-deterministic choice, in the probabilistic setting corresponds to the fact that every infinite sequence of τ actions has probability 0 (in case of a process with finitely many states).

Our aim now is to formulate algebraic rules (we will call them probabilistic verification rules) that exactly capture the idea of "zero probability for infinite τ sequences". The probabilistic verification rules for fully probabilistic process algebra that will be presented here arise rather in a natural way from the ones defined in standard process algebra (KFARs). These rules express the idea that due to a non-zero probability for a system to execute an external action, abstraction from internal steps will yield the external step(s) with probability 1 after finitely many repetitions. Moreover, they also determine the probability distribution over the external activities that may occur after the internal cycle (or a sequence of finitely many τ steps) is left.

We illustrate our ideas by the following motivating examples.

Example 6.3.1. An experimenter has one fair die D. He rolls it and if the outcome is one he rolls it again. If the outcome is an even number he announces "head" and if the outcome is $three$ or $five$ he announces "tail". In both cases the experiment finishes. The experiment - process can be specified by the following recursive specification:

$$D = one \cdot D \uplus_{1/6} (two \uplus_{1/3} four \uplus_{1/3} six) \cdot sayhead \uplus_{1/2} (three \uplus_{1/2} five) \cdot saytail$$

where $sayhead$ and $saytail$ are atomic actions expressing the observable events of announcing "head" and "tail", respectively. Note that the observer is not aware of the actions: one, two, $three$, $four$, $five$ and six, and so these actions are internal and will be renamed into τ. Clearly, the observer (sitting outside the room) eventually will hear either "head" or "tail", since the probability that the outcome is one infinitely many times equals 0. In Figure 6.1a. we have drawn a transition system

(informally presented) which corresponds to the specification of the experiment. Figure 6.1b. shows the behaviour of the observer, where the $?_1$ and $?_2$ labels on the edges express the probabilities that should be determined. □

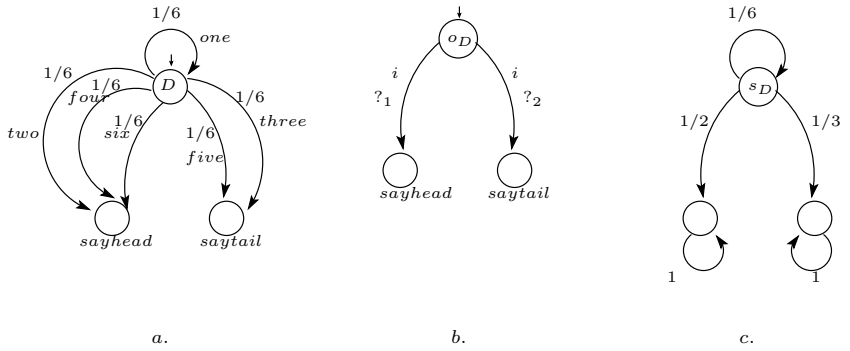


Figure 6.1: Experiment with one die - a. from the perspective of the experimenter; b. from the perspective of the observer; c. the underlying Markov chain.

Example 6.3.2. In a different "black room" another experiment is performed. An experimenter has two coins A and B. A is a fair coin with the probability distribution $\{1/2\ head, 1/2\ tail\}$, and B is biased with distribution $\{1/3\ head, 2/3\ tail\}$. First he throws coin A. If $head$ turns up the throwing is over and he announces "head". If $tail$ shows up then he throws coin B. If $tail$ turns up then the throwing is over and he announces "tail", but if $head$ turns up then he takes coin A and performs the experiment again. This experiment - process can be specified by the following recursive specification:

$$A = tail_A \cdot B \leftthreetimes_{1/2} head_A \cdot sayhead$$
$$B = head_B \cdot A \leftthreetimes_{1/3} tail_B \cdot saytail$$

where $sayhead$ and $saytail$ are atomic actions expressing the observable events of announcing "head" and "tail", respectively. Again we set unobservable actions which are $tail_A$, $head_A$, $tail_B$ and $head_B$. The probability to have infinitely many times tail on the first coin followed by head on the second coin equals 0 as well. Figure 6.2a. shows (informally) the behaviour of the experimenter and Figure 6.2b. shows the behaviour of the observer. □

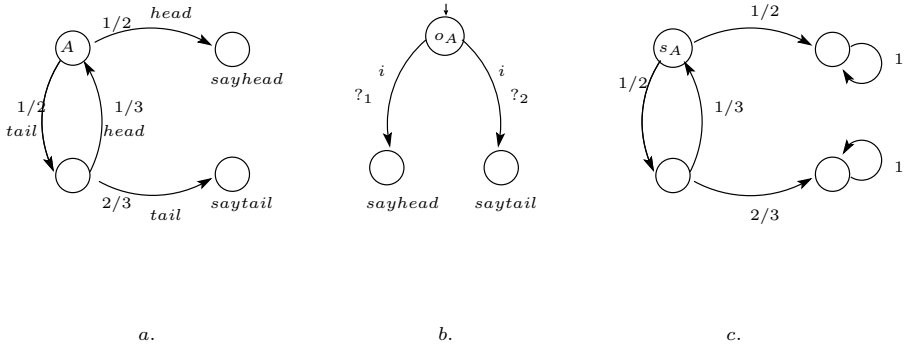


Figure 6.2: Experiment with two coins - a. from the perspective of the experimenter; b. from the perspective of the observer; c. the underlying Markov chain.

Clearly, in both experiments the probability to hear either "head" or "tail" equals 1. Our main aim now is to find probabilities $?_1$ and $?_2$, and to establish a method that formally gives an answer to the question: "With what probability the observer hears "head" (respectively "tail")?". In the case of the first experiment, [29] gives the answer to this question as: the probability of "head" is $3/5(=\frac{3\times 1/3}{1-1/6})$ and the probability of "tail" is $2/5(=\frac{3\times 1/3}{1-1/6})$. This corresponds exactly to the absorption probabilities for the discrete time Markov chain ([99]) given in Figure 6.1c. Using the syntax of our process algebra, this relation of the two processes can be easily expressed by the following rule: if $X = a \leftthreetimes_\pi b \leftthreetimes_\rho i \cdot X$ (where i is an internal action), then $\tau \cdot \tau_{\{i\}}(X) = \tau \cdot (a \leftthreetimes_{\pi/(\pi+\rho)} b)$. The resemblance with the $KFAR_1^b$ rule (Table 6.3) is obvious.

The second example presents a situation in which the method proposed in [29] cannot abstract away the internal cycle. But working with recursive equations in our process algebra we can introduce a probabilistic rule which is a counterpart of $KFAR_2^b$. So, the rule has the following form:

$$\frac{\begin{array}{l} X_1 = i \cdot X_2 \leftthreetimes_\pi Y_1 \\ X_2 = i \cdot X_1 \leftthreetimes_\rho Y_2,\ I = \{i\} \end{array}}{\tau \cdot \tau_I(X_1) = \tau \cdot (\tau_I(Y_1) \leftthreetimes_\alpha \tau_I(Y_2))} \qquad (PVR_2)$$

where X_1 is the root variable and $\alpha = \frac{1-\pi}{1-\pi\rho}$. The values of probabilities α and $\beta = 1 - \alpha = \frac{\pi(1-\rho)}{1-\pi\rho}$ are obtained as the absorption probabilities of the corresponding Markov chain when X_1 is the root variable, that is, X_1 is the initial state of the system. We point out that the absorption probabilities for this system differ for various initial distributions.

Back to the examples, we can easily calculate that in the both cases the probability for "head" is $3/5(=?_1)$ and the probability for "tail" is $2/5(=?_2)$, which are the absorption probabilities for Markov chains in Figure 6.1c. and 6.2c. for the relevant states, of course taking into account that the second experiment starts by flipping the coin A. To conclude, the processes in Figure 6.1a, 6.1b, 6.2a and 6.2b we consider equivalent after abstraction.

6.3.1 Process algebra - axiomatization

A formal definition of the axiomatization and a general form of the probabilistic verification rules are given below. The underlying process algebra is *fpBPA* introduced in Section 3.2.1. We choose to work with fully probabilistic process algebra. The presence of both choices (probabilistic and non-deterministic) and abstraction at the same time leads to a set of complex algebraic equalities. However, we figure out that it is still syntactically feasible, but unfortunately it is much more difficult to find a model for the equialities; we worked out some rules that resolve certain forms of non-deterministic choice in probabilistic systems, but the corresponding equivalence relation (for compositional semantics) is far from trivial. As a consequence, due to the absence of non-determinism the interleaving parallel composition as treated in Chapter 4 cannot be incorporated in this axiomatization. On the other hand, some version of *synchronous* parallel composition may be considered in such a process algebra (see [17]).

The signature of *fpBPA* (Section 3.2.1) is extended by the new constant τ and the abstraction operator τ_I for $I \subseteq A$. The new algebra will be denoted by *fpBPA*$_\tau$. The set of axioms of *fpBPA*$_\tau$ consists of the axioms of *fpBPA* in Table 3.1 and the axioms for the new operators given in Table 6.4.

Besides, we define a set of probabilistic verification rules PVR_n for $n \geq 1$ as given below:

$$\frac{X_1 = i \cdot X_1 \leftthreetimes_{\pi_1} Y_1, \tau \neq i \in I}{\tau \cdot \tau_I(X_1) = \tau \cdot \tau_I(Y_1)} \qquad (PVR_1)$$

$x \cdot \tau$	=	x		$T1$
$\tau_I(\tau)$	=	τ		$TI0$
$\tau_I(a)$	=	a	if $a \notin I$	$TI1$
$\tau_I(a)$	=	τ	if $a \in I$	$TI2$
$\tau_I(x \cdot y)$	=	$\tau_I(x) \cdot \tau_I(y)$		$TI4$
$\tau_I(x \leftthreetimes_\pi y)$	=	$\tau_I(x) \leftthreetimes_\pi \tau_I(y)$		$PrTI$

Table 6.4: Axioms for the abstraction operator ($I \subseteq A_\tau$).

$$\begin{array}{l} X_1 = i_1 \cdot X_2 \leftthreetimes_{\pi_1} Y_1 \\ X_2 = i_2 \cdot X_3 \leftthreetimes_{\pi_2} Y_2 \\ . \\ . \\ X_{n-1} = i_{n-1} \cdot X_n \leftthreetimes_{\pi_{n-1}} Y_{n-1} \\ X_n = i_n \cdot X_1 \leftthreetimes_{\pi_n} Y_n, I \cup \{\tau\} \supseteq \{i_1, i_2, \ldots, i_n\} \neq \{\tau\} \end{array} \quad (PVR_n)$$

$$\tau \cdot \tau_I(X_1) = \tau \cdot (\tau_I(Y_1) \leftthreetimes_{\alpha_1} \tau_I(Y_2) \leftthreetimes_{\alpha_2} \ldots \leftthreetimes_{\alpha_{n-2}} \tau_I(Y_{n-1}) \leftthreetimes_{\alpha_{n-1}} \tau_I(Y_n))$$

where $\alpha_1 = \frac{1-\pi_1}{1-\pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_n}$, $\alpha_j = \frac{\pi_1 \cdot \ldots \cdot \pi_{j-1} \cdot (1-\pi_j)}{1-\pi_1 \cdot \ldots \cdot \pi_n}$ for $j : 1 < j \leq n$ and $\pi_k \in \langle 0, 1 \rangle$ for $k : 1 \leq k \leq n$. If we refer to *fpBPA*$_\tau$ extended with these rules we write *fpBPA*$_\tau + PVR_1 + PVR_2 + \ldots$.

Special instantiations of PVR_2 are obtained when Y_1 or Y_2 do not occur. Then

$$\begin{array}{l} X_1 = i_1 \cdot X_2 \\ X_2 = i_2 \cdot X_1 \leftthreetimes_{\pi_2} Y_2 \\ I \cup \{\tau\} \supseteq \{i_1, i_2\} \neq \{\tau\} \end{array} \quad (PVR1_2)$$

$$\tau \cdot \tau_I(X_1) = \tau \cdot \tau_I(Y_2)$$

and

$$\begin{array}{l} X_1 = i_1 \cdot X_2 \leftthreetimes_{\pi_1} Y_1 \\ X_2 = i_2 \cdot X_1 \\ I \cup \{\tau\} \supseteq \{i_1, i_2\} \neq \{\tau\} \end{array} \quad (PVR2_2)$$

$$\tau \cdot \tau_I(X_1) = \tau \cdot \tau_I(Y_1)$$

These rules will be applied in Section 7.2.

General probabilistic verification rule

Besides the fairness rules $KFAR_n^b$ in *ACP*$_\tau$ (*ACP* with abstraction) a more general rule, called Cluster Fair Abstraction Rule ($CFAR^{(b)}$) [105, 27] that abstracts away sequences of internal actions has been defined. It is based on the notion of a cluster, a set of processes that can reach each other through sequences of τ transitions. In the probabilistic setting we can also be more general but only if we can keep track of the probabilities with which processes in the cluster can reach each other.

Here informally we propose a rule that can abstract away τ actions(loops) in a more general way than the rules introduced earlier. By a cluster we mean a set of states that can be reached one from each other through τ sequences with a positive probability. The cluster in the presence of probabilities can be expressed by a recursive specification. As a piece of additional notation, we use 0 and 1 as valid parameters of the probabilistic choice operator, which was not the case till now.

Thus, if we write $x \leftthreetimes_0 y$ it means that x can occur with probability 0, while y is assigned probability 1. Note that we do not claim that the permission of $\leftthreetimes_0$ and $\leftthreetimes_1$ does not affect the axiomatization of *pBPA*. Contrary, we will need additional axioms to relate added terms, for instance $x \leftthreetimes_0 y$ and y. However, for our needs at this point we will think that in a given finite set of processes a process i is assigned a zero probability in the equation of process j if j cannot make an internal transition to i with a positive probability. For a fixed $n \in I\!N$ the General Probabilistic Verification Rule $GPVR_n$ is defined as:

$$\begin{array}{l}
X_1 = i_{11} \cdot X_1 \leftthreetimes_{\pi_{11}} i_{12} \cdot X_2 \leftthreetimes_{\pi_{12}} \ldots i_{1n} \cdot X_n \leftthreetimes_{\pi_{1n}} Y_1 \\
X_2 = i_{21} \cdot X_1 \leftthreetimes_{\pi_{21}} i_{22} \cdot X_2 \leftthreetimes_{\pi_{22}} \ldots i_{2n} \cdot X_n \leftthreetimes_{\pi_{2n}} Y_2 \\
. \\
. \\
X_{n-1} = i_{n-11} \cdot X_1 \leftthreetimes_{\pi_{n-11}} i_{n-11} \cdot X_2 \leftthreetimes_{\pi_{n-12}} \ldots i_{n-1n} \cdot X_n \leftthreetimes_{\pi_{n-1n}} Y_{n-1} \\
X_n = i_{n1} \cdot X_1 \leftthreetimes_{\pi_{n1}} i_{n1} \cdot X_2 \leftthreetimes_{\pi_{n2}} \ldots i_{nn} \cdot X_n \leftthreetimes_{\pi_{nn}} Y_n \\
I \cup \{\tau\} \supseteq \{i_{11}, i_{12}, \ldots, i_{nn}\} \neq \{\tau\}
\end{array} \qquad (GPVR_n)$$

$$\tau \cdot \tau_I(X_1) = \tau \cdot (\tau_I(Y_1) \leftthreetimes_{\alpha_1} \tau_I(Y_2) \leftthreetimes_{\alpha_2} \ldots \leftthreetimes_{\alpha_{n-2}} \tau_I(Y_{n-1}) \leftthreetimes_{\alpha_{n-1}} \tau_I(Y_n))$$

where,

- $\pi_{ij} \in [0,1]$ such that $\sum_{j=1}^{n} \pi_{ij} \leq 1$ for all $i : 1 \leq i \leq n$;
- α_i for $1 \leq i \leq n$ is determined by the smallest solution of the system of linear equations:

$$\begin{aligned}
u_i &= 1 - \sum_{k=1}^{n} \pi_{ik} + \sum_{j=1}^{n} \pi_{ij} \cdot u_j \\
u_j &= \sum_{k=1}^{n} \pi_{jk} \cdot u_k \qquad\qquad \text{for } 1 \leq j \leq n,\ j \neq i
\end{aligned}$$

by taking $\alpha_i = u_1$ if $1 - \sum_{k=1}^{n} \pi_{ik} \neq 0$, otherwise $\alpha_i = 0$. If $Y_j = Y_i$ for some $j : 1 \leq j \leq n$, $j \neq i$, then the equation corresponding to the variable u_j should be replaced by the following equation:

$$u_j = 1 - \sum_{k=1}^{n} \pi_{jk} + \sum_{k=1}^{n} \pi_{jk} \cdot u_k \quad \text{for } j \neq i \text{ and } Y_j = Y_i$$

For this system of linear equations, the solution for u_i gives the probability to get absorbed in the state that corresponds to Y_i when the initial state is the one corresponding to X_i. This probability is obtain as the sum of two probabilities: the first summand $1 - \sum_{k=1}^{n} \pi_{ik}$ gives the probability to reach the state corresponding to Y_i from the state of X_i in one step; the second summand $\pi_{ij} \cdot u_j$ gives the probability that the state X_j is reached from X_i in one step multiplied by the probability to get absorbed in Y_i if the initial state is the one corresponding to Y_j. $Y_i = Y_j$ for some $j : 1 \leq j \leq n$, $j \neq i$ means that the state corresponding to Y_i can be reached from X_j in one step. For that reason, the summand $1 - \sum_{k=1}^{n} \pi_{jk}$ appears in the equation of u_j in the case $Y_i = Y_j$.

Probabilities α_i are obtained as absorption probabilities of the discrete time Markov chain generated by the recursive specification. α_i gives the probability to get absorbed in the state corresponding to Y_i when the initial state corresponds to X_1. The linear system of equations considered here can be

found in [79, 85]. The condition $1 - \sum_{k=1}^{n} \pi_{1k} \neq 0$ asserts that Y_i is reachable from X_i with a positive probability. Otherwise, the probability to reach Y_i is 0. It is not difficult to check that PVR_n^b is an instantiation of $GPVR_n^b$.

Recursion

The main goal in this chapter is to develop a strategy to eliminate (reduce) possibly infinite τ-sequences. Inevitably, it brings back the need of introducing the concept of recursion and recursive specification and the notions related to them. Related to this, many questions and problems arise by introducing the τ constant and τ_I operator. For instance, in the literature treating this problem (see e.g. [27, 13]) we can find examples showing that τ cannot be taken as a guard when one considers guarded recursion. Moreover, allowing the τ_I operator in recursive specifications complicates and even makes the formulation of guardedness for recursion impossible. Here we resort to the common approach: no recursive specifications containing the τ_I operator is considered. The notion of guardedness, guarded terms and guarded specification remain the same as in *fpBPA*. The formal definitions can be easily obtained from the definitions given in Section 3.2.4 by adapting them for the syntax of *fpBPA* ($+$ and Π_n operators should be excluded). Thus, a guard can be only a constant from A, but not τ.

After we define the equivalence relation and construct the model of *fpBPA* with recursion, no other properties of the model concerning projection and recursion (including recursive principles) will be investigated. We believe that by following the strategy used in [27], where AIP$^-$ and RSP for *BPA*$^\tau$ have been proved, and the one used to prove the validity of RSP in *pBPA* in Section 3.3.2, we can also prove RSP to be valid in *fpBPA*$_\tau$.

6.4 Model - fully probabilistic process graphs

The next question that will be discussed is to give a semantical meaning of the equalities in *fpBPA*$_\tau$ + PVR_1 + PVR_2 ... . In other words, to define a model for the set of axioms. First of all, the elements of the model domain should be defined and then an equivalence relation between them (similar to the pattern for the term model described on page 46). As already mentioned, we rather work with the process graph model than with the term model[1]. Thus, the elements of the domain are probabilistic variant of process graph, that is, process graphs supplied with a mechanism to capture probabilities. Every probabilistic process graph (also called probabilistic labelled transition systems) has two types of states (nodes): probabilistic and action (they correspond to static and dynamic process terms from the previous chapters) and two types of edges (transitions): probabilistic and action transitions. An action transition may have the termination state, denoted NIL as its incoming state. But NIL is not a process itself. To stay compatible with the notation used earlier, probabilistic edges will be presented by $\rightsquigarrow$ and action edges by $\stackrel{a}{\rightarrow}$. By allowing at most one action transition to leave an action state we obtain a model of fully probabilistic processes.

Definition 6.4.1. Let A be a countable set of atomic actions. A *fully probabilistic graph* g is a tuple

[1] In a model based on term-deduction system we find it rather difficult to express terminating and related processes in probabilistic setting if the constant for successful termination ε [27] is not included. In [53] the author introduces a new process $\surd \downarrow$. Working with the alternating model for probabilistic systems we find it rather counterintuitive and technically difficult to have such a process. Namely, it can neither be classified as a static nor as a dynamic process term.

$(S_p \cup S_n \cup \{NIL\}, \rightsquigarrow, \rightarrow, \mu, root)$ consisting of:
– a countable set S_p of probabilistic states,
– a countable set S_n of action states such that $S_p \cap S_n = \emptyset$ and $NIL \notin S_p \cup S_n$,
– $root \in S_p$,
– a relation $\rightsquigarrow \subseteq S_p \times S_n$,
– a function $\rightarrow$: $S_n \rightarrow (S_p \cup \{NIL\}) \times A_\tau$, and
– a partial function $\mu : S_p \times S_n \mapsto \langle 0, 1]$ such that $\mu(p, n)$ is defined iff $(p, n) \in \rightsquigarrow$ for $(p, n) \in S_p \times S_n$ and $\sum_{n \in S_n} \mu(p, n) = 1$ for any $p \in S_p$.

We denote $S = S_p \cup S_n$. If S is a finite set then we say that the probabilistic graph g is finite. NIL is called *the termination state*. If NIL is not reachable from the root of g then it can be ignored. Function μ is called *the probability distribution function* of g.

If $(p, n) \in \rightsquigarrow$, we write $p \rightsquigarrow n$. If $\rightarrow (n) = (p, a)$ we write $n \xrightarrow{a} p$. For sake of simplicity, instead of writing the value of function μ separately, if $p \rightsquigarrow n$ we write $p \overset{\mu(p,n)}{\rightsquigarrow} n$. By $\mathbf{G}$ we denote the set of all finite fully probabilistic graphs.

If $\rightarrow$ is not a function from S_n to $(S_p \cup \{NIL\}) \times A_\tau$, but a subset of $S_n \times (S_p \cup \{NIL\}) \times A_\tau$, we get the general class of probabilistic graphs for probabilistic processes that allow non-determinism, also called labelled concurrent transition systems or labelled concurrent Markov chains. In this case, action nodes are rather called *non-deterministic states*.

Obviously, for fully probabilistic process graphs it is not necessary to separate probabilistic from action transitions, they can be merged into one transition with two labels. In any case, here we follow the line of the alternating model for probabilistic systems from the previous chapters, but also we leave room for a possible extension of the definitions given in the remainder of this section with non-determinism.

The operators of *fpBPA*$_\tau$ are interpreted on $\mathbf{G}$ as shown below (cf. Definition 6.4.5). One can notice that the interpretation of the sequential composition and the abstraction operator are similar to the interpretation of the same operator in *BPA* ([27]). In order to define the probabilistic choice operator on the set of probabilistic process graphs we resort to the same method used for the alternative composition for *BPA* which requires the notion of unwinding. If probabilistic choice is applied on unwound probabilistic process graphs, the obtained result is misleading (see example 6.4.6).

Definition 6.4.2. Let $g = (S \cup \{NIL\}, \rightsquigarrow, \rightarrow, \mu, root)$ be a fully probabilistic graph. We say that g is *root acyclic* if there is no node $n \in S_n$ and $a \in A_\tau$ such that $n \xrightarrow{a} root$. Otherwise we say that g is root cyclic.
We define the root unwinding map $\rho : \mathbf{G} \rightarrow \mathbf{G}$ as follows:
• if g is root acyclic, then $\rho(g) = g$;
• if g is root cyclic, then $\rho(g) = (S \cup \{NIL\} \cup \{newroot\}, \rightsquigarrow', \rightarrow, \mu', newroot)$,
where
- $newroot$ is a new node, $newroot \notin S$ and $newroot$ is a probabilistic state,
- $\rightsquigarrow' = \rightsquigarrow \cup \{(newroot, n) \ : \ root \rightsquigarrow n\}$ and
- $\mu'(p, n) = \begin{cases} \mu(p, n) & \text{if } p \in S \\ \mu(root, n) & \text{if } p = newroot. \end{cases}$

We can easily prove the following result.

Proposition 6.4.3. Let g be a fully probabilistic graph.

i. Then $\rho(g)$ is root acyclic.
ii. $g \leftrightarrows \rho(g)$, that is, g and $\rho(g)$ are strongly bisimilar. □

Definition 6.4.4. (Interpretation of the constants) If $a \in A_\tau$, its interpretation is
$[a] = (\{s_p\} \cup \{s_n\} \cup \{NIL\}, \{s_p \rightsquigarrow s_n\}, \{s_n \xrightarrow{a} NIL\}, \mu(s_p, s_n) = 1, s_p)$.

Definition 6.4.5. (Interpretation of the operators)
Sequential composition Let g and h be graphs in **G** and
$g = (S_g \cup \{NIL_g\}, \rightsquigarrow_g, \rightarrow_g, \mu_g, root_g)$ and $h = (S_h \cup \{NIL_h\}, \rightsquigarrow_h, \rightarrow_h, \mu_h, root_h)$. $g \cdot h$ is defined as:

$$(S_g \cup S_h \cup \{NIL_h\}, \rightsquigarrow_g \cup \rightsquigarrow_h, \rightarrow, \mu, root_g),$$

where: $\rightarrow = (\rightarrow_g \setminus \{n \xrightarrow{a} NIL_g \ : \ n \in S_g, a \in Act_\tau\}) \cup \rightarrow_h$
$\cup \ \{n \xrightarrow{a} root_h \ : \ n \in S_g, a \in Act_\tau, n \xrightarrow{a} NIL_g\}$,

and $\mu(p,n) = \begin{cases} \mu_g(p,n) & \text{if } p,n \in S_g \\ \mu_h(p,n) & \text{if } p,n \in S_h; \end{cases}$

Probabilistic choice Let g and h be graphs in **G** and
$\rho(g) = (S_g \cup \{NIL_g\}, \rightsquigarrow_g, \rightarrow_g, \mu_g, root_g)$ and $\rho(h) = (S_h \cup \{NIL_h\}, \rightsquigarrow_h, \rightarrow_h, \mu_h, root_h)$.
$g \boxplus_\pi h$, for $\pi \in \langle 0, 1 \rangle$, is defined as:

$$(S \cup \{NIL\}, \rightsquigarrow, \rightarrow, \mu, root),$$

where: $S = (S_g \setminus \{root_g\}) \ \cup \ (S_h \setminus \{root_h\}) \ \cup \ \{root\}$, $root \notin S_g \cup S_h$,
$\rightsquigarrow = (\rightsquigarrow_g \setminus \{root_g \rightsquigarrow n \ : \ n \in S_g\}) \cup (\rightsquigarrow_h \setminus \{root_h \rightsquigarrow n \ : \ n \in S_h\})$
$\cup \{root \rightsquigarrow n \ : \ n \in S_g, root_g \rightsquigarrow n\} \cup \{root \rightsquigarrow n \ : \ n \in S_h, root_h \rightsquigarrow n\}$,
$\rightarrow = \rightarrow_g \ \cup \ \rightarrow_h$ with the remark that NIL_g and NIL_h are identified and this node is named NIL,

and $\mu(p,n) = \begin{cases} \mu_g(p,n) & \text{if } p,n \in S_g \setminus \{root_g\} \\ \mu_h(p,n) & \text{if } p,n \in S_h \setminus \{root_h\} \\ \pi \cdot \mu_g(root_g, n) & \text{if } p = root \ \& \ n \in S_g \ \& \ root_g \rightsquigarrow n \\ (1-\pi) \cdot \mu_h(root_h, n) & \text{if } p = root \ \& \ n \in S_h \ \& \ root_h \rightsquigarrow n; \end{cases}$

Abstraction Let g be a graph in **G** and $g = (S_g \cup \{NIL_g\}, \rightsquigarrow_g, \rightarrow_g, \mu_g, root_g)$.
$\tau_I(g)$ for $I \subseteq A$ is defined as:

$$(S_g \cup \{NIL_g\}, \rightsquigarrow_g, \rightarrow, \mu_g, root_g),$$

where: $p \xrightarrow{a} n$ iff $p \xrightarrow{a}_g n$ and $a \notin I$ and
$p \xrightarrow{\tau} n$ iff $p \xrightarrow{a}_g n$ and $a \in I \cup \{\tau\}$.

Example 6.4.6. If the unwinding of the original graph is omitted in the definition of the probabilistic choice operator we obtain the situation shown in Figure 6.3c if g and h are as in Figure 6.3a and Figure 6.3b, respectively. Figure 6.3c allows unwanted behaviour, since after choosing to perform a, c can still be executed. Figure 6.3d. shows the probabilistic graph $g \boxplus_\rho h$. □

6.4.1 Probability measure on graphs

Similarly to the non-probabilistic case (see Definition 6.2.2) we allow here an observable action a ($a \neq \tau$) to be simulated by a sequence of transitions such that exactly the last transition is an a-transition and the rest are internal transitions within the same equivalence class. The new problem

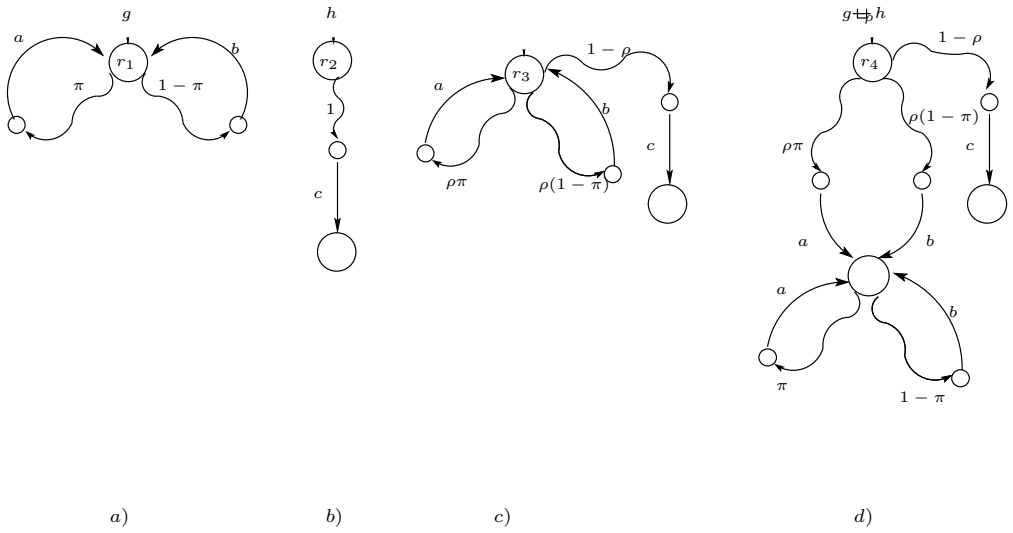


Figure 6.3: Probabilistic choice of g and h.

we should think about is the way we calculate the probability measure of such a sequence or a set of sequences of transitions according to the probability distribution function μ. In the sequel, we sketch (repeat) the standard concept used to define a probability measure (see [28, 29, 100]), adapted for the alternating model of fully probabilistic graphs.

Let $g = (S_p \cup S_n \cup \{NIL\}, \rightsquigarrow, \rightarrow, \mu, root)$ be a finite fully probabilistic graph. If it is not mentioned explicitly, we abbreviate $S_p \cup \{NIL\}$ by S_p.

Definition 6.4.7. For $p \in S_p$, $n \in S_n$, $C \subseteq S_p$, $a \in A_\tau$ and $L \subseteq A_\tau$ we define:

- $n \xrightarrow{a} C$ iff $\exists q \in C \ : \ n \xrightarrow{a} q$;
- $\mathbf{P}(p, a, C) = \sum_{n : n \xrightarrow{a} C} \mu(p, n)$, $\mathbf{P}(p, a, q) = \mathbf{P}(p, a, \{q\})$, $\mathbf{P}(p, a) = \mathbf{P}(p, a, S_p)$ and $\mathbf{P}(p, L) = \sum_{a \in L} \mathbf{P}(p, a)$;
- *An execution fragment* or *finite path* is a nonempty finite alternating sequence

$$\sigma = p_0 \rightsquigarrow n_0 \xrightarrow{a_1} p_1 \rightsquigarrow n_1 \xrightarrow{a_2} p_2 \ldots p_{k-1} \rightsquigarrow n_{k-1} \xrightarrow{a_k} p_k$$

such that $p_0, \ldots, p_k \in S_p \cup \{NIL\}$, $n_0, \ldots, n_{k-1} \in S_n$, $a_1, \ldots, a_k \in A_\tau$. We say that σ starts in p_0 and we write $first(\sigma) = p_0$, and also $trace(\sigma) = a_1 a_2 \ldots a_k$ and $last(\sigma) = p_k$. $|\sigma|$ denotes the length of σ, $|\sigma| = k$. If $last(\sigma) = NIL$, then σ is maximal.

- If $k = 0$ we define $\mathbf{P}(\sigma) = 1$. If $k \geq 1$ we define
$$\mathbf{P}(\sigma) = \mu(p_0, n_0) \cdot \mu(p_1, n_2) \cdot \ldots \cdot \mu(p_{k-1}, n_{k-1}).$$
- $\sigma(i)$ denotes the $(i+1)$-st probabilistic state of σ, $\sigma(i) = p_i$, $i = 0, 1, \ldots, k$;
- $\sigma^{(i)}$ denotes the i-th prefix of σ (counting only probabilistic states), that is, $\sigma^{(i)} = p_0 \rightsquigarrow n_0 \xrightarrow{a_1} p_1 \rightsquigarrow n_1 \xrightarrow{a_2} p_2 \ldots p_{i-1} \rightsquigarrow n_{i-1} \xrightarrow{a_i} p_i$ for $i = 0, 1, \ldots, k$; for $i > k$ we put $\sigma^{(i)} = \sigma$. If σ passes through probabilistic state q, by $\sigma^{(\rightarrow q)}$ we denote the prefix of σ which ends with the first occurrence of q in σ. By $\sigma^{(q \rightarrow)}$ we denote the subsequence of σ that starts at the first occurrence of q in σ.

Definition 6.4.8. *An execution* or *fullpath* is either a maximal execution fragment or an infinite sequence

$$\pi = p_0 \rightsquigarrow n_0 \xrightarrow{a_1} p_1 \rightsquigarrow n_1 \xrightarrow{a_2} p_2 \dots$$

such that $p_0, p_1, p_2, \dots \in S_p$, $n_0, n_1, n_2 \dots \in S_n$, $a_1, a_2, \dots \in A_\tau$. *A path* is a finite path or a fullpath.

- $Path_{ful}$ denotes the set of fullpaths in g;
- $Path_{ful}(p)$ denotes the set of fullpaths starting in p;
- $Path_{fin}$ denotes the set of finite paths in g;
- $Path_{fin}(p)$ denotes the set of finite paths starting in p;
- if Π is a set of fullpaths in g and $p \in S_p$, then $\Pi(p) = \Pi \cap Path_{ful}(p)$;
- if Σ is a set of finite paths in g and $p \in S_p$, then $\Sigma(p) = \Sigma \cap Path_{fin}(p)$;
- $\leq_{prefix}$ denotes the prefix relation on paths. Namely, if σ_1 and σ_2 are finite or infinite paths then $\sigma_1 \leq_{prefix} \sigma_2$ iff $\sigma_1 = \sigma_2$ or $\sigma_1 = \sigma_2^{(k)}$ for some k;
- if σ_1 is a finite path and σ_2 is a finite or infinite path such that $last(\sigma_1) = first(\sigma_2)$ then $\sigma_1 \circ \sigma_2$ is the path that arises by appending σ_2 at the end of σ_1 where the last state of σ_1 and the first state of σ_2 are identified;
- $\sigma \uparrow$ denotes the basic cylinder induced by σ, that is, $\sigma \uparrow = \{\pi \in Path_{ful}(p) \ : \ \sigma \leq_{prefix} \pi\}$ where $p = first(\sigma)$;
- $\sigma \uparrow_{fin} = \{\sigma' \in Path_{fin}(p) \ : \ \sigma \leq_{prefix} \sigma'\}$;
- $\sigma \downarrow = \{\sigma' \in Path_{fin}(p) \ : \ \sigma' \leq_{prefix} \sigma\}$;
- if Σ is a set of finite paths, $\Sigma \uparrow = \bigcup_{\sigma \in \Sigma} \sigma \uparrow$, $\Sigma \downarrow = \bigcup_{\sigma \in \Sigma} \sigma \downarrow$, $\Sigma \uparrow_{fin} = \bigcup_{\sigma \in \Sigma} \sigma \uparrow_{fin}$.

For each state p, $\mathbf{P}$ induces a probability space on $Path_{ful}(p)$ as follows. If $SigmaField(p)$ is the smallest sigma-field ([68]) on $Path_{ful}(p)$ which contains all basic cylinders $\sigma \uparrow$ where σ ranges over all finite paths starting in p, then the probability measure $Prob$ on $SigmaField(p)$ is the unique measure with $Prob(\sigma \uparrow) = \mathbf{P}(\sigma)$.

Lemma 6.4.9. ([28] Lemma 3.1.4) Let $p \in S_p$ and $\Sigma \subseteq Path_{fin}(p)$ such that $\sigma, \sigma' \in \Sigma$, $\sigma \neq \sigma'$ implies $\sigma \not\leq_{prefix} \sigma'$. Then, $Prob(\Sigma \uparrow) = \sum_{\sigma \in \Sigma} \mathbf{P}(\sigma)$. □

Now we turn our attention to the problem of reaching a certain set S_2 via a path going only through states of a certain set S_1. Let S_1, S_2 be subsets of S_p, Σ be the set of all finite paths σ such that $\sigma(i) \in S_1 \setminus S_2$, for $i = 0, 1, \dots, |\sigma| - 1$ and $last(\sigma) \in S_2$ and let $\Pi = \Sigma \uparrow$. Then our aim is to compute the probabilities $Prob(\Pi(p))$. The following result expresses this probability by use of the probabilities of the finite paths in $\Sigma(p)$. Moreover, it induces a linear equation system whose solution gives exactly the desired probabilities. Let us note that the definition of Σ guarantees that paths of $\Sigma(s)$ are pairwise disjoint.

Lemma 6.4.10. ([28]) Let g, S_1, S_2, Σ and Π be defined as above.

[Theorem 3.1.5] For all $p \in S_p$, $\sum_{\sigma \in \Sigma(p)} \mathbf{P}(\sigma) = Prob(\Pi(p))$.

[Theorem 3.1.6] The function $\pi : S_p \to [0,1], \pi(p) = Prob(\Pi(p))$ is the least fixed point of the operator $F : (S_p \to [0,1]) \to (S_p \to [0,1])$ which is given by $F(f)(p) = 1$ if $p \in S_2$, $F(f)(p) = 0$ if $p \in S_p \setminus (S_1 \cup S_2)$, and $F(f)(p) = \sum_{t \in S_p} \mathbf{P}(p,t) \cdot f(t)$ if $p \in S_1 \setminus S_2$.

[Lemma 3.1.10] If $T = \{last(\sigma) : \sigma \in Path_{fin}(p), \sigma \notin \Sigma\uparrow_{fin}\}$, then $\Sigma(t) \neq \emptyset$ for all states $t \in T$ iff $Prob(\Pi(p)) = 1$. □

Up to now we ignored traces of considered paths. From the definitions above and the construction of a probability measure on a given probabilistic graph and probabilities over a set of paths it is easy to include traces into the probability space. Informally, instead of measuring all finite paths starting at p and that reach a certain set of states C, now only the paths from p to C with certain traces are measured. Therefore, it is not surprising that similar results are obtained under these new conditions. From now on, by ε we denote the empty word in A_τ^*, for $\Omega \subseteq A_\tau^*$ $\Omega/\omega = \{\omega' : \omega\omega' \in \Omega\}$ where $\omega\omega'$ denotes concatenation of words.

- $Path_{fin}(p, \Omega, C)$ is the set of all finite paths σ such that $\sigma \in Path_{fin}(p)$, $trace(p) \in \Omega$ and $last(\sigma) \in C$;
- $Path_{ful}(p, \Omega, C) = \bigcup_{\sigma \in Path_{fin}(p,\Omega,C)} \sigma\uparrow$;
- $Prob(p, \Omega, C) = Prob(Path_{ful}(p, \Omega, C))$;
- For $Q \subseteq S_p$, $Path_{fin,Q}(p, \Omega, C)$ is the set of all finite paths $\sigma \in Path_{fin,Q}(p, \Omega, C)$ such that $\sigma(i) \in Q$, for all $0 \leq i \leq |\sigma| - 1$;
- $Path_{ful,Q}(p, \Omega, C)$ is the set of all fullpaths σ such that there exists $k \geq 0$ for which $\sigma^{(k)} \in Path_{fin,Q}(p, \Omega, C)$;
- $Prob_Q(p, \Omega, C) = Prob(Path_{ful,Q}(p, \Omega, C))$.

Proposition 6.4.11. ([28] Proposition 3.3.4) Let g be a fully probabilistic graph and $C \subseteq S_p$. The function from $S_p \times 2^{A^*}$ to $[0,1]$ defined by $(p, \Omega) \mapsto Prob(p, \Omega, C)$ is the least fixed point of the operator $F : (S_p \times 2^{A^*} \to [0,1]) \to (S_p \times 2^{A^*} \to [0,1])$ which is given by $F(f)(p, \Omega) = 1$ if $p \in C$ and $\varepsilon \in \Omega$, and if $p \notin C$ or $\varepsilon \notin \Omega$

$$F(f)(p, \Omega) = \sum_{(a,t) \in A \times S_p} \mathbf{P}(p, a, t) \cdot f(t, \Omega/a, C).$$

□

The following lemma which basically follows from the previous one expresses that under a certain condition we can "look compositionally at" the probability measure. In other words, if all considered paths from a certain state p to a set of states S pass through a state q (or in general case through a set of states Q) then the total probability can be obtained by multiplication of the probability of reaching q (Q) from p and the probability of reaching C from q (any state of Q). It will be used later when we investigate sequential composition of two probabilistic graphs.

Lemma 6.4.12. Let g be a fully probabilistic graph, $p \in S_p$, $Q \subseteq S_p$, $C \subseteq S_p \cup \{NIL\}$ and $\Omega_1, \Omega_2 \subseteq A_\tau^*$. Furthermore, if σ is a finite path from p to C with a trace in $\Omega_1\Omega_2 = \{\omega_1\omega_2 \,:\, \omega_1 \in \Omega_1, \omega_2 \in \Omega_2\}$, then it passes through q for some $q \in Q$, and additionally $trace(\sigma^{(\to q)}) \in \Omega_1$ and $trace(\sigma^{(q\to)}) \in \Omega_2$. Then

$$Prob(p, \Omega_1\Omega_2, C) = Prob(p, \Omega_1, Q) \cdot Prob(q, \Omega_2, C).$$

Proof. For the sake of simplicity we assume that Q is a singleton, $Q = \{q\}$. The proof can easily be expanded to the case of an arbitrary Q.

Let $\Sigma(p)$ denotes the set of all finite paths from p to C that pass through q and have traces as defined above. Furthermore, let $\Sigma^k(p)$ denotes the subset of $\Sigma(p)$ which contains those paths which reach q (for the first time) in exactly k steps. Namely, if

$$\sigma = p \equiv p_0 \rightsquigarrow n_0 \xrightarrow{a_1} p_1 \rightsquigarrow n_1 \xrightarrow{a_2} \dots p_{k-1} \rightsquigarrow n_{k-1} \xrightarrow{a_k} q \rightsquigarrow m_0 \xrightarrow{b_1} s_1 \rightsquigarrow \dots s_{l-1} \rightsquigarrow m_{l-1} \xrightarrow{b_l} C,$$

and $\sigma \in \Sigma(p)$ with $p_i \neq q$ for all $i = 0, 1, \dots, k-1$, $a_1a_2 \dots a_k \in \Omega_1$ and $b_1b_2 \dots b_l \in \Omega_2$, then $\sigma \in \Sigma^k(p)$. Thus, $\Sigma(p) = \bigcup\limits_{k\geq 1} \Sigma^k(p)$ under assumption that $p \neq q$. It is clear that these sets are pairwise disjoint and moreover, for all $\sigma \in \Sigma^i(t), \sigma' \in \Sigma^j(t)$, $(i \neq j)$ $\sigma \not\leq_{prefix} \sigma'$. Therefore, by Lemma 6.4.9 $Prob(\Sigma(p)\uparrow) = \sum\limits_{k\geq 1} Prob(\Sigma^k(p)\uparrow)$. Also, we note that if $\sigma \in \Sigma^k(p)$ then $\sigma^{(\to q)}$ is a finite path from p to q with $|\sigma^{(\to q)}| = k$ and $trace(\sigma^{(\to q)}) \in \Omega_1 \cap A_\tau^k$. We denote the set of such paths by $\Sigma^k(p, q)$.

Let us first consider the probability measure over paths in $\Sigma^1(p)$. According to Proposition 6.4.11

$$\begin{aligned} Prob(\Sigma^1(p)\uparrow) &= \sum_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot Prob(t_1, \Omega/l_1, C) \\ &= \sum_{l_1\in\Omega_1, t_1 = q} \mathbf{P}(p, l_1, t_1) \cdot Prob(t_1, \Omega/l_1, C) \text{ (for the other summands the value is 0)} \\ &= \sum_{l_1\in\Omega_1\cap A_\tau} \mathbf{P}(p, l_1, q) \cdot Prob(q, \Omega/l_1, C) = Prob(p, \Omega_1, q) \cdot Prob(q, \Omega_2, C). \end{aligned}$$

To make it more clear let us consider the probability measure of $\Sigma^2(p)\uparrow$.

$$\begin{aligned} Prob(\Sigma^2(p)\uparrow) &= \sum_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot Prob(t_1, \Omega/l_1, C) \\ &= \sum_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot \sum_{(l_2,t_2)\in A_\tau \times S_p} \mathbf{P}(t_1, l_2, t_2) \cdot Prob(t_2, \Omega/l_1l_2, C) \\ &= \sum_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot \sum_{l_1l_2\in\Omega_1, t_2 = q} \mathbf{P}(t_1, l_2, t_2) \cdot Prob(t_2, \Omega/l_1l_2, C) \\ &\qquad \text{(for the other summands the value is 0)} \\ &= \sum_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot \sum_{l_2 : l_1l_2\in\Omega_1} \mathbf{P}(t_1, l_2, q) \cdot Prob(q, \Omega/l_1l_2, C). \end{aligned}$$

We claim that $\sum\limits_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot \sum\limits_{l_2 : l_1l_2\in\Omega_1} \mathbf{P}(t_1, l_2, q) \cdot Prob(q, \Omega/l_1l_2, C) = Prob(p, \Omega_1 \cap A_\tau^2, q) \cdot Prob(q, \Omega_2, C)$, where by $Prob(p, \Omega_1 \cap A_\tau^2, q) = Prob(\Sigma^2(p, q)\uparrow)$.

First, the conclusion $\Omega/l_1l_2 = \Omega_2$ follows easily from the definition of Ω and the fact that $l_1l_2 \in \Omega_1$. Next, from the definition of $\Sigma^2(p, q)$ it follows easily that $Prob(\Sigma^2(p, q)\uparrow) = Prob(p, \Omega_1 \cap A_\tau^2, q)$. Then,

$$\begin{aligned} Prob(p, \Omega_1 \cap A_\tau^2, q) &= \sum_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot \sum_{(l_2,t_2)\in A_\tau \times S_p} \mathbf{P}(t_1, l_2, t_2) \cdot Prob(t_2, \Omega_1 \cap A_\tau^2/l_1l_2, q) \\ &= \sum_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot \sum_{l_2 : l_1l_2\in\Omega_1\cap A_\tau^2} \mathbf{P}(t_1, l_2, q) \cdot Prob(q, \Omega_1 \cap A_\tau^2, q) \\ &= \sum_{(l_1,t_1)\in A_\tau \times S_p} \mathbf{P}(p, l_1, t_1) \cdot \sum_{l_2 : l_1l_2\in\Omega_1\cap A_\tau^2} \mathbf{P}(t_1, l_2, q) \end{aligned}$$

since $Prob(q, \Omega_1 \cap A_\tau^2/l_1l_2, q) = 1$ under assumption that $\Sigma^2(p,q) \neq \emptyset$ and $l_1l_2 \in \Omega_1$, otherwise the entire sum equals 0. Moreover, $\{l_2 \ : \ l_1l_2 \in \Omega_1\} = \{l_2 \ : \ l_1l_2 \in \Omega_1 \cap A_\tau^2\}$ since l_2 is an action in A_τ.

In a similar way (extending the expression for k steps) for the probability measure of $\Sigma^k(p) \uparrow$ we obtain:

$Prob(\Sigma^k(p) \ \uparrow) \ = \ Prob(p, \Omega_1 \cap A_\tau^k, q) \cdot Prob(q, \Omega_2, C)$, where $Prob(p, \Omega_1 \cap A_\tau^k, q) = Prob(\Sigma^k(p,q) \uparrow)$.

Finally, from the results for the probability measure $Prob(p, \Omega, C)$ on $\Sigma(p)$ obtained above we conclude:

$$\begin{aligned} Prob(\Sigma(p) \uparrow) &= \sum_{k\geq 1} Prob(\Sigma^k(p,q) \uparrow) = \sum_{k\geq 1} Prob(p, \Omega_1 \cap A_\tau^k, q) \cdot Prob(q, \Omega_2, C) \\ &= Prob(q, \Omega_2, C) \cdot \left(\sum_{k\geq 1} Prob(p, \Omega_1 \cap A_\tau^k, q) \right) = Prob(q, \Omega_2, C) \cdot Prob(p, \Omega_1, q). \end{aligned}$$

□

6.5 Probabilistic branching bisimulation

The bisimulation on the set of fully probabilistic graphs we propose here is based on the notion of a *set of entries* (a subset of the set of probabilistic nodes) and a *set of exits* (a subset of the set of action nodes). If R is a given equivalence relation on a probabilistic graph g, an *exit* of a probabilistic state p in g is an action state e reachable from p through and internal path ($p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \cdot \rightsquigarrow e$) that is the outgoing state of an external action transition ($e \stackrel{a}{\rightarrow} q$) or an internal transition that leads to a new equivalence class ($e \stackrel{\tau}{\rightarrow} q$ and $(p,q) \notin R$). Every probabilistic state has a unique set of exits. Having *the sets of exits* determined for each probabilistic node in the graph we can obtain *the set of entries*. The procedure to get the set of entries of graph g is iterative. First, the root of the graph is an entry. Further, an entry in one equivalence class is a node that is first entered from an exit of an entry obtained in the previous iteration, say r, by taking either an external or an internal action. An external action may lead to the same equivalence class of r, but an internal action has to lead to an equivalence class different from $[r]_R$. In this way, each entry determines the set of its succeeding entries. A probabilistic node q is not an entry if it is reachable from entries belonging to the equivalence class of q only through internal paths passing through this equivalence class. Finally, for each entry the probabilities for reaching the equivalence classes of its succeeding entries are computed. All entries with the same probability distribution are considered bisimilar. For non-entry nodes the probabilities are not computed. Technically this involves the existence of an equivalence relation $\tilde{R}$ obtained from R that relates only entries with the same probability measures. Formal definitions follow.

Definition 6.5.1. [Entry] If g is a fully probabilistic graph and if R is an equivalence relation on the set of states then:

$Entry_0(g) = \{root(g)\}$,

$Entry_{i+1}(g) = \{q \ : \ \exists r \in Entry_i : \exists e \in Exit_R(r) : e \stackrel{a}{\rightarrow} q, a \in A_\tau \ \& \ q \notin [r]_R\}$
$\cup \{q \ : \ \exists r \in Entry_i : \exists e \in Exit_R(r) : e \stackrel{a}{\rightarrow} q, a \in A \ \& \ q \in [r]_R\}$,

where $Exit_R(r) = \{s \ : \ r \stackrel{\tau^*}{\Longrightarrow}_{[r]_R} \cdot \rightsquigarrow s \ \& \ \exists C \neq [r]_R : s \stackrel{a}{\rightarrow} C, a \in A_\tau\}$
$\cup \{s \ : \ r \stackrel{\tau^*}{\Longrightarrow}_{[r]_R} \cdot \rightsquigarrow s \ \& \ s \stackrel{a}{\rightarrow} [r]_R, a \in A\}$.

Finally, $Entry_R(g) = \bigcup_{i\geq 0} Entry_i(g)$.

By $\stackrel{\tau^*}{\Longrightarrow}$ we denote the transitive and reflexive closure of $\rightsquigarrow \cdot \stackrel{\tau}{\rightarrow}$ and by $\stackrel{\tau^*}{\Longrightarrow}_Q$ we denote the transitive and reflexive closure of $\{p \rightsquigarrow \cdot \stackrel{\tau}{\rightarrow} p' \ : \ p, p' \in Q\}$ for $Q \subseteq S_p \cup \{NIL\}$.

Definition 6.5.2. If g is a fully probabilistic graph, R and $\tilde{R}$ are equivalence relations on the set of states such that $\tilde{R} \subseteq R$ and if $r \in S_p$, then:
$NextEntry(r) = \{q \ : \ \exists e \in Exit_R(r) : e \stackrel{a}{\rightarrow} q, a \in A_\tau \ \& \ q \notin [r]_R\}$
$\cup \{q \ : \ \exists e \in Exit_R(r) : e \stackrel{a}{\rightarrow} q, a \in A \ \& \ q \in [r]_R\}$
and $NextEntryC_{\tilde{R}}(r) = \{[q]_{\tilde{R}} \ : \ q \in NextEntry(r)\}$.

Example 6.5.3. Let g and h be the graphs given in Figure 6.4. For the equivalence relation R induced by the partition $\{\{1,2,4,6,8,9\},\{3,5,7,12,15,18\},\{10,13,16\},\{11,14,17\}\}$, $Entry_R(g \cup h) = \{1,2,3,4,5,6,7\}$ and

r	1	3	2	4	5	6	7
$Exit_R(r)$	$10,11$	12	$10,11$	$13,14$	15	$16,17$	18
$NextEntry_R(r)$	3	2	3	5	6	7	6

For T defined by $\{\{1,2,4,6,8,9,12,15,18\},\{10,13,16\},\{11,14,17\}\}$, $Entry_T(g \cup h) = \{1,3,4,5,7\}$ and

r	1	3	4	5	7
$Exit_T(r)$	$10,11$	$10,11$	$13,14$	$16,17$	$16,17$
$NextEntry_T(r)$	3	3	5	7	7

By $Entry(g \cup h)$ we mean $Entry(g) \cup Entry(h)$. The state shading given in Figure 6.4 corresponds to the relation R. □

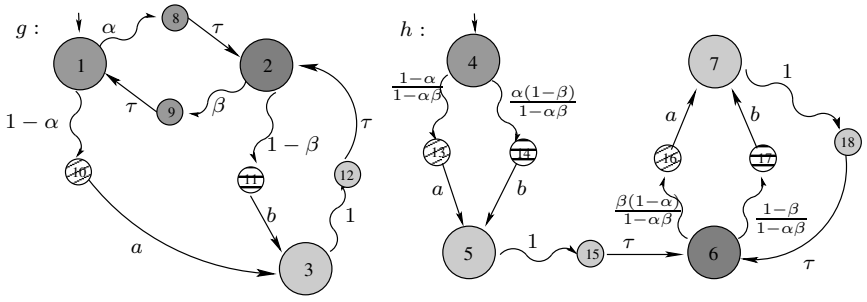


Figure 6.4: Probabilistic process graphs together with an equivalence relation on states.

Proposition 6.5.4. Let R be an equivalence relation on a fully probabilistic graph g and p be a probabilistic node in g. There is a probabilistic node q such that $(p,q) \in R$, $q \in Entry_R(g)$ and $q \stackrel{\tau^*}{\Longrightarrow}_{[q]_R} p$.

Proof. It is clear that the claim is true for all entries in g w.r.t. R. Having in mind that every node in g is reachable from $root(g)$ we define a *distance* from the root as:

if $\sigma \equiv root(g) \rightsquigarrow e_1 \xrightarrow{a_1} p_1 \rightsquigarrow e_2 \xrightarrow{a_2} \ldots p_{n-1} \rightsquigarrow e_n \xrightarrow{a_n} p$ is the shortest path from $root(g)$ to p then $dist(p) = n$. We put $dist(root(g)) = 0$.

The proof of the claim above is given by induction on $dist(p)$. Let us assume that p is a probabilistic node in g.

`Basis` If $dist(p) = 0$ then $p \equiv root(g)$ and the claim is true.

`Inductive step` Let us assume that for all r such that $dist(r) < n$ the statement is true and let p be a node with $dist(p) = n$. Thus, $root(g) \rightsquigarrow e_1 \xrightarrow{a_1} p_1 \rightsquigarrow e_2 \xrightarrow{a_2} \ldots p_{n-1} \rightsquigarrow e_n \xrightarrow{a_n} p$ is the shortest path from $root(g)$ to p. From graph theory we conclude that $\forall i < n \ : \ dist(p_i) = i$. Therefore, if $p_{n-1} \in [p]_R$ and $a_n = \tau$ by the induction hypothesis there is a node r such that $r \in [p_{n-1}]_R = [p]_R$, $r \in Entry_R(g)$ and $r \stackrel{\tau^*}{\Longrightarrow}_{[r]_R} p_{n-1}$. Then $r \stackrel{\tau^*}{\Longrightarrow}_{[r]_R} p$ as well. In any other case $a_n \neq \tau$ and so, p is an entry and the statement is true. □

Corollary 6.5.5. If R is defined as above, then for any R equivalence class C such that $C \cap (S_p \cup \{NIL\}) \neq \emptyset$, there is a $c \in C$, $c \in Entry_R(g)$. □

Due to the fact that two entries from the same equivalence class may have different sets of equivalence classes of their next entries, these sets have to be parametrized by the entry they are associated to (see Example 6.5.8).

Definition 6.5.6. (Probabilistic branching bisimulation) Let g and h be fully probabilistic graphs. If R is an equivalence relation on $S_g \cup S_h \cup \{NIL_g, NIL_h\}$ such that:

0. $(root(g), root(h)) \in R$;

1. if $(p, q) \in R$ and $p \rightsquigarrow s$ then either

1.0 $(s, q) \in R$ or

1.1 there are v, t such that $(p, v), (s, t) \in R$ and $q \stackrel{\tau^*}{\Longrightarrow} v \rightsquigarrow t$ or $q \xrightarrow{\tau} \cdot \stackrel{\tau^*}{\Longrightarrow} v \rightsquigarrow t$;

2. if $(p, q) \in R$ and $p \xrightarrow{a} s$ then either

2.0 $a = \tau$ and $(s, q) \in R$ or

2.1 there are v, t such that $(q, v), (s, t) \in R$ and $q \stackrel{\tau^*}{\Longrightarrow} \cdot \rightsquigarrow v \xrightarrow{a} t$ or $q(\xrightarrow{\tau} \cdot \rightsquigarrow)^* v \xrightarrow{a} t$;

3. there is an equivalence relation $\tilde{R}$ on $Entry_R(g) \cup Entry_R(h)$ such that $\tilde{R} \subseteq R$ and

3.0. $(root(g), root(h)) \in \tilde{R}$;

3.1. if $(p, q) \in \tilde{R}$ then for any $C \in NextEntryC_{\tilde{R}}(p) \cup NextEntryC_{\tilde{R}}(q)$ and for any $a \in A$,
$Prob_{[p]_R}(p, \tau^*, C) = Prob_{[q]_R}(q, \tau^*, C)$ and
$Prob_{[p]_R}(p, \tau^* a, C) = Prob_{[q]_R}(q, \tau^* a, C)$;

then $(R, \tilde{R})$ is a *probabilistic branching bisimulation relation* between g and h. We write $g \underline{\leftrightarrow}_{pb} h$ if there is a probabilistic branching bisimulation $(R, \tilde{R})$ between g and h.

g and h are probabilistically rooted branching bisimilar, $g \underline{\leftrightarrow}_{prb} h$, if there is a probabilistic branching bisimulation $(R, \tilde{R})$ between g and h such that

4.1 if $root(g) \rightsquigarrow p$ then there is q in h such that $root(h) \rightsquigarrow q$ and $(p,q) \in R$;

4.2 if $root(g) \rightsquigarrow q$ then there is p in g such that $root(g) \rightsquigarrow p$ and $(p,q) \in R$;

5.1 if $root(g) \rightsquigarrow p \xrightarrow{a} s$ for $a \in A_\tau$ then there are q and t in h such that $root(h) \rightsquigarrow q \xrightarrow{a} t$ and $(p,q) \in R$ and $(s,t) \in R$;

5.2 if $root(h) \rightsquigarrow q \xrightarrow{a} t$ for $a \in A_\tau$ then there are p and s in g such that $root(s) \rightsquigarrow q \xrightarrow{a} s$ and $(p,q) \in R$ and $(s,t) \in R$.

The condition expressed by 4.1, 4.2, 5.1 and 5.2 is called *probabilistic root branching conditions*.

The requirements 0, 1 and 2 are counterparts for the requirements 1 and 2 in Definition 6.2.2. In other words, if probabilistic transitions are treated as internal transitions then the conditions 0, 1 and 2 express that (first of all) two bisimilar probabilistic graphs have to match on their branching structure in the sense of branching bisimulation.

From now on, instead of $Prob_{[p]_R}(p, \tau^*, C)$ and $Prob_{[p]_R}(p, \tau^* a, C)$ we will write $Prob_R(p, \tau^*, C)$ and $Prob_R(p, \tau^* a, C)$, respectively. (From $Prob_R(p, \tau^*, C)$ it is clear that $[p]_R$ is the subscript set in the original notation.) Even if $[p]_{\tilde{R}}$ is not a $NextEntry$ class for p, we take by default $Prob_{[p]_R}(p, \tau^*, [p]_{\tilde{R}}) = 1$. As usual we write $\hat{a}$ for a if $a \in A$ and λ (the empty word) if $a = \tau$.

Example 6.5.7. Let g and h be fully probabilistic graphs given in Figure 6.5. We consider the relation R induced by the following partition: $\{\{1,2,3,4,5\},\{6,8\},\{7,9\},\{NIL\}\}$. Then $Entry_R(g \cup h) =$

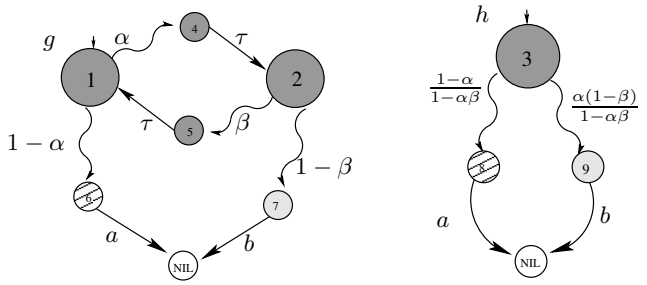


Figure 6.5: Probabilistic branching bisimilar graphs.

$\{1,3,NIL\}$ and we take $\tilde{R}$ to be efined by the partition $\{\{1,3\},\{NIL\}\}$. Probabilities of these entries to the $\tilde{R}$ equivalence classes are given in the following table. In the table we put $-$ in the (r,C) field if $C \notin NextEntryC_{\tilde{R}}(r)$. We omit the row of the NIL entry.

τ^*	$\{1,3\}$	$\{NIL\}$	$\tau^* a$	$\{1,3\}$	$\{NIL\}$	$\tau^* b$	$\{1,3\}$	$\{NIL\}$
1	1	0	1	$-$	$\frac{1-\alpha}{1-\alpha\beta}$	1	$-$	$\frac{\alpha(1-\beta)}{1-\alpha\beta}$
3	1	0	3	$-$	$\frac{1-\alpha}{1-\alpha\beta}$	3	$-$	$\frac{\alpha(1-\beta)}{1-\alpha\beta}$

Hence, $(R, \tilde{R})$ is a probabilistic branching bisimulation between g and h. This example shows the need to take all paths going through R but not through $\tilde{R}$ equivalence classes. Note that these graphs are related to the processes in our motivating examples 6.3.1 and 6.3.2. □

Example 6.5.8. For the graphs g and h in Figure 6.6 there are two equivalence relations that satisfy the condition 0, 1 and 2 in Definition 6.5.6: R_1 induced by the partition $\{\{1,3\},\{2,4,5,6\},\{NIL\}\}$

and R_2 induced by the partition $\{\{1,2,3,4,5,6\},\{NIL\}\}$. But only for R_2 an equivalence relation $\tilde{R}_2$ that satisfies the third condition of the definition can be defined, namely, $\tilde{R}_2$ can be defined by the partition $\{\{1,3\},\{NIL\}\}$. Therefore, $g \leftrightarrow_{pb} h$. But, $g \not\leftrightarrow_{prb} h$ because R_2 does not satisfy the root condition in Definition 6.5.6, and no other bisimulation between g and h can be established. This example actually shows that $\tau \cdot a \not\leftrightarrow_{prb} a$ and so $\mathit{fpBPA}_\tau \not\models \tau \cdot a = a$ as is the case for BPA^τ. □

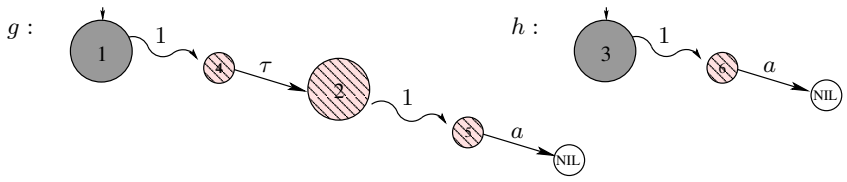


Figure 6.6: Probabilistic bisimilar but not root bisimilar graphs.

In order to conclude that graphs g and h from the previous example are not probabilistic rooted branching bisimilar we investigated two equivalence relations R_1 and R_2 likely to give the desired bisimulation. The following proposition states that it was enough to check only R_1 because it has a specific property: the roots of the graphs constitute an equivalence class.

Proposition 6.5.9. If g and h are root acyclic graphs that are probabilistic rooted branching bisimilar, then there is a probabilistic rooted branching bisimulation $(R, \tilde{R})$ between g and h such that $\{root(g), root(h)\}$ forms an R equivalence class. □

Proposition 6.5.10. $\leftrightarrow_{prb}$ is an equivalence relation on $\mathbf{G}$. □

From now on our main aim is to show that $\leftrightarrow_{prb}$ preserves the operators of fpBPA_τ and on this basis to construct the model of the algebra. For that purpose we will establish certain properties, mainly concerning the probability measure, that will bring us close to the desired property of $\leftrightarrow_{prb}$. Our primary intention is to describe what happens with the equivalence classes, the set of entries and the probability measure of a graph g with equivalence relation R on its set of states when it is considered as a composition of few smaller graphs. It will turn out that all important issues can be "decomposed" over the smaller graphs.

Let R be a equivalence relation on g that satisfies the conditions 0, 1 and 2 from Definition 6.5.6.

Proposition 6.5.11. If e_{NIL} is an entry from $[NIL]_R$ then $NextEntry_R(e_{NIL}) = \emptyset$.

Proof. Follows directly from the definition of the set $NextEntry_R$ and the fact that NIL is a termination state. □

In the sequel by e_{NIL} we will denote an entry from the $[NIL]_R$ equivalence class. We do so because not always NIL is an entry, but according to Proposition 6.5.4 e_{NIL} always exists. Entries from $[NIL]_R$ play an important role when a sequential composition of two graphs is constructed.

Proposition 6.5.12. $\forall p \in [NIL]_R \ : \ Prob_R(p, \tau^*, NIL) = 1$.

Proof. If $p \in [NIL]_R$ then NIL can be reached from p only via paths with trace τ^*. Moreover, NIL is reachable from every state in $[NIL]_R$. Take $\Sigma(p)$ to be the set of all paths from p to NIL. Then, $\Sigma(p) \uparrow_{fin} = \Sigma(p)$. Hence, the result follows from Lemma 6.4.10 (the third item) with $T \subseteq [NIL]_R \setminus \{NIL\}$ since no terminal state belongs to T from which $\Sigma(t) \neq \emptyset$ for $t \in T$. □

Stated differently, if graph g is viewed as a discrete time Markov chain (if the labels are not taken into account) the $[NIL]_R$ class forms a subset of the set of states of g such that once it entered it cannot be left. Furthermore, NIL appears as the only absorbing state in this subset of states. (Also it is the only absorbing state for the entire graph but possibly reached via traces different from τ^*.)

Proposition 6.5.13. If $x \notin NextEntry_R(p)$ and $x \notin [p]_R$ then

$$Prob_R(p, \tau^* a, C) = Prob_R(p, \tau^* a, C \cup \{x\}) = Prob_R(p, \tau^* a, C \setminus \{x\})$$

Proof. From the definition of the probability measure on g we have that $Prob_R(p, \tau^* a, C) = Prob(\Sigma_1)$ and $Prob_R(p, \tau^* a, C \cup \{x\}) = Prob(\Sigma_2)$, where $\Sigma_1 = \{\sigma \in Path_{fin}(p, \tau^* a, C) : \sigma = p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} C\}$ and $\Sigma_2 = \{\sigma \in Path_{fin}(p, \tau^* a, C \cup \{x\}) : \sigma = p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} C$ or $\sigma = p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} x\}$. But if there exists a path $\sigma \in \Sigma_2$ such that $\sigma = p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} x$ then we obtain that $x \in NextEntry_R(p)$ which contradicts the assumption. Therefore, no such a path exists, which implies that $\Sigma_1 = \Sigma_2$ and also $Prob_R(p, \tau^* a, C) = Prob_R(p, \tau^* a, C \cup \{x\})$. □

Now we look at sequential composition of two graphs. Let R_g and R_s be equivalence relations on fully probabilistic graphs g and s respectively, that satisfy the conditions 0, 1 and 2 from Definition 6.5.6. These relations induce an equivalence relation $R_{g \cdot s}$ on $g \cdot s$ defined by the following partition:

$$\begin{array}{ll} & \{C \,:\, C \text{ is an } R_g \text{ equivalence class } \& \; C \neq [NIL_g]_{R_g}\} \\ \cup & \{C \,:\, C \text{ is an } R_s \text{ equivalence class } \& \; C \neq [root(s)]_{R_s}\} \\ \cup & \{([NIL_g]_{R_g} \cup [root(s)]_{R_s}) \setminus \{NIL_g\}\}. \end{array}$$

Of course this definition of $R_{g \cdot s}$ and in general the sequential composition of g and s makes sense only if NIL_g is a state in g (reachable from $root(g)$). Otherwise, by definition $g \cdot s = g$ and no further investigation needs to be done. So, from now on we assume that NIL_g is a state of g when the sequential composition is considered.

Now we are interested in the relation between the set of entries of $g \cdot s$ and the set of entries of g and s with respect to associated equivalence relations. We will show that the way $R_{g \cdot s}$ is chosen does not disturb the set of entries of the original graphs except for the equivalence class which merges $[NIL]_{R_g}$ and $[root(s)]_{R_s}$. In that way, we can derive certain properties of $g \cdot s$ from some assumed properties of g and s. We aim it to be used later in the proof of the congruence property of $\underline{\leftrightarrow}_{prb}$. In particular, we would like to express the probability measure on $g \cdot s$ by means of the probability measures on g and s because it will allow as to compare the reachability probabilities in $g \cdot s$ on the basis of the reachability probabilities of g and s. We abbreviate $R_{g \cdot s}$ by R.

Lemma 6.5.14. R satisfies the requirements 0, 1 and 2 from Definition 6.5.6. □

Proposition 6.5.15. $Entry_R(g \cdot s) = \big(Entry_{R_g}(g) \cup Entry_{R_s}(s)\big) \setminus \{NIL_g\}$
or $Entry_R(g \cdot s) = \big(Entry_{R_g}(g) \cup Entry_{R_h}(s)\big) \setminus \{NIL_g, root(s)\}$.

Proof. First, it is obvious that $Entry_{R_g}(g) \setminus \{NIL_g\} \subseteq Entry_R(g \cdot s)$ and that NIL_g cannot be an entry of $g \cdot s$ because it is not a state of this graph.

Second, if $NIL_g \in Entry_{R_g}(g)$ then

$$\exists r \in Entry_{R_g}(g) : \exists e \in Exit_{R_g}(r) : \quad \Big(\big(e \stackrel{a}{\rightarrow} NIL_g \;\&\; NIL_g \notin [r]_R \;\&\; a \in A_\tau\big) \text{ or } \big(e \stackrel{a}{\rightarrow} NIL_g \;\&\; NIL_g \in [r]_R \;\&\; a \in A\big)\Big).$$

The latter case is not possible (NIL cannot have entries), and so, by the definition of $g \cdot s$ and the definition of R follows that $r \in Entry_R(g \cdot s)$, $e \in Exit_R(r)$ and $\big(e \xrightarrow{a} root(s)\ \&\ root(s) \notin [r]_R\ \&\ a \in A_\tau\big)$. Therefore, $root(s) \in Entry_R(g \cdot s)$ which implies $Entry_{R_s}(s) \subseteq Entry_R(g \cdot s)$ (see graphs in Figure 6.8 and Figure 6.7).

Third, if $NIL_g \notin Entry_{R_g}(g)$ then there are two possibilities. If $root(s) \notin Entry_i(s)$ for any $i > 0$ then $root(s) \notin Entry_R(g \cdot s)$; otherwise we would be able to construct a path which makes NIL_g an entry of g (graphs $g_2 \cdot s_1$ and $g_2 \cdot s_3$ in Figure 6.9). The second possibility is that $root(s)$ is reached by an entry of s in which case $root(s) \in Entry_i(s)$ for some $i > 0$. Then $root(s) \in Entry_R(g \cdot s)$ even though NIL_g is not an entry of g (graph $g_2 \cdot s_2$ in Figure 6.9 for g_2 and s_2 given in Figure 6.7). □

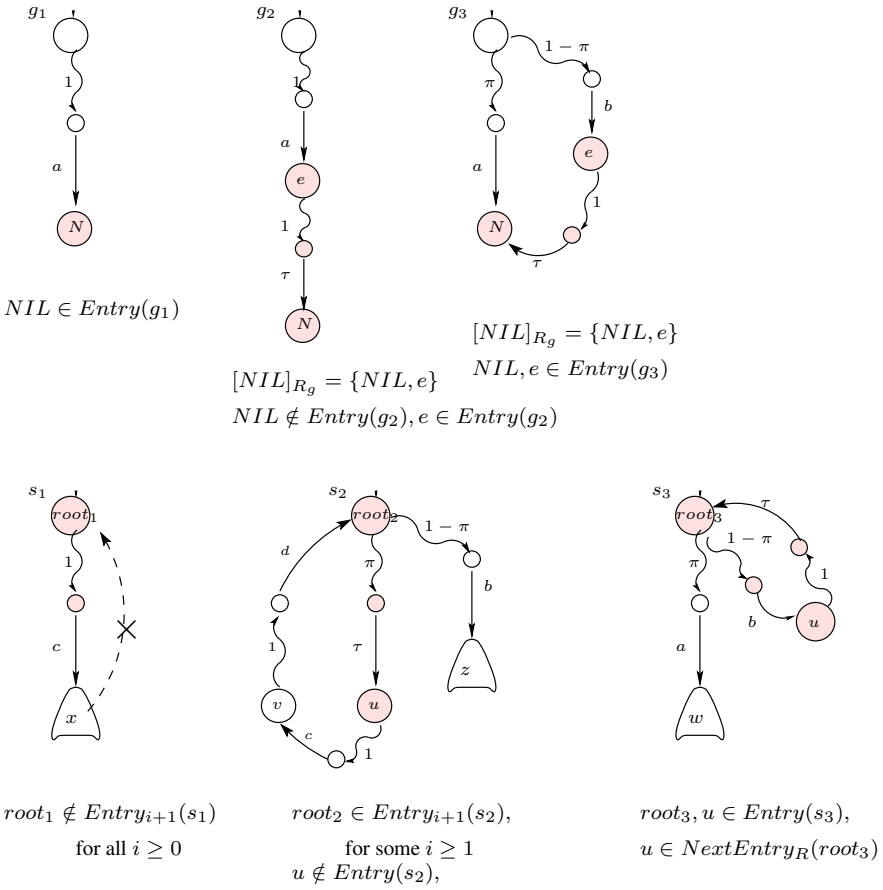


Figure 6.7: Probabilistic graphs with their entries (partially).

Next, we go a step forward and consider probability measures on $g \cdot s$. Our intention is to express probability $Prob_R(p, \tau^* \hat{a}, C)$ through probabilities in g and s which gives a compositional look at the bisimulation we defined earlier. In general, C can be an arbitrary set of states of $g \cdot s$. However, according to the definition of probabilistic branching bisimulation we do not need to consider any set of states but for the following result we restrict C to range only over R equivalence classes or a subset of them such that it contains only entries of g. In such a way we avoid unnecessary complications that arise by allowing an arbitrary C. Due to the definition of the probabilistic branching bisimulation

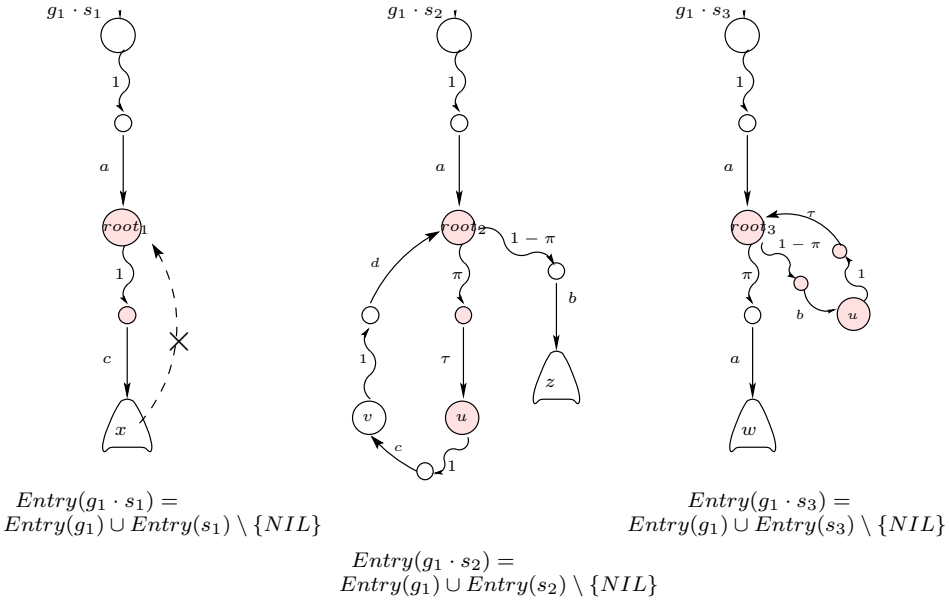


Figure 6.8: Sequential composition - part 1 (graph g_1)

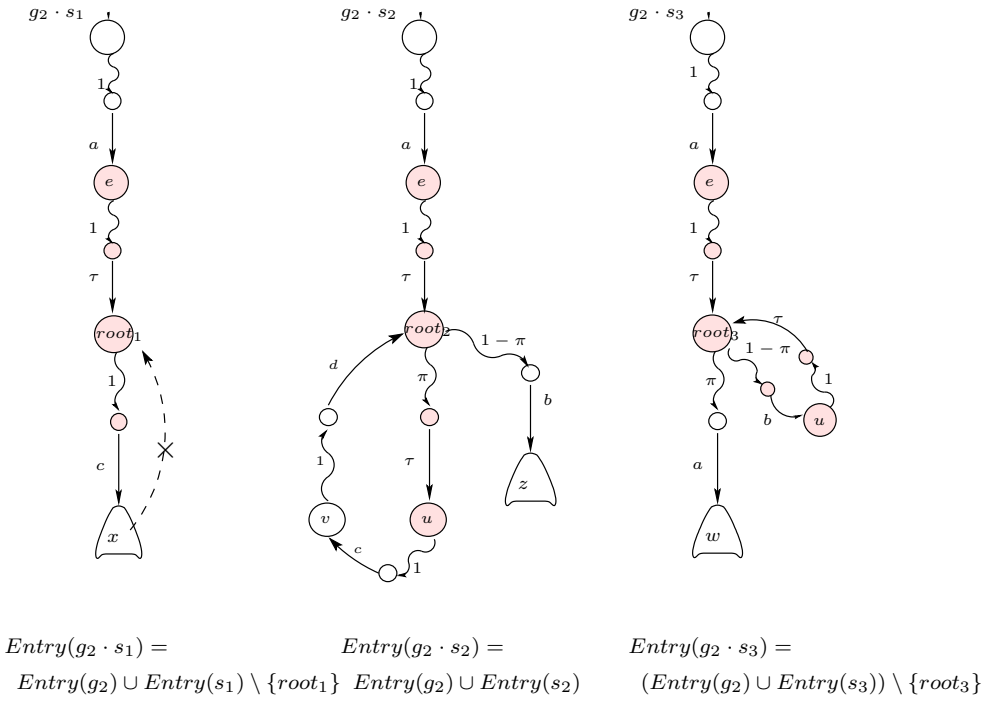


Figure 6.9: Sequential composition - part 2 (graph g_2).

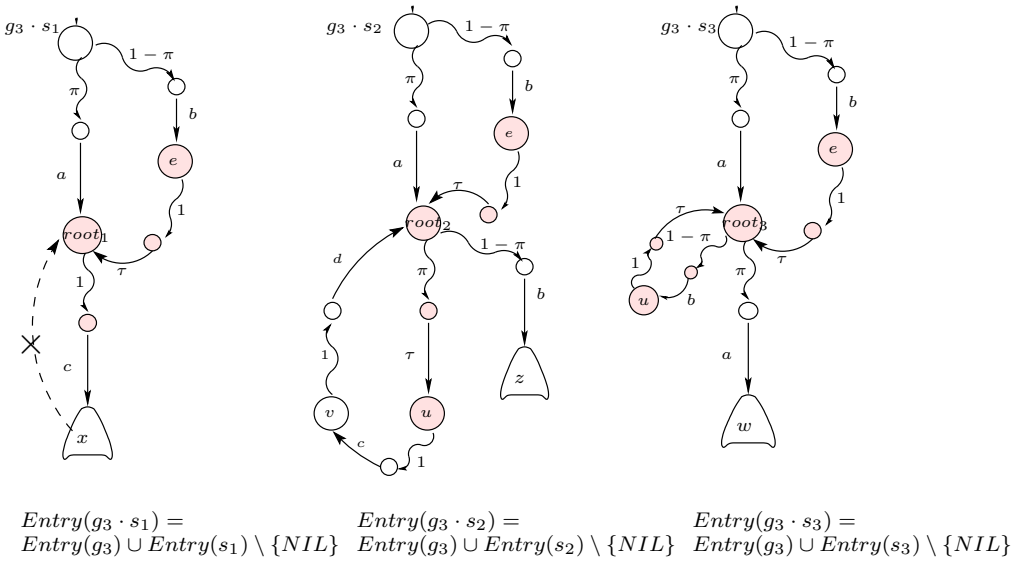


Figure 6.10: Sequential composition - part 3 (graph g_3).

this restriction on C will be done later anyway in the proof of the Congruence theorem where this lemma is used. Namely, in the proof of the Congruence theorem C ranges over $\tilde{R}_g$ and $\tilde{R}_s$ equivalence classes, where the existence of $\tilde{R}_g$ and $\tilde{R}_s$ is guaranteed by the assumption of the theorem according to Definition 6.5.6. We claim that

Lemma 6.5.16. If $p \in Entry_R(g \cdot s)$ and C is a subset of an R equivalence class such that C contains only entries, then $Prob_R(p, \tau^*\hat{a}, C)$ can be expressed by means of $Prob_{R_g}(t, \tau^*\hat{a}, D)$ and $Prob_{R_s}(u, \tau^*\hat{a}, E)$ for D and E subsets of some equivalence classes of R_g and R_s and for some $t \in S_g$ and $u \in S_s$.

Proof. If C is (a subset of) an R equivalence class then $C = D$ for D (a subset of) an R_g equivalence class different from $[e_{NIL}]_{\tilde{R}_g}$, or $C = E$ for E (a subset of) an R_s equivalence class different from $[root(s)]_{\tilde{R}_s}$, or $C \subseteq B$ for $B = \left([NIL]_{R_g} \cup [root(s)]_{R_s}\right)$ according to the definition of $R_{g \cdot s}$. Recall that $p \in Entry_R(g \cdot s)$ if either $p \in Entry_{R_g}(g) \setminus [NIL_g]_{R_g}$ or $p \in Entry_{R_s}(s) \setminus [root(s)]_{R_s}$ or p is an entry from $[root(s)]_R$ equivalence class. Clearly, if p is a state in s (g) and C is a subset of the states of g (s) then the probability to reach C from p equals 0 and this case is not of our interest. Depending on p and C we have the following non-trivial cases:

1. if $p \in Entry_{R_g}(g)$ and $C = D$ as given above, it follows directly that $Prob_R(p, \tau^*a, C) = Prob_{R_g}(p, \tau^*a, D)$;

2. if $p \in Entry_{R_s}(s)$ and $C = E$ as given above, then $Prob_R(p, \tau^*a, C) = Prob_{R_s}(p, \tau^*a, E)$;

3. if $p \in Entry_{R_g}(g)$ and $C \subseteq B$ and $p \notin [NIL]_{R_g}$. We assume that $[e_{NIL_g}]_{R_g} \cap NextEntry_{R_g}(p) \neq \emptyset$ for e_{NIL_g} is an entry from $[NIL_g]_{R_g}$; otherwise C is not reachable from p and the probability is 0. From the definition of $g \cdot s$ it is clear that $NextEntry_R(p) \subseteq S_g \cup \{root(s)\}$ since $NextEntry_{R_g}(p) \subseteq S_g \cup \{NIL_g\}$. In other words, whether or not C contains states from S_s, the relevant finite paths for the measure $Prob_R(p, \tau^*\hat{a}, C)$ reaches C in states from S_g or in $root(s)$. Therefore,
$Prob_R(p, \tau^*\hat{a}, C) = Prob_R(p, \tau^*\hat{a}, C \cap (S_g \cup \{root(s)\}))$

$$= \begin{cases} Prob_{R_g}(p, \tau^*\hat{a}, C \cap S_g), & if\ root(s) \notin C \\ Prob_{R_g}(p, \tau^*\hat{a}, C \cap (S_g \cup \{NIL_g\})), & if\ root(s) \in C \end{cases}$$

(For instance $g_3 \cdot s_3$ in Figure 6.10 with $p \equiv root(g_3)$ and $C = \{e, root_3, u\}$.)

4. if $p \in [root(s)]_R$, $C \subseteq B$ and $B \cap NextEntry_R(p) \neq \emptyset$: Then $p \in [NIL_g]_{R_g}$ or $p \in [root(s)]_{R_s}$. Clearly, $B \cap NextEntry_R(p) \subseteq [root(s)]_{R_s}$, no state from $[NIL]_{R_g}$ can be an entry of p. Therefore, $Prob_R(p, \tau^*\hat{a}, C) = Prob_R(p, \tau^*\hat{a}, C \cap [root(s)]_{R_s})$.

4.1 If $p \in [NIL_g]_{R_g}$ then by use of Lemma 6.4.12 we obtain:
$Prob_R(p, \tau^*\hat{a}, C \cap [root(s)]_{R_s})$
$= Prob_R(p, \tau^*, root(s)) \cdot Prob_R(root(s), \tau^*\hat{a}, C \cap [root(s)]_{R_s})$
$= Prob_{R_g}(p, \tau^*, NIL_g) \cdot Prob_{R_s}(root(s), \tau^*\hat{a}, C \cap [root(s)]_{R_s})$
$= Prob_{R_s}(root(s), \tau^*\hat{a}, C \cap [root(s)]_{R_s})$,
since $Prob_{R_g}(p, \tau^*, NIL_g) = 1$ by Proposition 6.5.12 (it is the case with graph $g_2 \cdot s_3$ in Figure 6.9 if $p \equiv e$);

4.2 If $p \in [root(s)]_{R_s}$ then the result is trivial because
$Prob_R(p, \tau^*a, C \cap [root(s)]_{R_s}) = Prob_{R_s}(p, \tau^*a, C \cap [root(s)]_{R_s})$. (For instance $g_2 \cdot s_3$ in Figure 6.9 or $g_3 \cdot s_3$ in Figure 6.10 with $p \equiv u$ and $C = \{e, root_3, u\}$.)

5. if $p \in [root(s)]_R$ and $C \subseteq E$ as E described above: we assume that $C \cap NextEntry_{R_s}(root(s)) \neq \emptyset$; otherwise $Prob_R(p, \tau^*a, C) = 0$. In a similar way as in the previous case, there are two posible situatioins: either $p \in [NIL_g]_{R_g}$ (p is a state of g) or $p \in [root(s)]_{R_s}$ (p is a state of s).

5.1 If $p \in [NIL_g]_{R_g}$ from the definition of $g \cdot s$ every finite path σ from p to C passes through $root(s)$ and like in 4.1 applying Lemma 6.4.12 and Proposition 6.5.12 we obtain:
$Prob_R(p, \tau^*a, C) = Prob_R(p, \tau^*, root(s)) \cdot Prob_R(root(s), \tau^*a, C)$
$= Prob_{R_g}(p, \tau^*, NIL_g) \cdot Prob_{R_s}(root(s), \tau^*a, C)$
$= Prob_{R_s}(root(s), \tau^*a, root(s))$.
(For example $g_2 \cdot s_2$ in Figure 6.9 if $p \equiv e$ and $C = \{v\}$.)

5.2 If $p \in [root(s)]_{R_s}$ then it is straightforward that $Prob_R(p, \tau^*a, C) = Prob_{R_s}(p, \tau^*a, C)$. (For example $g_3 \cdot s_2$ in Figure 6.10 if $p \equiv root_2$ and $C = \{v\}$.)

□

Next we will investigate transformations that arise when the abstraction operator τ_I is applied on a probabilistic graph g on which an equivalence relation R is defined. Our goal is to keep R as an equivalence relation on $\tau_I(g)$, check the way the set of entries transforms and find strong links between the probability measure on g with respect to R and the one on $\tau_I(g)$ also with respect to R. Thus, some properties of $\tau_I(g)$ can be easily derived from certain properties of g.

For that purpose, let us assume that R is an equivalence relation on g which satisfies the conditions 0,1 and 2 from Definition 6.5.6. According to the definition of $\tau_I(g)$, R is an equivalence relation on $\tau_I(g)$ as well (both graphs have the same set of states). Thus, R divides the sets of states of both graphs into the same classes. But, due to the renaming of atomic actions from I into τ, many paths in g containing observable action may become completely or partially internal in $\tau_I(g)$. Thus, inside one equivalence class the possibility of taking an internal path in $\tau_I(g)$ before executing a certain observable action (action from $A \setminus I$) are at least as in g. Then intuitively the probability of reaching a certain state by executing an observable action in $\tau_I(g)$ is at least the probability in g.

For the set of entries we have the following expected result:

Proposition 6.5.17. $Entry_R(\tau_I(g)) \subseteq Entry_R(g)$.

Proof. An entry e of g may become a non-entry in $\tau_I(g)$ if and only if for every entry r of g for which there exists a path $r \stackrel{\tau^*}{\Longrightarrow}_{[r]_R} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} e$ it also holds that $e \in [r]_R$ and $a \in I$. In any other case there is an entry r in g such that either $r \stackrel{\tau^*}{\Longrightarrow}_{[r]_R} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} e$ and $(r, e) \notin R$ or $r \stackrel{\tau^*}{\Longrightarrow}_{[r]_R} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} e$ and $(r, e) \in R$ and $a \in A \setminus I$, e remains an entry of $\tau_I(g)$. □

The next lemma answers the second part of our problem; it states that the probability of reaching a set of states from one entry in $\tau_I(g)$ can be expressed as a function of probabilities with which the same set of states is reached from the same entry in g. As we have already mentioned it may be the case that the probability in $\tau_I(g)$ is a sum of more than one probability in g. But before we formulate the claim, we need to make a few more assumptions. Let us assume that $\tilde{R}$ is an equivalence relation on $Entry_R(g)$ such that $\tilde{R} \subseteq R$ and let $\tilde{R}_I = \tilde{R} \cap Entry_R(\tau_I(g))$. It is obvious that $\tilde{R}$ is a "relaxed" version on $\tilde{R}$ in Definition 6.5.6, but at this point we do not need to have it defined in more restrictive manner. In order to distinguish the probability measure induced by R on g from the probability measure induced also by R on $\tau_I(g)$, the second one will be put subscript R_I instead of R.

Proposition 6.5.18. Let e be an entry in g and an entry in $\tau_I(g)$, C' an $\tilde{R}$ equivalence class in g and C the $\tilde{R}_I$ equivalence class in $\tau_I(g)$ which is obtained from C, that is, $C = C' \cap Entry_{R_I}(\tau_I(g))$. Then, $Prob_R(e, \tau^*\hat{a}, C) = Prob_R(e, \tau^*\hat{a}, C')$ where $a \in A \setminus I$ or if $a = \tau$ then $C \not\subseteq [e]_R$.

Proof. First note that the both probabilities are measured on g but not on $\tau_I(g)$. We only need to prove that the same states are reachable in C' and C.

Let us assume that $c \in C'$ and that there is a path $e \stackrel{\tau^*}{\Longrightarrow}_{[e]_R} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} c$, that is, c is a next entry of e in C' reachable by a action for $a \in A \setminus I$. Then, $e \stackrel{\tau^*}{\Longrightarrow}_{[e]_{R_I}} \cdot \rightsquigarrow \cdot \stackrel{a}{\rightarrow} c$ is a path in $\tau_I(g)$ as well which implies that c is a next entry of e in $\tau_I(g)$ reachable by a action from e. Therefore, $c \in Entry_{R_I}(\tau_I(g))$ and $c \in C$ as well. From here we conclude that the set of finite paths over which $Prob_R(e, \tau^*a, C)$ and $Prob_R(e, \tau^*a, C')$ are taken are the same which implies an equality between these probabilities.

The case when $a = \tau$ can be proved in a similar way because by the assumption C', and therefore C as well, are not subsets of $[e]_R$. Then, doing an observable action a like above, or doing a τ step to a different equivalence class in g does not make any difference in the course of the proof. □

Lemma 6.5.19. Let g, R, $\tilde{R}$ and $\tilde{R}_I$ be defined as above and let p be an entry of $\tau_I(g)$ and C an $\tilde{R}_I$ equivalence class. Then

$$Prob_{R_I}(p, \tau^*a, C) = Prob_R(p, \tau^*a, C') + \sum_{n\geq 1} \sum_{(E_1,\ldots,E_n)} \sum_{(b_1,\ldots,b_n)\in I^n} \sum_{(t_1,\ldots,t_n)} Prob_R(p, \tau^*b_1, t_1) \cdot \Big(\prod_{i\geq 1}^{n-1} Prob_R(t_i, \tau^*b_{i+1}, t_{i+1})\Big) \cdot Prob_R(t_n, \tau^*a, C'), \text{ and}$$

$$Prob_{R_I}(p, \tau^*, C) = Prob_R(p, \tau^*, C') + \sum_{n\geq 1} \sum_{(E_1,\ldots,E_n)} \sum_{(b_1,\ldots,b_n)\in I^n} \sum_{(t_1,\ldots,t_n)} Prob_R(p, \tau^*b_1, t_1) \cdot \Big(\prod_{i\geq 1}^{n-1} Prob_R(t_i, \tau^*b_{i+1}, t_{i+1})\Big) \cdot Prob_R(t_n, \tau^*, C'),$$

where:

- the first sum is taken over all n-tuples of $\tilde{R}$ equivalence classes $(E_1 \ldots, E_n)$ where $E_i \subseteq [p]_R$, $1 \leq i \leq n$

- the third sum is taken over all $n-$tuples $(t_1, \ldots, t_n) \in E_1 \times \ldots \times E_n$ and
- C' is the $\tilde{R}$ equivalence class which contains C.

Proof. We will prove only the first case with traces from $\tau^* a$ for $a \in A \setminus I$. The second case can be proved in a similar way.

Let $\Sigma(p)$ be the set of all finite paths σ in g from p to C which pass only through $[p]_R$ before reaching C and with a trace in $\tau^* a_1 \tau^* a_2 \ldots \tau^* a_k \tau^* a$ for $a_1, a_2 \ldots, a_k \in I$ and $a \in A \setminus I$,

$$\sigma = p \equiv p_0 \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \rightsquigarrow n_0 \stackrel{a_1}{\rightarrow} p_1 \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \rightsquigarrow n_1 \stackrel{a_2}{\rightarrow} p_2 \ldots p_{k-1} \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \rightsquigarrow n_{k-1} \stackrel{a_k}{\rightarrow} p_k \stackrel{\tau^* a}{\Longrightarrow}_{[p]_R} C \in \Sigma(p),$$

with $p_i \in [p]_{R_I}$ for all $i = 0, 1, \ldots, k-1$. According to the definition of $\tau_I(g)$,

$$\tau_I(\sigma) = p \equiv p_0 \stackrel{\tau^*}{\Longrightarrow}_{[p]_{R_I}} p_1 \stackrel{\tau^*}{\Longrightarrow}_{[p]_{R_I}} p_2 \ldots p_{k-1} \stackrel{\tau^*}{\Longrightarrow}_{[p]_{R_I}} p_k \stackrel{\tau^* a}{\Longrightarrow}_{[p]_{R_I}} C = p \stackrel{\tau^*}{\Longrightarrow}_{[p]_{R_I}} p_k \stackrel{\tau^* a}{\Longrightarrow}_{[p]_{R_I}} C$$

is a unique path in $\tau_I(g)$ from p to C going only through $[p]_{R_I}$ before reaching C with a trace in $\tau^* a$ which is induced by σ. Let denote the set of all paths in $\tau_I(g)$ that correspond to the paths in $\Sigma(p)$ by $\Sigma_I(p)$. Then it is clear that $\Sigma(p)$ and $\Sigma_I(p)$ are equivalent sets (there is a bijection between them) and for all pairs of corresponding paths, like σ and $\tau_I(\sigma)$ above, $\mathbf{P}(\sigma) = \mathbf{P}(\tau_I(\sigma))$. And consequently, $Prob_R(\Sigma \uparrow) = Prob_{R_I}(\Sigma_I \uparrow)$.

Now, for $k \geq 1$ we define $\Sigma^k(p) \subseteq \Sigma(p)$ to be the set of all paths in Σ with a trace in $\Omega^k = \bigcup_{(a_1, a_2, \ldots, a_k) \in I^k} \tau^* a_1 \tau^* a_2 \ldots \tau^* a_k \tau^* a$. Then $\Sigma(p) = \bigcup_{k \geq 0} \Sigma^k(p)$ and for any $i, j, i \neq j$, $\Sigma^i(p) \cap \Sigma^j(p) = \emptyset$. Furthermore, $Prob(\Sigma \uparrow) = \sum_{k \geq 0} Prob(\Sigma^k) = \sum_{k \geq 0} Prob_R(p, \Omega^k, C)$. In the rest of the proof we focus on transforming $Prob_R(p, \tau^* a_1 \tau^* a_2 \ldots \tau^* a_k \tau^* a, C)$ for fixed $a_1, \ldots, a_k$. Let $T = \{t \in [p]_R : p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \cdot \rightsquigarrow \cdot \stackrel{a_1}{\rightarrow} t\}$. Then applying Lemma 6.4.12 we obtain:

$$\begin{aligned} Prob_R(p, \tau^* a_1 \tau^* a_2 \ldots \tau^* a_k \tau^* a, C) &= \sum_{t_1 \in T} Prob_R(p, \tau^* a_1, t_1) \cdot Prob_R(t_1, \tau^* a_2 \ldots \tau^* a_k \tau^* a, C) \\ &= \sum_{t_1 \in [p]_R} Prob_R(p, \tau^* a_1, t_1) \cdot Prob(t_1, \tau^* a_2 \ldots \tau^* a_k \tau^* a, C) \end{aligned}$$

because all paths go through $[p]_R$ and for $t_1 \notin T$ the probability is 0. Now, if $Prob_R(p, \tau^* a_1, t_1) > 0$ then there is a path $p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \rightsquigarrow n \stackrel{a_1}{\rightarrow} t_1$ and since $a_1 \neq \tau$ and p is an entry in g follows that t_1 is an entry in g as well. Thus, the sum can be taken only over the entries in $[p]_R$ which exactly gives the union of all $\tilde{R}$ classes $E_1, E_2, \ldots, E_l$ which are subsets of $[p]_R$. Hence, the sum above can be split in the following way:

$$\begin{aligned} &\sum_{t_1 \in [p]_R} Prob_R(p, \tau^* a_1, t_1) \cdot Prob_R(t_1, \tau^* a_2 \ldots \tau^* a_k \tau^* a, C) \\ &= \sum_{i \geq 1}^{l} \sum_{t_1 \in E_i} Prob_R(p, \tau^* a_1, t_1) \cdot Prob_R(t_1, \tau^* a_2 \ldots \tau^* a_k \tau^* a, C). \end{aligned}$$

Next, we expand $Prob_R(t_1, \tau^* a_2 \ldots \tau^* a_k \tau^* a, C)$ in a similar way and obtain:

$$Prob_R(t_1, \tau^* a_2 \ldots \tau^* a_k \tau^* a, C) = \sum_{i \geq 1}^{l} \sum_{t_2 \in E_i} Prob_R(t_1, \tau^* a_2, t_2) \cdot Prob_R(t_2, \tau^* a_3 \ldots \tau^* a_k \tau^* a, C).$$

After k steps and putting everything together and applying Proposition 6.5.18 in the last step we have:

$Prob_R(p, \tau^* a_1 \tau^* a_2 \ldots \tau^* a_k \tau^* a, C)$

$$= \sum_{i_1\geq 1}^{l} \sum_{t_1\in E_{i_1}} Prob_R(p,\tau^*a_1,t_1)\cdot \sum_{i_2\geq 1}^{l} \sum_{t_2\in E_{i_2}} Prob_R(t_1,\tau^*a_2,t_2)\cdot Prob_R(t_2,\tau^*a_3\ldots\tau^*a_k\tau^*a,C)$$

$$= \sum_{(E_{i_1},E_{i_2})} \sum_{(t_1,t_2)\in E_{i_1}\times E_{i_2}} Prob_R(p,\tau^*a_1,t_1) \cdot Prob_R(t_1,\tau^*a_2,t_2) \cdot Prob_R(t_2,\tau^*a_3\ldots\tau^*a_k\tau^*a,C)$$

$$\stackrel{k}{=} \sum_{(E_{i_1},E_{i_2},\ldots,E_{i_k})} \sum_{(t_1,t_2,\ldots,t_k)} Prob_R(p,\tau^*a_1,t_1)\cdot \Big(\prod_{j\geq 1}^{k-1} Prob_R(t_j,\tau^*a_{j+1},t_j)\Big)\cdot Prob_R(t_k,\tau^*a,C)$$

$$= \sum_{(E_{i_1},E_{i_2},\ldots,E_{i_k})} \sum_{(t_1,t_2,\ldots,t_k)} Prob_R(p,\tau^*a_1,t_1)\cdot \Big(\prod_{j\geq 1}^{k-1} Prob_R(t_j,\tau^*a_{j+1},t_j)\Big)\cdot Prob_R(t_k,\tau^*a,C').$$

Finally, if we sum over all $k \geq 1$, which basically means to sum over all Ω^k, and we sum over all elements in Ω^k the second summand of the final result of the claim will be obtained. The first summand $Prob_R(p,\tau^*a,C')$ adds the probability to reach C' from p in g only via τ^* paths (no action from I occurs in these paths). Clearly, these are also path in $\tau_I(g)$ that should be taken into account when $Prob_{R_I}(p,\tau^*a,C)$ is measured. □

Finally, we should obtain similar results for the third operator, $\leftrightarrows_\pi$. Again, if g and s are given probabilistic graphs, but additionally we require them to be root acyclic, and R_g, R_s are equivalence relations on g and s respectively, we try to adjust/combine appropriately these relations into an equivalence relation on $g \leftrightarrows_\pi s$ such that a strong link between the issues of interest (set of entries, set of next entries, probability measure) of g and s on one side and $g \leftrightarrows_\pi s$ on the other side can be established.

For that purpose, let us assume that R_g and R_s are equivalence relations on g and s respectively, which satisfy the conditions 0,1 and 2 from Definition 6.5.6. Moreover, $[root(g)]_{R_g} = \{root(g)\}$ and $[root(s)]_{R_s} = \{root(s)\}$. We define an equivalence relation R on $g \leftrightarrows_\pi s$ in the following way:

$$\begin{array}{ll} & \{C \;:\; C \text{ is an } R_g \text{ equivalence relation on } g \;\&\; C \neq [root(g)]_{R_g}\} \\ \cup & \{C \;:\; C \text{ is an } R_s \text{ equivalence relation on } s \;\&\; C \neq [root(s)]_{R_s}\} \\ \cup & \{\{root(g \leftrightarrows_\pi s)\}\}. \end{array}$$

Shortly we write R instead of $R_{g\leftrightarrows_\pi s}$. From the definition of $g \leftrightarrows_\pi s$ the following result is obtained straightforwardly:

Proposition 6.5.20. $Entry_R(g \leftrightarrows_\pi s) = \big(Entry_{R_g}(g) \cup Entry_{R_s}(s) \cup \{root(g \leftrightarrows_\pi s)\}\big) \setminus \{root(g), root(s)\}$. □

Lemma 6.5.21. R satisfies the requirements 0,1,2 from Definition 6.5.6. □

Lemma 6.5.22. If $p \in Entry_R(g \leftrightarrows_\pi s)$ and C is a subset of an R equivalence class which contains only entries, then $Prob_R(p,\tau^*\hat{a},C)$ can be expressed by means of $Prob_{R_g}(t,\tau^*\hat{a},D)$ and $Prob_{R_s}(u,\tau^*\hat{a},E)$ for D and E subsets of some equivalence classes of R_g and R_s and for some $t \in S_g$ and $u \in S_s$.

Proof. From Proposition 6.5.20 follows that either p is an entry in g, or p is an entry of s or $p \equiv root(g \leftrightarrows_\pi s)$. In the first case if $C \subseteq S_g$ then $Prob_R(p,\tau^*\hat{a},C) = Prob_{R_g}(p,\tau^*\hat{a},C)$; otherwise $Prob_R(p,\tau^*\hat{a},C) = 0$. Similarly, in the second case if $C \subseteq S_s$ then $Prob_R(p,\tau^*\hat{a},C) = Prob_{R_s}(p,\tau^*\hat{a},C)$; otherwise $Prob_R(p,\tau^*\hat{a},C) = 0$. Also, if $p \neq root(r \leftrightarrows_\pi s)$ then $Prob_R(p,\tau^*a,[root(r \leftrightarrows_\pi s)]_R) = 0$.

In the third case let $C \subseteq S_g$. From Proposition 6.4.11 we obtain

$$Prob_R(root(g \leftrightarrows_\pi s),\tau^*\hat{a},C) = \sum_{(l_1,t_1)\in A_\tau\times S} \mathbf{P}(g \leftrightarrows_\pi s,l_1,t_1)\cdot Prob_R(t_1,\tau^*\hat{a}/l_1,C).$$

Since $t_1 \neq root(g \uplus_\pi s)$, $t_1 \in S_g$ or $t_1 \in S_s$. If $t_1 \in S_s$, $Prob_R(t_1, \tau^* \hat{a}, C) = 0$. If $t_1 \in S_g$, $Prob_R(t_1, \tau^* \hat{a}, C) = Prob_{R_g}(t_1, \tau^* \hat{a}, C)$. Moreover, by the definition of $\mathbf{P}$, $\mathbf{P}(g \uplus_\pi s, l_1, t_1) = \pi \cdot \mathbf{P}(g, l_1, t_1) + (1 - \pi) \cdot \mathbf{P}(s, l_1, t_1) = \pi \cdot \mathbf{P}(g, l_1, t_1)$, (because $t_1 \notin S_s$). For $C \subseteq S_s$ we obtain similar equations. Finally, if
$C = [root(g \uplus_\pi s)]_R$, then $Prob_R(root(g \uplus_\pi s), \tau^* a, [root(g \uplus_\pi s)]_R) = 0$ for $a \in A$ and
$Prob_R(root(g \uplus_\pi s), \tau^*, [root(g \uplus_\pi s)]_R) = 1$. □

Proposition 6.5.23. Let g be a fully probabilistic graph. Then $g \leftrightarrows_{prb} \rho(g)$.

Proof. We assume that g is a root cyclic graph, otherwise the result follows from Proposition 6.4.3. Thus, we have that
$g = (S \cup \{NIL\}, Act, \rightsquigarrow, \rightarrow, \mu, root(g))$ and
$\rho(g) = (S' \cup \{NIL\} \cup \{newroot\}, Act, \rightsquigarrow', \rightarrow', \mu', newroot)$
as it states in Definition 6.4.2. Here by $'$ we denote the isomorphism between $S \cup \{NIL\}$ and $S' \cup \{NIL\}$. We define an equivalence relation R on the nodes of g and $\rho(g)$ by the following partition:

$$\{\{root(g), root'(g), newroot\}\} \cup \{\{x, x'\} \ : \ x \in S, x' \in S' \ and \ x \neq root(g)\}.$$

It is easy to prove that R satisfies requirements 0, 1 and 2 from Definition 6.5.6. Then, we know from the definition of $\rho(g)$ that x is entry in g iff x' is entry in $\rho(g)$ for $x \neq root(g)$. Thus we take $\tilde{R}$ to be defined by one of the following partitions:

$$\{\{root(g), root'(g), newroot\}\} \cup \{\{r, r'\} \ : \ r \in S \cap Entry(g) \ and \ r \neq root(g)\} \text{ or}$$
$$\{\{root(g), newroot\}\} \cup \{\{r, r'\} \ : \ r \in S \cap Entry(g) \ and \ r \neq root(g)\}.$$

The only critical point now is to prove that the probability measure of $newroot$ in $\rho(g)$ and the one of $root(g)$ in g are equal. The proof is based on a bijection between the paths in $\rho(g)$ starting in $newroot$ and the paths in g starting in $root(g)$ and hence over the whole path-prefixes contributing to the two probability measures as it is shown in Figure 6.11.

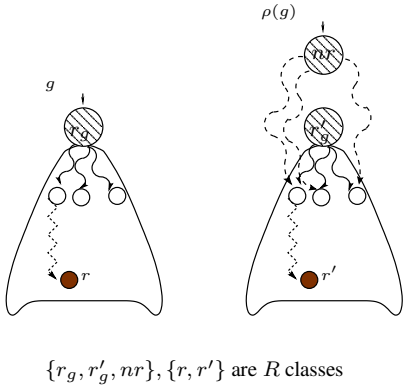


Figure 6.11: Bisimulation between g and $\rho(g)$.

□

Proposition 6.5.24. Let $(R, \tilde{R})$ be a probabilistic branching bisimulation between g and h. If $p, q \in S_g \cup S_h$ and $(p, q) \in \tilde{R}$, then $NextEntryC_{\tilde{R}}(p) = NextEntryC_{\tilde{R}}(q)$.

Proof. Since $(R, \tilde{R})$ is a probabilistic branching bisimulation between g and h and $(p, q) \in R$ for some $p, q \in S_g \cup S_h$ then by the definition of the bisimulation we have:

$\forall C \in NextEntryC_{\tilde{R}}(p) : \forall a \in A :$

$$Prob_{[p]_R}(p, \tau^*, C) = Prob_{[q]_R}(q, \tau^*, C) \text{ and}$$
$$Prob_{[p]_R}(p, \tau^* a, C) = Prob_{[q]_R}(q, \tau^* a, C). \quad (1)$$

And $\forall E \in NextEntryC_{\tilde{R}}(q) : \forall a \in A :$

$$Prob_{[p]_R}(p, \tau^*, E) = Prob_{[q]_R}(q, \tau^*, E) \text{ and}$$
$$Prob_{[p]_R}(p, \tau^* a, E) = Prob_{[q]_R}(q, \tau^* a, E). \quad (2)$$

Let us assume that $C \in NextEntryC_{\tilde{R}}(p)$ (3)

and $C \notin NextEntryC_{\tilde{R}}(q)$. (4)

From (4) we obtain: $\forall c \in C : \forall e \in Exit_R(q) :$

$$\neg \left(\exists a \in A_\tau : e \xrightarrow{a} c \,\&\, c \notin [q]_R \right) \quad (5)$$
$$\& \neg \left(\exists a \in A : e \xrightarrow{a} c \,\&\, c \in [q]_R \right) \quad (6)$$

From (3) we obtain:

$\exists s \in C : \exists e \in Exit_R(p) : \exists a \in A_\tau : e \xrightarrow{a} s \,\&\, s \notin [p]_R$

or $\exists s \in C : \exists e \in Exit_R(p) : \exists a \in A : e \xrightarrow{a} s \,\&\, s \in [p]_R$

from which:

$$\exists s \in C : \exists e \in Exit_R(p) : \exists a \in A_\tau : p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \cdot \rightsquigarrow e \,\&\, e \xrightarrow{a} s \,\&\, s \notin [p]_R \quad (3.1)$$

or $$\exists s \in C : \exists e \in Exit_R(p) : \exists a \in A : p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \cdot \rightsquigarrow e \,\&\, e \xrightarrow{a} s \,\&\, s \in [p]_R \quad (3.2)$$

If $s \notin [p]_R$ then from (3.1) we have:

$\exists \sigma \in Path_{fin,[p]_R}(p, \tau^* a, C) : \sigma \equiv p \stackrel{\tau^*}{\Longrightarrow}_{[p]_R} \rightsquigarrow e \xrightarrow{a} s$, for $a \in A_\tau$, and $\mathbf{P}(\sigma) > 0$ from which $Prob_{[p]_R}(p, \tau^* a, C) > 0$. (7)

And from (5) follows that: $\forall c \in C : \forall e \in Exit_R(q) : \forall a \in A_\tau : q \stackrel{\tau^*}{\Longrightarrow}_{[q]_R} \cdot \rightsquigarrow e \;\Rightarrow\; \neg(e \xrightarrow{a} c)$ that is $Path_{fin,[q]_R}(q, \tau^* a, C) = \emptyset$ and so, $Prob_{[q]_R}(q, \tau^* a, C) = 0$ which together with (7) contradicts (1).

In a similar way we derive that (3.2) and (6) contradict (2). □

Corollary 6.5.25. Let $(R, \tilde{R})$ be a probabilistic branching bisimulation between g and h. If $p \in Entry_R(g)$ then there is a node q in h such that $(p, q) \in \tilde{R}$.

The following proposition expresses that all entries from $[NIL]_R$ form an $\tilde{R}$ equivalence class, and consequently, they all have the same probability measure.

Proposition 6.5.26. Let g and h be a probabilistically branching bisimilar graphs. There is a probabilistic branching bisimulation relation $(R, \tilde{R})$ such that if $e, e' \in Entry_R(g \cup h) \cap [NIL]_R$, then $(e, e') \in \tilde{R}$.

From the definition of $NextEntryC_{\tilde{R}}(p)$ and from Proposition 6.5.24 we can easily conclude that if $(p, q) \in \tilde{R}$, then for any $C \in NextEntryC_{\tilde{R}}(p)$,

$Prob_R(p, \tau^*, C) = Prob_R(q, \tau^*, C) \geq 0$ and $Prob_R(p, \tau^* a, C) = Prob_R(q, \tau^* a, C) \geq 0$.

And for any $\tilde{R}$ equivalence class E which does not belong to $NextEntryC_{\tilde{R}}(p)$, and such that $E \not\subseteq [p]_R$ (and so $E \not\subseteq [q]_R$),

$Prob_R(p, \tau^*, E) = Prob_R(q, \tau^*, E) = 0$ and $Prob_R(p, \tau^* a, E) = Prob_R(q, \tau^* a, E) = 0$, for any $a \in A$.

Thus p and q can have different probabilities $Prob_R(p, \tau^*, E)$ and $Prob_R(q, \tau^*, E)$ only if E is an $\tilde{R}$ equivalence class which is a subset of $[p]_R$ and E is reachable from p only with τ^* paths, hence

$E \notin NextEntryC_{\tilde{R}}(p)$. (See example 6.6.3 where probabilities with which 1 and 4 reach $[2]_{\tilde{R}}$ are different.)

We have obtained results necessary to prove the congruence property of $\underline{\leftrightarrow}_{prb}$ with respect to $\cdot$, τ_I and $\leftthreetimes_\pi$ operators. Actually, the proof can be easily derived from Lemma 6.5.16, 6.5.19 and 6.5.22.

Theorem 6.5.27 (*Congruence theorem*). $\underline{\leftrightarrow}_{prb}$ is a congruence relation on $\mathbf{G}$ with respect to the probabilistic choice operator, the sequential composition and the abstraction operator.

Proof.

Sequential composition. Let $g \underline{\leftrightarrow}_{prb} h$ and $s \underline{\leftrightarrow}_{prb} t$, and let $(R_1, \tilde{R}_1)$ and $(R_2, \tilde{R}_2)$ be probabilistic root branching bisimulations between g and h, and s and t respectively. We define relation R between $g \cdot s$ and $h \cdot t$ on the basis of R_1 and R_2 in the same way it was done on page 203 where $R_{g\cdot s}$ was defined from R_g and R_s.

Furthermore, we define an equivalence relation $\tilde{R}$ on $Entry_R(g\cdot s \cup h\cdot t)$ by the following partition:

$$\begin{array}{ll} & \{C \,:\, C \text{ is an } \tilde{R}_1 \text{ equivalence class } \& \; C \neq [e_{NIL_g}]_{\tilde{R}_1}\} \\ \cup & \{C \,:\, C \text{ is an } \tilde{R}_2 \text{ equivalence class } \& \; C \neq [root(s)]_{\tilde{R}_2}\} \\ \cup & \{([e_{NIL}]_{\tilde{R}_1} \cup [root(s)]_{\tilde{R}_2}) \cap Entry_R(g \cdot s \cup h \cdot t)\}. \end{array}$$

We repeat once again that $[e_{NIL_g}]_{\tilde{R}_1}$ contains all entries from $[NIL_g]_{R_1} = [NIL_h]_{R_1}$ and $[root(s)]_{\tilde{R}_2}$ contains $root(t)$.

That R satisfies the requirement 0,1 and 2 of Definition 6.5.6 follows easily from Lemma 6.5.14. Also it is clear that R satisfies the root condition because R_1 satisfies it by the assumption. We still need to prove the fourth requirement of the definition. From the assumption we know that

- if $(p,q) \in \tilde{R}_1$ and if D is an $\tilde{R}_1$ equivalence class such that $D \in NextEntryC_{\tilde{R}_1}(p)$, then $Prob_{R_1}(p, \tau^*\hat{a}, D) = Prob_{R_1}(q, \tau^*\hat{a}, D)$;

- if $(p,q) \in \tilde{R}_2$ and if E is an $\tilde{R}_2$ equivalence class such that $E \in NextEntryC_{\tilde{R}_2}(p)$, then $Prob_{R_2}(p, \tau^*\hat{a}, E) = Prob_{R_2}(q, \tau^*\hat{a}, E)$.

Then, the result follows easily from Lemma 6.5.16 by which $Prob_R(p, \tau*\hat{a}, C)$ and $Prob_R(q, \tau*\hat{a}, C)$ can be expressed by means of $Prob_{R_1}(p, \tau * \hat{a}, D)$ and/or $Prob_{R_2}(p, \tau * \hat{a}, E)$

Abstraction operator. Let $g \underline{\leftrightarrow}_{prb} h$ and let $(R, \tilde{R})$ be probabilistic root branching bisimulations between g and h. We consider relations $(R_I, \tilde{R}_I)$ where $R_I = R$ and $\tilde{R}_I = \tilde{R} \cap Entry_R(\tau_I(g))$ (the same way we did it on page 208). Clearly, we have to check only the fourth requirement from Definition 6.5.6. From the assumption we know that if $(p,q) \in \tilde{R}$ and if C' is an $\tilde{R}$ equivalence class such that $C' \in NextEntryC_{\tilde{R}}(p)$, then $Prob_R(p, \tau^*a, C') = Prob_R(q, \tau^*a, C')$. (AS)
Let us assume that $(p,q) \in \tilde{R}_I$ and $C \in NextEntryC_{\tilde{R}_I}(p)$. Then, $C \subseteq C'$ for a certain $C \in NextEntryC_{\tilde{R}}(p)$. From Lemma 6.5.19 we have:

$$Prob_{R_I}(p, \tau^*\hat{a}, C) = Prob_R(p, \tau^*a, C') + \sum_{n\geq 1} \sum_{(E_1,\ldots,E_n)} \sum_{(b_1,\ldots,b_n)\in I^n} \sum_{(t_1,\ldots,t_n)} Prob_R(p, \tau^*b_1, t_1) \cdot \Big(\prod_{i\geq 1}^{n-1} Prob_R(t_i, \tau^*b_{i+1}, t_{i+1})\Big) \cdot Prob_R(t_n, \tau^*\hat{a}, C'),$$ where:

- the first sum is taken over all n-tuples of $\tilde{R}$ equivalence classes $(E_1 \ldots, E_n)$ all of them subsets of $[p]_R$,

- the third sum is taken over all $n-$tuples $(t_1,\ldots,t_n)\in E_1\times\ldots\times E_n$.

Because a is an observable action or $a=\tau$ and a-transition enters a new R class, $Prob_R(t_n,\tau^*a,C')>0$ iff $C'\in NextEntryC_{\tilde{R}}(t_n)$. Then, $Prob_R(t,\tau^*a,C')>0$ for all $t\in E_n=[t_n]_{\tilde{R}}$ and from the assumption that (R,R) is a probabilistic branching bisimulation this probability is a constant for any $t\in E_n$ which we will denote by $Prob_R(E_n,\tau^*a,C')$. Similarly, $\sum\limits_{t_{i+1}} Prob_R(t_i,\tau^*b_{i+1},t_{i+1})=Prob_R(t_i,\tau^*b_{i+1},E_{i+1})$ and this is a constant for all $t\in E_i$ which we denote by $Prob_R(E_i,\tau^*b_{i+1},E_{i+1})$. Thus we can transform the expression above into:

$$Prob_{R_I}(p,\tau^*\hat{a},C)=Prob_R(p,\tau^*a,C')+\sum_{n\geq 1}\sum_{(E_1,\ldots,E_n)}\sum_{(b_1,\ldots,b_n)}Prob_R(p,\tau^*b_1,E_1)\cdot(\prod_{i\geq 1}^{n-1}Prob_R(E_i,\tau^*b_{i+1},E_{i+1}))\cdot Prob_R(E_n,\tau^*a,C').$$

The same expression we obtain for $Prob_{R_I}(q,\tau^*\hat{a},C)$ and then the result follows from the assumption (AS).

Probabilistic choice. Let $g\leftrightarrows_{prb}h$ and $s\leftrightarrows_{prb}t$ g, h, s and t and let $(R_1,\tilde{R}_1)$ and $(R_2,\tilde{R}_2)$ be probabilistic root branching bisimulations between $\rho(g)$ and $\rho(h)$, and $\rho(s)$ and $\rho(t)$ respectively such that $\{root(\rho(g)),root(\rho(h))\}$ and $\{root(\rho(s)),root(\rho(t))\}$ form an equivalence class of the relevant relation. We define relation R between $\rho(g)\leftrightarrows_\pi\rho(s)$ and $\rho(h)\leftrightarrows_\pi\rho(t)$ on the basis of R_1 and R_2 in the same way it was done on page 210 where $R_g\leftrightarrows_\pi s$ was defined from R_g and R_s.

Furthermore, we define an equivalence relation $\tilde{R}$ on $Entry_R(\rho(g)\leftrightarrows_\pi\rho(s)\cup\rho(h)\leftrightarrows_\pi\rho(t))$ by the following partition:

$$\begin{array}{ll} & \{C\ :\ C \text{ is an } \tilde{R}_1 \text{ equivalence class } \&\ C\neq[root(\rho(g))]_{\tilde{R}_1}\}\\ \cup & \{C\ :\ C \text{ is an } \tilde{R}_2 \text{ equivalence class } \&\ C\neq[root(\rho(s))]_{\tilde{R}_2}\}\\ \cup & \{\{root(\rho(g)\leftrightarrows_\pi\rho(s)),root(\rho(h)\leftrightarrows_\pi\rho(t))\}\}.\end{array}$$

Thus, the roots of all four graphs are not included, but the new roots are related by $\tilde{R}$. (Do not forget that $[root(\rho(g))]_{\tilde{R}_1}=[root(\rho(h))]_{\tilde{R}_1}=\{root(\rho(g)),root(\rho(h))\}$ and $[root(\rho(s))]_{\tilde{R}_2}=[root(\rho(t))]_{\tilde{R}_2}=\{root(\rho(s)),root(\rho(t))\}$.)

That R satisfies the requirement 0,1 and 2 of Definition 6.5.6 follows easily from Lemma 6.5.21. Also R satisfies the root condition because R_1 and R_2 satisfy it by the assumption. We still need to prove the fourth requirement of the definition. From the assumption we know that

if $(p,q)\in\tilde{R}_1$ and if D is an $\tilde{R}_1$ equivalence class such that $D\in NextEntryC_{\tilde{R}_1}(p)$, then $Prob_{R_1}(p,\tau^*a,D)=Prob_{R_1}(q,\tau^*a,D)$;

if $(p,q)\in\tilde{R}_2$ and if E is an $\tilde{R}_2$ equivalence class such that $E\in NextEntryC_{\tilde{R}_2}(p)$, then $Prob_{R_2}(p,\tau^*a,E)=Prob_{R_2}(q,\tau^*a,E)$.

Then, the result follows easily from Lemma 6.5.22. Thus, we proved that $\rho(g)\leftrightarrows_\pi\rho(s)\leftrightarrows_{prb}\rho(h)\leftrightarrows_\pi\rho(t)$ and therefore, $g\leftrightarrows_\pi s\leftrightarrows_{prb}h\leftrightarrows_\pi t$ according to Definition 6.4.5. □

After we showed that $\leftrightarrows_{prb}$ is congruence we can define the model of *fpBPA*$_\tau$ as stated in the following theorem.

Theorem 6.5.28 (*Soundness theorem*). $\mathbf{G}/\leftrightarrows_{prb}$ is a model of *fpBPA*$_\tau$ +PVR1+PVR2+....

Proof. To prove the result is very easy. For the axioms of *fpBPA* the result follows straightforward from Proposition 6.4.3 *ii.* and Theorem 3.3.37 on page 66.

Soundness of the axioms $TI0$-$TI2$ in Table 6.4 is straightforward. For axioms $TI4$ and $PrTI$ from Definition 6.4.5 follows easily that $(\triangle_S, \triangle_S)$ is the desired probabilistic root branching bisimulation which relates the left-hand side and the right-hand side of the axiom. Here, $\triangle_S$ denotes the identity (diagonal) relation on the set of states of the considered graph. Clearly, if $R = \triangle_S$, then $\tilde{R} = \triangle_S$ as well.

For soundness of axiom $T1$ we need to find a probabilistic root branching between graphs g and $g \cdot \tau$ which have the form as given in Figure 6.12. Obviously, relation R defined by the partition

$$\{\{r, r'\}, \{NIL_g, r_\tau, 1, NIL_{g\cdot\tau}\} \mid r \in S_g \text{ and } r' \text{ is the corresponding state of } r \text{ in } S_{g\cdot\tau}\}$$

satisfies the conditions 0, 1 and 2 from Definition 6.5.6 as well as the root condition. Take $\tilde{R}$ to be the relation defined by the partition

$$\{\{r, r'\}, \{NIL_g, r_\tau, NIL_{g\cdot\tau}\} \mid r \in S_g \text{ and } r' \text{ is the corresponding state of } r \text{ in } S_{g\cdot\tau}\}.$$

To check condition 3 for $\tilde{R}$ is trivial.

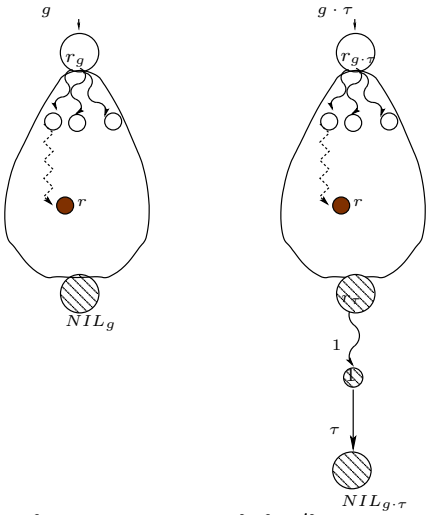


Figure 6.12: Probabilistic graph of $g \cdot \tau$ for a given g.

Finally, we need to prove soundness of the verification rules PVR1, PVR2,.... But, our guiding idea has been to construct such an equivalence relation that relates the processes in the motivating example which are instances of the verification rules (the graphs in Figure 6.5 correspond to $PVR2$). Therefore, we explain once again the way a probabilistic root branching bisimulation can be constructed for PVR3 and for any other rule the construction will be similar.

Let g_1, g_2, g_3, h_1, h_2 and h_3 be fully probabilistic graphs and

$$g_1 \leftrightarrows_{prb} i \cdot g_2 \between_{\pi_1} h_1, \qquad g_2 \leftrightarrows_{prb} i \cdot g_3 \between_{\pi_2} h_2, \qquad g_3 \leftrightarrows_{prb} i \cdot g_1 \between_{\pi_3} h_3,$$

for $i \in I$ and $\pi_1, \pi_2, \pi_3 \in \langle 0, 1\rangle$. According to the Congruence theorem 6.5.27 g_1 is probabilistically bisimilar to the graph shown in Figure 6.13. Again from the Congruence theorem follows that the graphs $\tau \cdot \tau_I(g_1)$ and $\tau \cdot \tau_I(G)$ in Figure 6.14 are probabilistically root branching bisimilar. Thus, we need to construct a probabilistic root branching bisimulation between $\tau \cdot \tau_I(G)$ and $\tau \cdot H$ in the same figure which will conclude the proof. Take R to be the relation defined by the partition

$$\{\{0, 0'\}, \{1, 1'\}, \{2, 2', 3, 4, 5, 6, 7\}\} \cup \{\{s\} \ : \ s \in S_{h_i}, s \neq root(h), i = 1, 2, 3\ \}$$

and $\tilde{R}$ the relation defined by the partition

$$\{\{0,0'\},\{2,2'\}\} \cup \{\{s\} \ : \ s \in S_{h_i}, \text{s is a probabilistic state}, s \neq root(h), i = 1,2,3\ \}.$$

Note that the construction of the probabilistic choice of two graphs guarantees that 2, 3 and 4 are not incoming states for any transitions except for $1 \xrightarrow{\tau} 2$, $5 \xrightarrow{\tau} 3$ and $6 \xrightarrow{\tau} 4$, respectively. It means that these states cannot become entries. Now it is easy to check that $(R, \tilde{R})$ is a probabilistic root branching bisimulation.

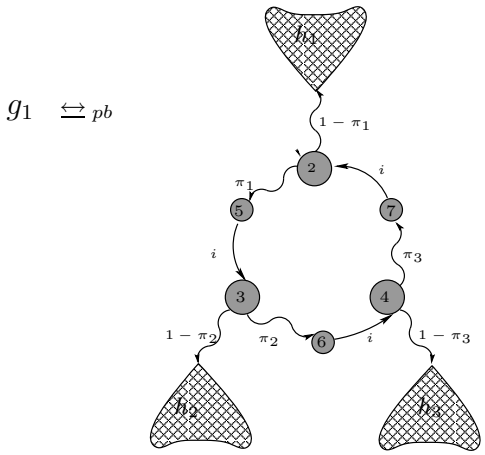


Figure 6.13: Probabilistically root bisimilar graph to g_1.

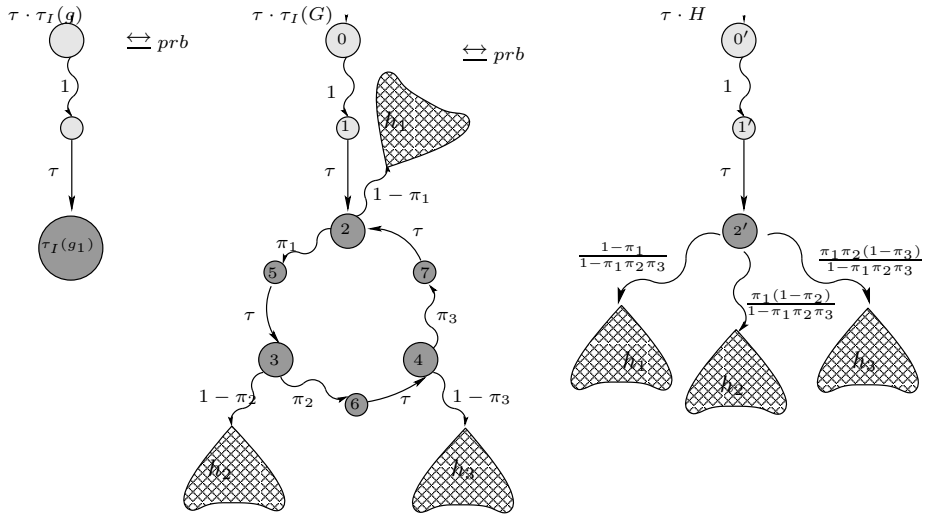


Figure 6.14: Probabilistically root bisimilar graph to $\tau \cdot \tau_I(g_1)$.

□

6.6 Deciding probabilistic branching bisimulation

In this section, we present an algorithm that computes a probabilistic branching bisimulation equivalence relation for given fully probabilistic graphs. The algorithm decides whether the root nodes of

the graphs have the same branching structure and, further, if they have the same probability measures. At the end it returns a pair of relations that relates these graphs if such relations exist.

The basic idea of the algorithm is to start with the coarsest branching bisimulation relation that relates two nodes if and only if they have the same branching structure, regardless of their probability measures. In Definition 6.5.6 one can notice that probabilistic transitions in the part which concerns the branching structure (items 0, 1 and 2) can be viewed as internal transitions. This gives us liberty to employ any algorithm that decides branching bisimulation on non-probabilistic systems. In particular, here we use the algorithm for deciding branching bisimulation equivalence in [64]. The original algorithm is defined on one graph in which case the output is the coarsest branching bisimulation on that graph. The algorithm can slightly be modified into an algorithm that works on a union of two graphs (which is what we need). In this case ($Step1$) the output is either the branching bisimulation equivalence relation R between the two graphs with roots $root_1$ and $root_2$, and it is the input of the second part of our algorithm; or it has found that the two graphs are not branching bisimilar (the root nodes are not R-related) and it returns the empty relation meaning that two graphs are not branching bisimilar. In the latter case the given graphs are not probabilistically branching bisimilar as well ($Step2$). Before the second part is run, the set of entries w.r.t. R is calculated ($Step3$).

The second part of the algorithm is concerned with probabilities. Starting from the R equivalence classes restricted on the entries as the initial value for $\tilde{R}$ ($Step4$, where BB is the partition induced by R), the algorithm refines the $\tilde{R}$ equivalence classes by comparing the probability measures for the nodes belonging to the same class ($Step5$). If it has been established that two or more nodes from the same equivalence class have different probabilities, then it is split into separate subclasses. Finally, if it has been detected that the roots have been split then the algorithm terminates ($Step6$) with the conclusion that the two graphs are not probabilistically bisimilar (returning the pair $(\emptyset, \emptyset)$). Otherwise, the algorithm returns the pair of relations that makes graphs g and h probabilistically branching bisimilar ($Step7$). The crucial point here is the definition of a *splitter*. (Note: many algorithms concerning bisimulation are based on the notion of a splitter defined in an appropriate way for that particular relation.)

Definition 6.6.1. Let g be a fully probabilistic graph and R an equivalence relation on g. Let $\tilde{R}$ be an equivalence relation that is a subset of R and let Π be the partition induced by $\tilde{R}$. A pair (a, C) for $a \in A_\tau$ and $C \in \Pi$ is a splitter of Π if for some $E \in \Pi$ and $p, p' \in E$, if $C \in NextEntryC_\Pi(p)$ or $C \in NextEntryC_\Pi(p')$ then

$$Prob_R(p, \tau^* a, C) \neq Prob_R(p', \tau^* a, C).$$

Thus a splitter (a, C) of a partition Π indicates a class in Π that contains states which prevent (R, Π) from being a probabilistic branching bisimulation. Moreover, it indicates that partition Π has to be refined to Π' in such a way that (a, C) is not a splitter of Π'. And thus, we split the set of entries in finer classes, subsets of corresponding R classes, until we obtain a partition (the $\tilde{R}$ relation) that meets the third requirement in Definition 6.5.6. Formally,

Definition 6.6.2. Let g, R and Π be defined like in the previous definition and let (a, C) be a splitter of Π. If $E \in \Pi$ we define a refinement of E w.r.t. (a, C), $Refine(E, a, C)$, in the following way:

$$Refine(E, a, C) = \{E_n \ : \ n \in N\},$$

for some set of indices N such that

1. $\{E_n \ : \ n \in N\}$ is a partition of E and

2. $\forall n \in N : \forall s,t \in E_n : Prob_R(s,\tau^* a, C) = Prob_R(t,\tau^* a, C)$.
The refinement of Π w.r.t. splitter (a, C) is:

$$Refine(\Pi, a, C) = \bigcup_{E \in \Pi} Refine(E, a, C).$$

The probabilities $Prob_R(p, \tau^* a, C)$ can be computed by solving the linear equation system (see e.g. [28, 29])

$x_p = 1$	if $a = \tau$ and $p \in C$
$x_p = 0$	if $Path_{fin,[p]_R}(p, \tau^* a, C) = \emptyset$
$x_p = \sum_{t \in [p]_R} \mathbf{P}(p,\tau,t) \cdot x_t + \mathbf{P}(p,a,C)$	otherwise

Example 6.6.3. The splitter idea applied to the graphs g and h in Figure 6.4 works in the following way. Take $\tilde{R}_0$ to be induced by the partition $\{\{1,2,4,6\},\{3,5,7\}\}$ (which is the initial value of Π (and therefore of $\tilde{R}$) in the algorithm. By solving the linear equation system we get that $(a, \{3,5,7\})$ is a splitter of Π because $Prob_R(1, \tau^* a, \{3,5,7\}) \neq Prob_R(2, \tau^* a, \{3,5,7\})$. As a result of the next step of refining Π the value of Π is: $\{\{1,4\},\{2,6\},\{3,5,7\}\}$. Again a system of linear equations is solved and since there are no splitters of Π the refining procedure finishes. By this we have found that (R, Π) defines a probabilistic branching bisimulation between g and h, where R is defined in Example 6.5.3. □

The algorithm is given step-by-step in Figure 6.15. The input is given as a union of two graphs g and h with roots: $root_1$ and $root_2$, respectively.

$Input$:	finite fully probabilistic graphs g and h with $(S, \rightsquigarrow, \rightarrow, \mu, root_1, root_2)$
$Output$:	(R, Π) probabilistic branching bisimulation between g and h if it exists $(\emptyset, \emptyset)$ if g and h are not probabilistically branching bisimilar
$Method$:	
$Step1$:	Call the coarsest branching bisimulation relation algorithm for the graphs g and h, and receive R;
$Step2$:	If $R = \emptyset$ then Return $(\emptyset, \emptyset)$;
$Step3$:	Compute the sets: $Entry_R$, $NextEntry_R(r)$;
$Step4$:	$\Pi := \{E \cap Entry_R \ : \ E \in BB\} \setminus \{\emptyset\}$;
$Step5$:	While Π contains a splitter (a, C) do $\Pi := Refine(\Pi, a, C)$;
$Step6$:	If $root_1$ and $root_2$ are not Π-related then Return $(\emptyset, \emptyset)$;
$Step7$:	Return (R, Π).

Figure 6.15: Algorithm for computing probabilistic branching bisimulation.

Lemma 6.6.4. The algorithm can be implemented in polynomial time in the number of states n.

Proof. Let g and h be finite fully probabilistic graphs with n states and m transitions (total number of states and transitions for both graphs).

For the first part of the algorithm, finding the coarsest bisimulation relation we use the algorithm in [64] which has time complexity $\mathcal{O}(n \cdot m)$. In this step the probabilistic transitions are treated as internal transitions. The set of entries with respect to R can be found with a depth first search with the algorithm in [4] (with time complexity $\mathcal{O}(m)$).

The second part of the algorithm consists of solving the system of linear equations and refining the current partition with respect to a found splitter. The test whether $Path_{fin,[p]_R}(p, \tau^* a, C) = \emptyset$ can be done by a reachability analysis of the underlying directed graph. In the worst case we have to repeat the refinement step n times. And in each of them we have to solve a system of linear equations with n variables and n equations which takes $\mathcal{O}(n^{2.8})$ time with the method in [4]. Thus we obtain the time complexity of the second part of the algorithm to be in the worst case $\mathcal{O}(n^{3.8})$.

In total since $m \leq n^2 \cdot |A_\tau|$ we obtain $\mathcal{O}(n^{3.8})$ time complexity of the algorithm. □

Chapter 7

Applications

7.1 Introduction

This chapter presents several examples using the process algebras previously defined. In the first example we give a specification of an unreliable communication channel used in a communication protocol - in this case the PAR protocol. By some additional operators we reduce the specification of the protocol to a process that can be treated by the technique from Chapter 6. In the second section we use the discrete-time algebra from Chapter 5 to capture the timing aspects of the protocol behaviour.

The goal of the third section is not a study of system specification but a discussion over some theoretical aspects regarding verification techniques for concurrent systems that exhibit both probabilistic and non-deterministic behaviour. Mainly, we expose some problems and in some cases the solutions for several questions arising from studying the CABP.

7.2 PAR protocol

In this section, we consider a simple communication protocol called the Positive Acknowledgment with Retransmission (PAR) protocol [104]. The protocol concerns the communication between two processes that cooperate in an asynchronous manner. The communication is carried out via a communication channel which communicates in a synchronous way with two processes to which it is connected. Important properties that one needs to check when considering communication protocols are: 1) data is not duplicated and 2) data is received in the same order it has been sent. If additionally the communication channel is considered to be unreliable, then it is of high importance to prove that no data is lost. This is the case with the PAR protocol where we assume that communication channels connecting two communicating processes are unreliable. For that purpose, the acknowledgment mechanism is used to prevent loss of messages; receiving a correct acknowledgment asserts that the datum sent has been successfully transmitted. The attribute "positive" in the name of the protocol denotes that only one type of acknowledgment is in use (contrary to the ABP, for instance, where two types of acknowledgment are used).

7.2.1 Specification

The protocol is modeled as a composition of five processes (cf. Figure 7.1): a sender process S, which is equipped with a timer T, a receiver R and two communication channels K and L.

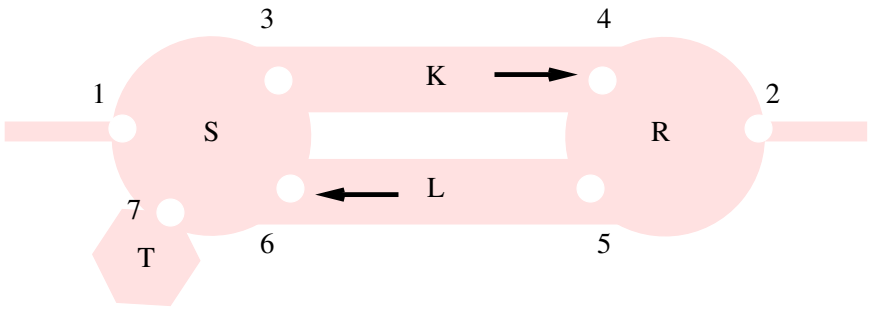


Figure 7.1: Components and connection diagram for the protocol.

The frames that can be transmitted from port 1 to port 2 are of the form (d, b) (db for short) where $d \in D$ for D a *finite* data set and $b \in B = \{0, 1\}$. A control bit $(0, 1)$ is used to avoid duplication of data. The set of atomic actions A contains read, send and communication actions, parametrized by $D \times B \cup \{st, to, ack, \bot\}$, and actions k and l which denote loss of a message and an acknowledgment, respectively. We use the read/send communication function given by $r_p(x) \mid s_p(x) = c_p(x)$ for communication port p and message x. In Figure 7.1, communication ports are $1, 2, 3, 4, 5, 6$ and 7. At the communication port 1 the sender receives a datum from the upper level (host) and at the communication port 2 the receiver sends a datum to the upper level.

Behaviour and specification of the sender After it has received a datum at port 1, the sender sends it to the receiver via a communication channel K through port 3. When the datum is sent the sender starts the timer (action $s_7(st)$) and waits for an acknowledgment before a new datum is transmitted. Due to the unreliable channel, the sender either receives an acknowledgment correctly (action $r_5(ack)$), or something corrupted arrives (action $r_5(\bot)$), or the timer goes off (action $r_7(to)$). In the first case, the sender changes the control bit and fetches the next message. Otherwise, it retransmits the datum.

A recursive specification that specifies the behaviour of the sender is given in Figure 7.2. The following process variables are used: S, SR^b, SS^{db} and SW^{db} for $d \in D$ and $b \in B$. In the equation of SW^{db} we use alternative composition to specify a choice between the possible events. We do it in this way, because SW^{db} behaves as a receiving process that has to accept every possible message sent, and the process itself does not determine the outcome of this choice, nor can its internal behaviour influence this choice.

$$
\begin{array}{lcll}
Sender: & & & \\
\quad S & = & SR^0 & \\
\quad SR^b & = & \sum_{d \in D} r_1(d) \cdot SS^{db} & (b = 0, 1) \\
\quad SS^{db} & = & s_3(db) \cdot s_7(st) \cdot SW^{db} & (b = 0, 1, d \in D) \\
\quad SW^{db} & = & r_5(ack) \cdot SR^{1-b} + (r_5(\bot) + r_7(to)) \cdot SS^{db} & (b = 0, 1, d \in D)
\end{array}
$$

Figure 7.2: Specification of the sender.

Behaviour and specification of the receiver After having received a valid frame, the receiver checks the control bit to find out whether the datum has been received earlier. If not, it accepts it,

writes the message to the output port 2 and sends an acknowledgment to the sender via the channel L (action $s_6(ack)$). Afterwards it changes the control bit. On the receipt of a duplicate (action $r_4(d, 1-b)$) the receiver responds by re-sending the acknowledgment. In case of an invalid message arrival (action $r_4(\bot)$) the receiver just ignores it. The specification of the receiver with process variables R, RW^b, RD^{db}, RA^b, for $b \in B$ is given in Figure 7.3.

$Receiver$:

$$\begin{array}{lcll} R & = & RW^0 & \\ RW^b & = & r_4(\bot) \cdot RW^b + \sum\limits_{d \in D} r_4(d\,1-b) \cdot RA^b + \sum\limits_{d \in D} r_4(db) \cdot RS^{db} & (b = 0, 1) \\ RS^{db} & = & s_2(d) \cdot RA^{1-b} & (b = 0, 1, d \in D) \\ RA^b & = & s_6(ack) \cdot RW^b & (b = 0, 1) \end{array}$$

Figure 7.3: Specification of the receiver.

Specification of the channels If a message or an acknowledgment is transmitted through the (unreliable) channels K or L three scenarios can occur: 1) the message is transmitted correctly, 2) the message is damaged in transit, 3) the message is lost. Unreliability of the channel K (likewise for L) is specified as a probabilistic choice between: correct transmission of a message which occurs with probability π (ρ for L), corruption of a message that occurs with probability σ (η for L) and loss of a message which occurs with probability $1 - \pi - \sigma$ ($1 - \rho - \eta$ for L). The recursive specifications of the channels are given in Figure 7.4.

$Channels$:

$$\begin{array}{lcl} K & = & \sum\limits_{d \in D, b \in \{0,1\}} r_3(db) \cdot K^{db} \\ K^{db} & = & (s_4(db) \mathbin{+\!\!\!+}_\pi s_4(\bot) \mathbin{+\!\!\!+}_\sigma k) \cdot K \\ & & \\ L & = & r_6(ack) \cdot L^a \\ L^a & = & (s_5(ack) \mathbin{+\!\!\!+}_\rho s_5(\bot) \mathbin{+\!\!\!+}_\eta l) \cdot L \end{array}$$

Figure 7.4: Specification of the two channels.

Specification of the timer The timer process is essential for the correct behaviour of the protocol, i.e. it behaves as a one-place buffer. If the message sent or the acknowledgment as been lost in a communication channel, no other action can be performed except the time-out communication action between the timer and the sender. The time-out message directs the sender to send a duplicate of the message. Without a timer it is not possible to detect the loss of a message (datum or acknowledgment). The specification of the timer process, shown in Figure 7.5, is very simple. The sender can reset the timer any time, but a time out can be generated only if the timer has been set already.

As described in [105] a premature time-out can disturb the functioning of the protocol. If an acknowledgment ack_1 is still on the way when a time out occurs prematurely, then the sender retransmits the current frame, say x. When the acknowledgment ack_1 finally arrives, the sender relates it with the frame just sent x and fetches a new datum, say y, without knowing that there is another acknowledgment ack_2 on the way (which in fact acknowledges x). If this acknowledgment arrives correctly,

$Timer$:

$$\begin{aligned} T &= r_7(st) \cdot T^r \\ T^r &= r_7(st) \cdot T^r + s_7(to) \cdot T \end{aligned}$$

Figure 7.5: Specification of the timer.

the sender mistakenly decides that the y has been successfully received and does not retransmits this frame. In case y gets lost in the channel there is no way it might be retrieved. So, the protocol fails.

In order to prevent a premature time-out we follow the concept of priorities used in [105]. By this, the time-out action $c_7(to)$ is given lower priority than every other action, so it is prevented from happening if there is some other alternative.

7.2.2 Priorities and priority operator

Priorities in process algebra are introduced for the first time in [12] as a mechanism for process interruption. *ACP* was extended with a unary priority operator Θ and an auxiliary binary operator $\triangleleft$ (unless operator). The priority operator is parametrized by a partial order $<$ on the set of atomic actions A. Priorities over atomic actions play a role only between alternatives (in alternative composition) whose initial actions are related by $<$. If there are two alternatives $a \cdot x$ and $b \cdot y$, and if $a < b$ the summand $a \cdot x$ cannot proceed (it is blocked by $b \cdot y$) because it has lower priority than $b \cdot y$. If a and b are incomparable then no summand is lost. An auxiliary operator $\triangleleft$ is introduced to obtain a clearer axiomatization of Θ. It "carries out" the information about the ordering $<$ down to the action level. (In case A is finite, there is a finite axiomatization of Θ without auxiliary operators, see [33].)

In this section, we extend *pACP*$^+$ with these two operators; we keep the priority operator and the alternative composition and just add/modify several axioms that include the probabilistic choice. In Table 7.1 and Table 7.2 we give the axioms of the priority operator and axioms of the auxiliary unless operator $\triangleleft$ in the probabilistic setting. Axiom $DyTH3$ is a variant of the $TH3$ axiom in [27]. Again, we restrict the axiom to be applied only on trivial probabilistic processes. This restriction is not necessary but it is done because letting x and y be arbitrary probabilistic processes goes beyond the meaning of the priority operator. In fact, it is difficult to give any logical meaning of the right-hand side of the unless operator if its topmost operator is the probabilistic choice operator. By the constraint in the axiom $DyTH3$ this situation is ruled out. Besides, starting from a term without $\triangleleft$ operator, no term in the form $(x \leftplus_\pi y) \triangleleft z$ can be derived. Hence, no axiom for terms with such a structure is included in Table 7.2.

The priority operator Θ can be eliminated from closed terms in favour of the basic operators of *BPA*$_\delta$. This is not the case with the unless operator. This operator can be eliminated only if both arguments are terms with associated basic terms in $\mathcal{B}_+$. As mentioned earlier, this should not be considered as a problem, because in the specification of processes this operator appears only as an auxiliary operator of the priority operator, and the conditional axiom $DyTH3$ guarantees that its arguments cannot be different from ones the described above.

In the proof of the Elimination theorem of the Θ operator, since we consider the signature of *pACP*$^+$ extended with Θ, we just continue the proof of the Elimination theorem of *pACP*$^+$ (Theorem 4.2.5 on pg. 94) by adding an item in the induction proof about the priority operator. By *pACP*$^+_\Theta$ we denote the axiom system *pACP*$^+ + TH1 + TH2 + DyTH3 + PrTH4 + P1 - 6$. By closed terms of *pACP*$^+_\Theta$ we mean closed terms over the signature of *pACP*$^+$ expanded with Θ only.

Theorem 7.2.1 (*Elimination theorem of the priority operator*). Let p be a closed *pACP*$^+_\Theta$ term. Then there is a closed *pBPA* term q such that *pACP*$^+_\Theta \vdash p = q$.

$\Theta(a)$	=	a	$TH1$
$\Theta(x \cdot y)$	=	$\Theta(x) \cdot \Theta(y)$	$TH2$
$\Theta(x \between_\pi y)$	=	$\Theta(x) \between_\pi \Theta(y)$	$PrTH4$

$$x = x + x, y = y + y \Rightarrow \Theta(x + y) = \Theta(x) \triangleleft y + \Theta(y) \triangleleft x \quad DyTH3$$

Table 7.1: Axioms for the priority operator.

$a \triangleleft b$	=	a	if $\neg(a < b)$	$P1$
$a \triangleleft b$	=	δ	if $a < b$	$P2$
$x \triangleleft (y \cdot z)$	=	$x \triangleleft y$		$P3$
$x \triangleleft (y + z)$	=	$(x \triangleleft y) \triangleleft z$		$P4$
$x \cdot y \triangleleft z$	=	$(x \triangleleft z) \cdot y$		$P5$
$(x + y) \triangleleft z$	=	$(x \triangleleft z) + (y \triangleleft z)$		$P6$

Table 7.2: Axioms for the unless operator.

Proof. (Continuation of the inductive proof of Theorem 4.2.5.) Assume that $p \equiv \Theta(p_1)$ for certain closed $pACP^+_\Theta$ term p_1. By the induction hypothesis there is a closed *pBPA* term q_1 such that $pACP^+_\Theta \vdash p_1 = q_1$. By Theorem 3.2.23 there is a basic term r_1 such that *pBPA* $\vdash q_1 = r_1$. Then also, $pACP^+_\Theta \vdash p_1 = r_1$. By induction on the structure of basic term r_1 we prove that there is a basic term r (which means closed as well) such that $pACP^+_\Theta \vdash \Theta(r_1) = r$ and moreover if $r_1 \in \mathcal{B}_+$ then $r \in \mathcal{B}_+$.

Case $r_1 \equiv a, a \in A_\delta$. Then $pACP^+_\Theta \vdash \Theta(r_1) = \Theta(a) = a$ and a is a basic *pBPA* term and $a \in \mathcal{B}_+$;

Case $r_1 \equiv a \cdot r'_1$, $a \in A_\delta$ *and basic term* r'_1. Then
$pACP^+_\Theta \vdash \Theta(r_1) = \Theta(a \cdot r'_1) = \Theta(a) \cdot \Theta(r'_1) = a \cdot \Theta(r'_1)$. By induction there is a basic term s' such that $pACP^+_\Theta \vdash \Theta(r'_1) = s'$. So, $a \cdot s'$ is a basic term and moreover $a \cdot s' \in \mathcal{B}_+$;

Case $r_1 \equiv r'_1 + r''_1$ *for basic* $\mathcal{B}_+$ *terms* r'_1 *and* r''_1. Then
$pACP^+_\Theta \vdash \Theta(r_1) = \Theta(r'_1 + r''_1) = \Theta(r'_1) \triangleleft r''_1 + \Theta(r''_1) \triangleleft r'_1$. By the induction hypothesis there are basic $\mathcal{B}_+$ terms s' and s'' such that $pACP^+_\Theta \vdash \Theta(r'_1) = s'$ and $pACP^+_\Theta \vdash \Theta(r''_1) = s''$. Therefore,
$pACP^+_\Theta \vdash \Theta(r_1) = s' \triangleleft r''_1 + s'' \triangleleft r'_1$. (1)

By induction on the structure of basic $\mathcal{B}_+$ terms p and q we prove that there is a basic $\mathcal{B}_+$ term z such that $pACP^+_\Theta \vdash p \triangleleft q = z$ and $op(z) \leq op(p)$.

Subcase $p \equiv a$ *and* $q \equiv b$, $a, b \in A_\delta$. The result follows from axioms $P1$ and $P2$;

Subcase $p \equiv a \cdot p'$ *and* $q \equiv b$, $a, b \in A_\delta$ *and some basic term* p'. $pACP^+_\Theta \vdash p \triangleleft q = a \cdot p' \triangleleft b = (a \triangleleft b) \cdot p' = c \cdot p'$ for $c \in A_\delta$ which is determined by axioms $P1$ and $P2$. Moreover $c \cdot p'$ is a basic $\mathcal{B}_+$ term and $op(c \cdot p') \leq op(p)$;

Subcase $p \equiv p' + p''$ *and* $q \equiv b$, $b \in A_\delta$ *and* p' *and* p'' *basic* $\mathcal{B}_+$ *terms.* Using axiom $P6$ we obtain

$pACP^+_\Theta \vdash p \lhd q = (p' + p'') \lhd b = (p' \lhd b) + (p'' \lhd b)$. By the induction hypothesis there are basic $\mathcal{B}_+$ terms z' and z'' such that $pACP^+_\Theta \vdash p' \lhd b = z'$, $pACP^+_\Theta \vdash p'' \lhd b = z''$ and $op(z') \leq op(p')$ and $op(z'') \leq op(p'')$. Thus $pACP^+_\Theta \vdash p \lhd b = z' + z''$ and $z' + z''$ is a basic $\mathcal{B}_+$ term and $op(z' + z'') \leq op(p)$;

Subcase $q \equiv b \cdot q'$, $b \in A_\delta$, q' *a basic term and* $p \in \mathcal{B}_+$. Using axiom $P3$ we get: $pACP^+_\Theta \vdash p \lhd q = p \lhd (b \cdot q') = p \lhd b$ and the result follows from the previous three cases.

Subcase $q \equiv q' + q''$, q' *and* q'' *are basic terms and* $p \in \mathcal{B}_+$. Using axiom $P4$ we obtain: $pACP^+_\Theta \vdash p \lhd q = p \lhd (q' + q'') = (p \lhd q') \lhd q''$. By the induction hypothesis we have that there is a basic $\mathcal{B}_+$ term z' such that $pACP^+_\Theta \vdash p \lhd q' = z'$ and $op(z') \leq op(p)$. Now we are allowed to use the induction hypothesis again and we obtain that there is a basic $\mathcal{B}_+$ term z'' such that $pACP^+_\Theta \vdash z' \lhd q'' = z''$ and $op(z'') \leq op(z')$. Thus we obtain $pACP^+_\Theta \vdash p \lhd q = z''$ and $op(z'') \leq op(p)$.

This result now can be applied on (1). Therefore, there are basic $\mathcal{B}_+$ terms s_1 and s_2 such that $pACP^+_\Theta \vdash s' \lhd r_1'' = s_1$ and $pACP^+_\Theta \vdash s'' \lhd r_1' = s_2$. Hence, $pACP^+_\Theta \vdash \Theta(r_1) = s_1 + s_2$ and $s_1 + s_2$ is a basic $\mathcal{B}_+$ term;

Case $r_1 \equiv r_1' \leftplus_\pi r_1''$ *for basic terms* r_1' *and* r_1'' *and* $\pi \in \langle 0, 1 \rangle$. Then $pACP^+_\Theta \vdash \Theta(r_1) = \Theta(r_1' \leftplus_\pi r_1'') = \Theta(r_1') \leftplus_\pi \Theta(r_1'')$. By the induction hypothesis there are basic terms s' and s'' such that $pACP^+_\Theta \vdash \Theta(r_1') = s'$ and $pACP^+_\Theta \vdash \Theta(r_1'') = s''$. Therefore, $pACP^+_\Theta \vdash \Theta(r_1) = s' \leftplus_\pi s''$ and $s' \leftplus_\pi s''$ is a basic term.

□

The operational semantics for the added operators is defined by the deduction rules in Table 7.3 and 7.4. Without going into details we claim that:

1. the semantics of $pACP^+$ extended with Θ and $\lhd$ operators including the deduction rules in Table 7.3 and 7.4 constitutes a model of $pACP^+_\Theta$;

2. The operational semantics of $pACP^+_\Theta$ is an operational conservative extension of the operational semantics of $pACP^+$ (with respect to probabilistic strong bisimulation);

3. $pACP^+_\Theta$ is a equational conservative extension of $pACP^+$;

4. The completeness property holds for all closed terms of $pACP^+_\Theta$ that do not contain the $\lhd$ operator.

$$\frac{p \rightsquigarrow x}{\Theta(p) \rightsquigarrow \Theta(x)}$$

$$\frac{x \xrightarrow{a} p, \text{ and for all } b > a.\ x \overset{b}{\not\rightarrow}}{\Theta(x) \xrightarrow{a} \Theta(p)} \qquad \frac{x \xrightarrow{a} \surd, \text{ and for all } b > a.\ x \overset{b}{\not\rightarrow}}{\Theta(x) \xrightarrow{a} \surd}$$

Table 7.3: Deduction rules for the priority operator.

$$\frac{p \rightsquigarrow x}{p \lhd q \rightsquigarrow x \lhd q}$$

$$\frac{x \xrightarrow{a} p, \text{ and for all } b > a.\ x \overset{b}{\not\rightarrow}}{x \lhd q \xrightarrow{a} p} \qquad \frac{x \xrightarrow{a} \surd, \text{ and for all } b > a.\ x \overset{b}{\not\rightarrow}}{x \lhd q \xrightarrow{a} \surd}$$

Table 7.4: Deduction rules for the unless operator.

7.2.3 Verification

Premature time-outs are prevented by giving $c_7(to)$ a lower priority than any other action. Hence, on the set of atomic actions A the following partial ordering is defined:

1. $a < c_7(st)$, for each $a \in A \setminus \{c_7(st)\}$;
2. $c_7(to) < a$, for each $a \in A \setminus \{c_7(to)\}$.

By giving $c_7(st)$ a higher priority than the other actions we express that immediately after sending a message the timer is started. This assumption is very realistic because in such a system a communication between the sender and the timer is usually faster than a communication between other processes in the system. In any case, it is not essential for the correctness of the protocol.

The behaviour of the protocol is obtained by composition of the five processes:

$$PAR = \tau_I \circ \Theta \circ \partial_H(S \parallel T \parallel K \parallel L \parallel R),$$

where

- $H = \{r_i(x), s_i(x) \ : \ 2 \leq i \leq 7, x \in (D \times B) \cup \{ack, \bot, st, to\}\}$ is the set of encapsulated atomic actions and
- $I = \{c_i(x) | i \in \{3, 4, 5, 6, 7\}, x \in (D \times B) \cup \{ack, \bot, st, to\}\} \cup \{k, l\}$.

We need to prove that:

$$PAR = \sum_{d \in D} r_1(d) \cdot s_2(d) \cdot PAR.$$

In the first part of the proof we linearize the expression $\Theta \circ \partial_H(S \parallel T \parallel K \parallel R \parallel L)$ using the axioms of ***pACP***$^+$ and eliminate every occurrence of $\parallel$ operator. As a result a guarded recursive specification is obtained with the root variable $[S \parallel T \parallel K \parallel R \parallel L]$. $[X]$ is used as an abbreviation of $\Theta \circ \partial_H(X)$. The graphical representation of the process is given in Figure 7.7. (How to read the graph: we omit probabilistic transitions labelled with probability 1 - trivial probabilistic transitions. The black notes represent non-probabilistic states, and the white nodes represent probabilistic states.)

Directly from the equations we obtain:

$$\begin{array}{rcl} [SS^{db} \parallel T \parallel K \parallel RW^b \parallel L] & = & [SS^{db} \parallel T^r \parallel K \parallel RW^b \parallel L], \\ [SR^b \parallel T \parallel K \parallel RW^b \parallel L] & = & [SR^b \parallel T^r \parallel K \parallel RW^b \parallel L], \\ [SS^{db} \parallel T \parallel K \parallel RW^{1-b} \parallel L] & = & [SS^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L]. \end{array}$$

In short, we will describe how some occurrences of the alternative composition operator have been eliminated in the derivation of the recursive specification in Figure 7.6. First of all, the alternative composition operators which are obtained by applying conditional axiom $PrMM4$ are eliminated by using the encapsulation operator. Secondly, by merge of terms whose initial actions are

$$
\begin{array}{lcl}
[S \parallel T \parallel K \parallel R \parallel L] & = & [SR^0 \parallel T \parallel K \parallel RW^0 \parallel L] \\
\left[SR^b \parallel T \parallel K \parallel RW^b \parallel L\right] & = & \sum\limits_{d \in D} r_1(d) \cdot \left[SS^{db} \parallel T \parallel K \parallel RW^b \parallel L\right] \\
\left[SS^{db} \parallel T \parallel K \parallel RW^b \parallel L\right] & = & c_3(db) \cdot c_7(st) \cdot \left[SW^{db} \parallel T^r \parallel K^{db} \parallel RW^b \parallel L\right] \\
\left[SW^{db} \parallel T^r \parallel K^{db} \parallel RW^b \parallel L\right] & = & c_4(db) \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RS^{db} \parallel L\right] \between_{\pi} \\
 & & c_4(\bot) \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RW^b \parallel L\right] \between_{\sigma} \\
 & & k \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RW^b \parallel L\right] \\
\left[SW^{db} \parallel T^r \parallel K \parallel RS^{db} \parallel L\right] & = & s_2(d) \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RA^{1-b} \parallel L\right] \\
\left[SW^{db} \parallel T^r \parallel K \parallel RW^b \parallel L\right] & = & c_7(to) \cdot \left[SS^{db} \parallel T \parallel K \parallel RW^b \parallel L\right] \\
\left[SW^{db} \parallel T^r \parallel K \parallel RA^{1-b} \parallel L\right] & = & c_6(ack) \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L^a\right] \\
\left[SW^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L^a\right] & = & c_5(ack) \cdot \left[SR^{1-b} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L\right] \between_{\rho} \\
 & & c_5(\bot) \cdot \left[SS^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L\right] \between_{\eta} \\
 & & l \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L\right] \\
\left[SS^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L\right] & = & c_3(db) \cdot c_7(st) \cdot \left[SW^{db} \parallel T^r \parallel K^{db} \parallel RW^{1-b} \parallel L\right] \\
\left[SW^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L\right] & = & c_7(st) \cdot \left[SS^{db} \parallel T \parallel K \parallel RW^{1-b} \parallel L\right] \\
\left[SW^{db} \parallel T^r \parallel K^{db} \parallel RW^{1-b} \parallel L\right] & = & c_4(db) \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RA^{1-b} \parallel L\right] \between_{\pi} \\
 & & c_4(\bot) \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L\right] \between_{\sigma} \\
 & & k \cdot \left[SW^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L\right] \\
\left[SS^{db} \parallel T \parallel K \parallel RW^{1-b} \parallel L\right] & = & c_3(db) \cdot c_7(st) \cdot \left[SW^{db} \parallel T^r \parallel K^{db} \parallel RW^{1-b} \parallel L\right] \\
\left[SR^b \parallel T^r \parallel K \parallel RW^b \parallel L\right] & = & \sum\limits_{d \in D} r_1(d) \cdot \left[SS^{db} \parallel T^r \parallel K \parallel RW^b \parallel L\right] \\
\left[SS^{db} \parallel T^r \parallel K \parallel RW^b \parallel L\right] & = & c_3(db) \cdot c_7(st) \cdot \left[SW^{db} \parallel T^r \parallel K^{db} \parallel RW^b \parallel L\right]
\end{array}
$$

Figure 7.6: Recursive specification of process.

not encapsulated, two sub-terms containing alternative composition operator are obtained. Firstly, we obtain the following sub-term: $c_7(st) \cdot Q + (c_4(db) \cdot X \between_{\pi} c_4(\bot) \cdot Y \between_{\sigma} k \cdot Y)$, for some processes variables Q, X and Y. Applying the distribution laws and the axioms of the Θ operator on this term and taking into account the partial ordering of the set of atomic actions, we obtain that $\Theta(c_7(st) \cdot Q + (c_4(db) \cdot X \between_{\pi} c_4(\bot) \cdot Y \between_{\sigma} k \cdot Y)) = c_7(st) \cdot \Theta(Q)$. (This situation corresponds to the state of the system in which in parallel the timer might be started or the message might be delivered to the receiver and as a result of the interleaving model non-determinism occurs. Under the assumption that the timer is started immediately after sending the message from the sender, it follows that *this non-deterministic choice actually is deterministic*[1].

In the second situation we obtain a non-deterministic choice between two processes, one represented by term $c_7(to) \cdot R$ and another process which we denote by term P that has the form $a \cdot Z \between_{\rho} b \cdot U \between_{\eta} c \cdot V$ or $a \cdot Z$ for certain processes variables R, Z, U, V and atomic actions a, b and c. (There are more variants where non-determinism with $c_7(to) \cdot R$ occurs and we consider all of them in general.) Again, using the axioms of Θ operator and axioms of *pACP*$^+$ and the partial ordering defined on the set A we obtain that $\Theta(c_7(to) \cdot R + P) = \Theta(P)$ and P does not have non-deterministic choice.

The only alternative composition operator left in the specification is $\sum_{d \in D} r_1(d)$, i.e. reading a datum $d \in D$ at the port 1. To make the verification of the protocol formally right we have to assume that D is a singleton. In this case the recursive specification in Figure 7.6 represents a fully probabilistic process. Then, it is a specification in *fpBPA* and the τ_I operator can be applied on it in

[1] A different choice for the partial order on atomic actions might have resulted in a process with non-determinism, such that abstraction cannot be applied.

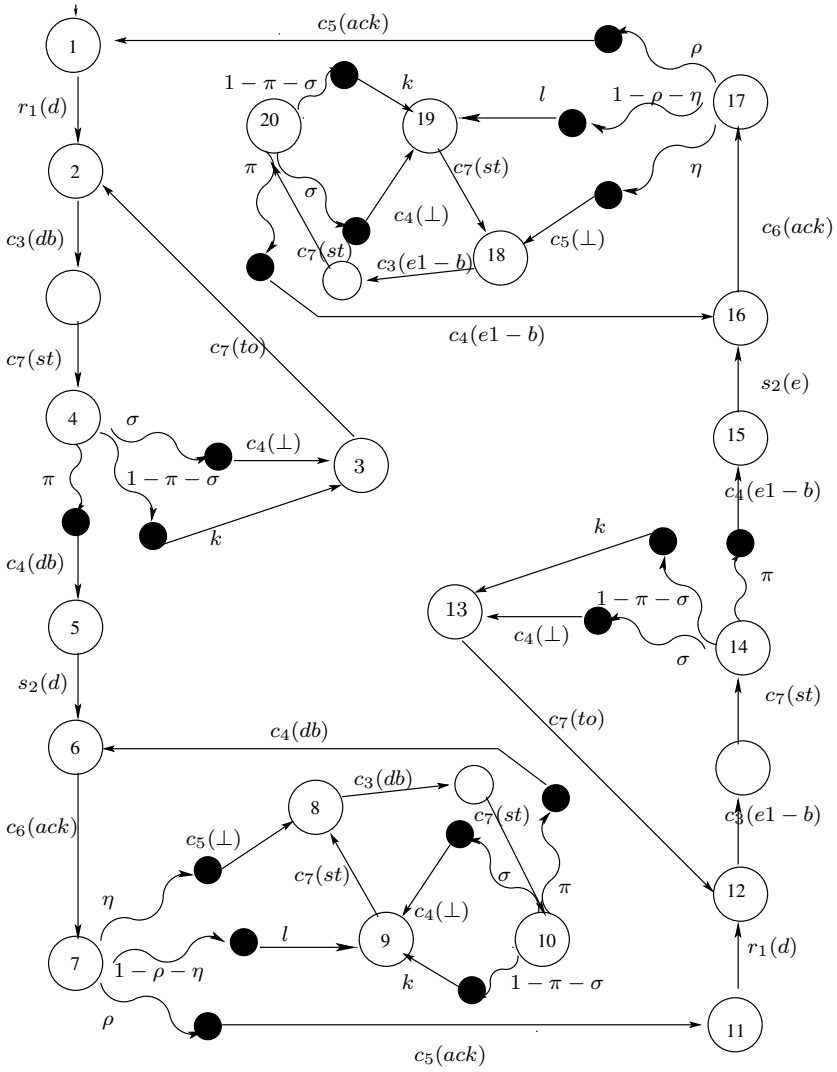


Figure 7.7: Process described by the specification in Figure7.6

$$
\begin{array}{lcllcl}
Y & = & Y_1^0 & & & \\
Y_1^b & = & \sum_{d\in D} r_1(d)\cdot Y_2^{db} & Y_5^{db} & = & c_6(ack)\cdot Y_6^{db} \\
Y_2^{db} & = & c_3(db)\cdot Y_3^{db} & Y_6^{db} & = & \tau\cdot Y_7^{db} \leftthreetimes_{1-\rho} \tau\cdot Y_1^{1-b} \\
Y_3^{db} & = & \tau\cdot Y_2^{db} \leftthreetimes_{1-\pi} c_4(db)\cdot Y_4^{db} & Y_7^{db} & = & c_3(db)\cdot Y_8^{db} \\
Y_4^{db} & = & s_2(d)\cdot Y_5^{db} & Y_8^{db} & = & c_4(db)\cdot Y_5^{db} \leftthreetimes_{\pi} \tau\cdot Y_7^{db}
\end{array}
$$

Figure 7.8: Recursive specification after first abstraction step.

order to rename actions from I into τ. This will be done in three steps. (Here we use the property of the abstraction operator which expresses that $\tau_I \circ \tau_K = \tau_{I\cup K}$ for disjoint sets of atomic actions I and K.) Each step reduces the recursive specification from the previous step to a simpler guarded recursive specification on which some verification rule can be applied. In the last step we apply the RSP principle. However, as one can notice from the verification proof that follows, the alternative composition in the form of $\sum_{d\in D} r_1(d)$, for D an arbitrary finite set, is harmless for the correctness of the proof. After a datum is received a non-deterministic state is not reached till the cycle is finished; in the Figure 7.7 this reads as: the process shows probabilistic behaviour from the state 2 till reaching the state 11. When process is in state 11 it receives a new datum and continues with its probabilistic behaviour. For this reasons, we do not remove the expression $\sum_{d\in D} r_1(d)$ from the specifications that follow, even we know that this makes the verification proof slightly imprecise.

First abstraction We take: $I' = \{c_5(x) \ : \ x \in D\times B\} \cup \{c_7(st), c_7(to), c_4(\bot), c_5(\bot), k, l\}$. Applying axiom $x = x\cdot\tau$ we obtain:
$\tau_{I'}(SW^{db} \parallel T^r \parallel K \parallel RW^b \parallel L) = \tau\cdot\tau_{I'}(SS^{db} \parallel T \parallel K \parallel RW^b \parallel L)$ and
$\tau_{I'}(SW^{db} \parallel T^r \parallel K \parallel RW^{1-b} \parallel L) = \tau\cdot\tau_{I'}(SS^{db} \parallel T \parallel K \parallel RW^{1-b} \parallel L)$.
We derive a new guarded recursive specification given in Figure 7.8 from the recursive specification in Figure 7.6.

Second abstraction Next we take: $I'' = \{c_4(x), c_3(x) \ : \ x \in D\times B\}$. For D a singleton and a fixed b we apply $PVR1_2$ on the equations for Y_2^{db} and Y_3^{db} and obtain:

$$\tau\cdot\tau_{I''}(Y_2^{db}) = \tau\cdot\tau_{I''}(Y_4^{db}).$$

Also, we apply $PVR1_2$ on the equations for Y_7^{db} and Y_8^{db} and obtain:

$$\tau\cdot\tau_{I''}(Y_7^{db}) = \tau\cdot\tau_{I''}(Y_5^{db}).$$

From the recursive specification in Figure 7.8 we obtain a simpler guarded recursive specification given in Figure 7.9.

Third abstraction Finally we take $I''' = \{c_6(ack)\}$. Applying PVR_2 on the equations for Z_3^{db} and Z_4^{db} we obtain:

$$\tau\cdot\tau_{I'''}(Z_3^{db}) = \tau\cdot\tau_{I'''}(Z_1^{1-b}).$$

$$\begin{aligned} Z &= Z_1^0 \\ Z_1^b &= \sum_{d\in D} r_1(d)\cdot Z_2^{db} \\ Z_2^{db} &= s_2(d)\cdot Z_3^{db} \\ Z_3^{db} &= c_6(ack)\cdot Z_4^{db} \\ Z_4^{db} &= \tau\cdot Z_1^{1-b} \trianglelefteq_\rho \tau\cdot Z_3^{db} \end{aligned}$$

Figure 7.9: Recursive specification after the second abstraction.

Therefore,

$$\begin{aligned} \tau_{I'''}(Z_1^b) &= \sum_{d\in D} r_1(d)\cdot \tau_{I'''}(Z_2^{db}) \\ &= \sum_{d\in D} r_1(d)\cdot s_2(d)\cdot \tau_{I'''}(Z_2^{db}) \\ &= \sum_{d\in D} r_1(d)\cdot s_2(d)\cdot \tau_{I'''}(Z_1^{1-b}) \end{aligned}$$

Then from above it follows that:

$$\tau_I(Z_1^0) = \sum_{d\in D} r_1(d)\cdot s_2(d)\cdot \tau_I(Z_1^1)$$

and also

$$\tau_I(Z_1^1) = \sum_{d\in D} r_1(d)\cdot s_2(d)\cdot \tau_I(Z_1^0).$$

According to RSP we obtain $\tau_{I'''}(Z_1^0) = \tau_{I'''}(Z_1^1)$. Hence,

$$\tau_I(Z_1^0) = \sum_{d\in D} r_1(d)\cdot s_2(d)\cdot \tau_I(Z_1^0).$$

□

7.3 PAR protocol in discrete-time model

The PAR protocol described in the previous section shows timing behaviour that in the untimed theory was specified by means of the priority operator parametrized by a partial ordering on the set of atomic actions. With the ability to express quantitatively the timing characteristics of the protocol, the priority operator is not needed when the protocol is considered in timed process theory [44, 23]. Since $pACP^+_{drt}$ is feasible to reason quantitatively about time, the time process T introduced in the untimed specification of the protocol is left out and time-out aspects are integrated in the specification of the sender behaviour. Instead of a time-out action, the sender process is parametrized by T (time-out period) denoting the period of time that it waits for an acknowledgment from the receiver. Thus, the protocol is modeled by four processes: a sender process S, a receiver R and communication channels K and L. The sender receives data from at port 1 and sends it to the receiver via a communication channel K trough port 3. After that, it waits for an acknowledgment from the receiver R (at port 5) before a new datum is transmitted. If an acknowledgment does not occur within period of time T ($T \in \mathbb{N}$), the sender resends the old datum. The receiver receives data from the channel K at port 4 and if the data are undamaged it delivers them to the upper level (at port 2) and sends an acknowledgment to the sender through the channel L (at port 6). A control bit is used in order to avoid multiple

writing of a message at the output port just like in the previous specification. The times d_K and d_L denote the delay through the channels K and L, and d_R denotes the message processing time taken by the receiver. For the correctness of the protocol the duration of the time-out period is of crucial importance. As we will see later, it should be longer than the sum of the delays through the channels and message processing time by the receiver, i.e., $T > d_K + d_L + d_R$.

Again we assume that D is a finite set of data. The set of atomic actions A contains read, send and communication actions and k and l actions which present loss of a message and loss of an acknowledgment, respectively. The read/send communication function given by $r_k(x) \mid s_k(x) = c_k(x)$ for communication port k and message x is used. Unreliability of the channel K is specified by the probabilistic choice operator. The specifications of the four processes are given by the following recursive equations:

$$
\begin{array}{lllll}
Sender: & S & = & SR^0 & \\
 & SR^b & = & \sum_{d\in D} r_1(d)\cdot SS^{db} & (b=0,1, d\in D)\\
 & SS^{db} & = & \underline{\underline{s_3(db)}}\cdot SW^{dbT} & \\
 & SW^{dbT} & = & \underline{\underline{r_5(ack)}}\cdot \sigma_{rel}(SR^{1-b}) + \underline{\underline{r_5(\bot)}}\cdot \sigma_{rel}(SS^{db}) & \\
 & & & + \sum_{t=1}^{T-1} \sigma_{rel}^t(\underline{\underline{r_5(ack)}}\cdot \sigma_{rel}(SR^{1-b})) + \sum_{t=1}^{T-1} \sigma_{rel}^t(\underline{\underline{r_5(\bot)}}\cdot \sigma_{rel}(SS^{db})) + \sigma_{rel}^T(SS^{db}) & \\
Receiver: & R & = & RW^0 & \\
 & RW^b & = & \sum_{d\in D} r_4(db)\cdot RS^{db} + \sum_{d\in D} r_4(d(1-b))\cdot RA^b + r_4(\bot)\cdot RW^b & \\
 & RS^{db} & = & \underline{\underline{s_2(d)}}\cdot \sigma_{rel}^{d_R}(RA^{1-b}) & (d_R\geq 1)\\
 & RA^b & = & \underline{\underline{s_6(ack)}}\cdot \sigma_{rel}(RW^b) & \\
\text{Channels:} & K & = & \sum_{d\in D, b\in\{0,1\}} r_3(db)\cdot \sigma_{rel}^{d_K}(K^{db}) & (d_K\geq 1)\\
 & K^{db} & = & (\underline{\underline{s_4(db)}} \leftthreetimes_\pi \underline{\underline{s_4(\bot)}} \leftthreetimes_\alpha \underline{\underline{k}})\cdot \sigma_{rel}(K) & \\
 & L & = & r_6(ack)\cdot \sigma_{rel}^{d_L}(L^a) & (d_L\geq 1)\\
 & L^a & = & (\underline{\underline{s_5(ack)}} \leftthreetimes_\eta \underline{\underline{s_5(\bot)}} \leftthreetimes_\zeta \underline{\underline{l}})\cdot \sigma_{rel}(L) &
\end{array}
$$

First we expand the term $\partial_H(S \parallel K \parallel L \parallel R)$ which describes the behaviour of the PAR protocol. We take H to be the set of all actions of sending or receiving messages at internal ports: $3, 4, 5$ and 6. $\lceil X \rceil$ is used as abbreviation for $\Theta \circ \partial_H(X)$. The obtained recursive specification is given in Figure 7.10. The graphical representation of the process described by this specification is shown n Figure 7.11. (How to read the graph: we omit trivial probabilistic transitions - transitions labelled with probability 1. The black notes represent non-deterministic states. The gray nodes basically do not represent processes but we use them to separate clearly action transitions from time transitions. Time transitions are denoted by dotted arrows and are labelled by the number of time slices that transitions take. For instance, the transition labelled with d_K that starts in a gray node and ends in the node 3 means that the process represented by state 3 idles d_K time slices.)

In order to obtain the specification in Figure 7.10 we have to assume the following:

1. $d_K \geq 1$, $d_R \geq 1$ and $d_L \geq 1$;

$$
\begin{array}{lcl}
\lceil S \parallel K \parallel R \parallel L \rceil & = & \lceil SR^0 \parallel K \parallel RW^0 \parallel L \rceil \\
\lceil SR^b \parallel K \parallel RW^b \parallel L \rceil & = & \sum_{d \in D} r_1(d) \cdot \lceil SS^{db} \parallel K \parallel RW^b \parallel L \rceil \\
\lceil SS^{db} \parallel K \parallel RW^b \parallel L \rceil & = & \underline{\underline{c_3(db)}} \cdot \sigma_{rel}^{d_K}(\lceil SW^{db(T-d_K)} \parallel K^{db} \parallel RW^b \parallel L \rceil) \\
\lceil SW^{db(T-d_K)} \parallel K^{db} \parallel RW^b \parallel L \rceil & = & \underline{\underline{c_4(db)}} \cdot \lceil SW^{db(T-d_K)} \parallel \sigma_{rel}(K) \parallel RS^{db} \parallel L \rceil \leftthreetimes_\pi \\
 & & \underline{\underline{c_4(\bot)}} \cdot \sigma_{rel}^{T-d_K}(\lceil SS^{db} \parallel T^r \parallel K \parallel RW^b \parallel L \rceil) \leftthreetimes_\alpha \\
 & & \underline{\underline{k}} \cdot \sigma_{rel}^{T-d_K}(\lceil SS^{db} \parallel K \parallel RW^b \parallel L \rceil) \\
\lceil SW^{db(T-d_K)} \parallel \sigma_{rel}(K) \parallel RS^{db} \parallel L \rceil & = & \underline{\underline{s_2(d)}} \cdot \sigma_{rel}^{d_R}(\lceil SW^{db(T-d_K-d_R)} \parallel K \parallel RA^{1-b} \parallel L \rceil) \\
\lceil SW^{db(T-d_K-d_R)} \parallel K \parallel RA^{1-b} \parallel L \rceil & = & \underline{\underline{c_6(ack)}} \cdot \sigma_{rel}^{d_L}(\lceil SW^{dbT'} \parallel K \parallel RW^{1-b} \parallel L^a \rceil) \\
\lceil SW^{dbT'} \parallel K \parallel RW^{1-b} \parallel L^a \rceil & = & \underline{\underline{c_5(ack)}} \cdot \sigma_{rel}(\lceil SR^{1-b} \parallel K \parallel RW^{1-b} \parallel L \rceil) \leftthreetimes_\eta \\
 & & \underline{\underline{c_5(\bot)}} \cdot \sigma_{rel}(\lceil SS^{db} \parallel K \parallel RW^{1-b} \parallel L \rceil) \leftthreetimes_\zeta \\
 & & \underline{\underline{l}} \cdot \sigma_{rel}^{T-d_K-d_R-d_L}(\lceil SS^{db} \parallel K \parallel RW^{1-b} \parallel L \rceil) \\
\lceil SS^{db} \parallel K \parallel RW^{1-b} \parallel L \rceil & = & \underline{\underline{c_3(db)}} \cdot \sigma_{rel}^{d_K}(\lceil SW^{db(T-d_K)} \parallel K^{db} \parallel RW^{1-b} \parallel L \rceil) \\
\lceil SW^{db(T-d_K)} \parallel K^{db} \parallel RW^{1-b} \parallel L \rceil & = & \underline{\underline{c_4(db)}} \cdot \lceil SW^{db(T-d_K)} \parallel \sigma_{rel}(K) \parallel RA^{1-b} \parallel L \rceil \leftthreetimes_\pi \\
 & & \underline{\underline{c_4(\bot)}} \cdot \sigma_{rel}^{T-d_K}(\lceil SS^{db} \parallel K \parallel RW^{1-b} \parallel L \rceil) \leftthreetimes_\sigma \\
 & & \underline{\underline{k}} \cdot \sigma_{rel}^{T-d_K}(\lceil SS^{db} \parallel K \parallel RW^{1-b} \parallel L \rceil) \\
\lceil SW^{db(T-d_K)} \parallel K \parallel RA^{1-b} \parallel L \rceil & = & \underline{\underline{c_6(ack)}} \cdot \sigma_{rel}^{d_L}(\lceil SW^{db} \parallel K^{db} \parallel RW^{1-b} \parallel L^a \rceil) \\
\lceil SW^{db(T-d_K-d_L)} \parallel K \parallel RA^{1-b} \parallel L^a \rceil & = & \underline{\underline{c_5(ack)}} \cdot \sigma_{rel}(\lceil SR^{1-b} \parallel K \parallel RW^{1-b} \parallel L \rceil) \leftthreetimes_\eta \\
 & & \underline{\underline{c_5(\bot)}} \cdot \sigma_{rel}(\lceil SS^{db} \parallel K \parallel RW^{1-b} \parallel L \rceil) \leftthreetimes_\zeta \\
 & & \underline{\underline{l}} \cdot \sigma_{rel}^{T-d_K-d_L}(\lceil SS^{db} \parallel K \parallel RW^{1-b} \parallel L \rceil)
\end{array}
$$

Figure 7.10: Encapsulated parallel composition of the components ($T' = T - d_K - d_R - d_L$).

2. $T > d_K$, otherwise we obtain equality: $\lceil SW^{db(T-d_K)} \parallel K^{db} \parallel RW^b \parallel L \rceil = \underline{\underline{c_4(db)}} \cdot \underline{\underline{\delta}} \leftthreetimes_\pi \underline{\underline{c_4(\bot)}} \cdot \underline{\underline{\delta}} \leftthreetimes_\alpha \underline{\underline{k}} \cdot \underline{\underline{\delta}}$;

3. $T > d_K + d_R$, otherwise we obtain equality: $\lceil SW^{db(T-d_K)} \parallel \sigma_{rel}(K) \parallel RS^{db} \parallel L \rceil = \underline{\underline{s_2(d)}} \cdot \underline{\underline{\delta}}$;

4. $T > d_K + d_R + d_L$, otherwise we obtain equality: $\lceil SW^{db(T-d_K-d_R)} \parallel K \parallel RA^{1-b} \parallel L \rceil = \underline{\underline{c_6(ack)}} \cdot \underline{\underline{\delta}}$.

Assuming that the recursive specification in Figure 7.10 defines a unique process, we can transform it into a simpler specification as given in Figure 7.12

The specification shows that every resending of a message is preceded by a delay (whose length depends on the time slice at which the channel lost the message) in the equation of X_3^{db} the sub-term $\underline{\underline{k}} \cdot \sigma_{rel}^{T-d_K}(X_2^{db})$, in the equation of X_6^{db} the sub-term $\underline{\underline{l}} \cdot \sigma_{rel}^{T-d_K-d_R-d_L}(X_7^{db})$, In the equitation of X_8^{db} the sub-terms $c_4(\bot) \cdot \sigma_{rel}^{T-d_K}(X_7^{db})$ and $\underline{\underline{k}} \cdot \sigma_{rel}^{T-d_K}(X_7^{db})$ and the equation of X_{10}^{db} the sub-term $\underline{\underline{l}} \cdot \sigma_{rel}^{T-d_K-d_L}(X_7^{db})$. Thus, as described above we conclude that if the time-out period $T < d_K + d_R + d_L$ at least one of these subterms becomes $\underline{\underline{\delta}}$ and the process deadlocks; our assumptions are not satisfied. Hence, the protocol does not deadlock iff $T > d_K + d_R + d_L$.

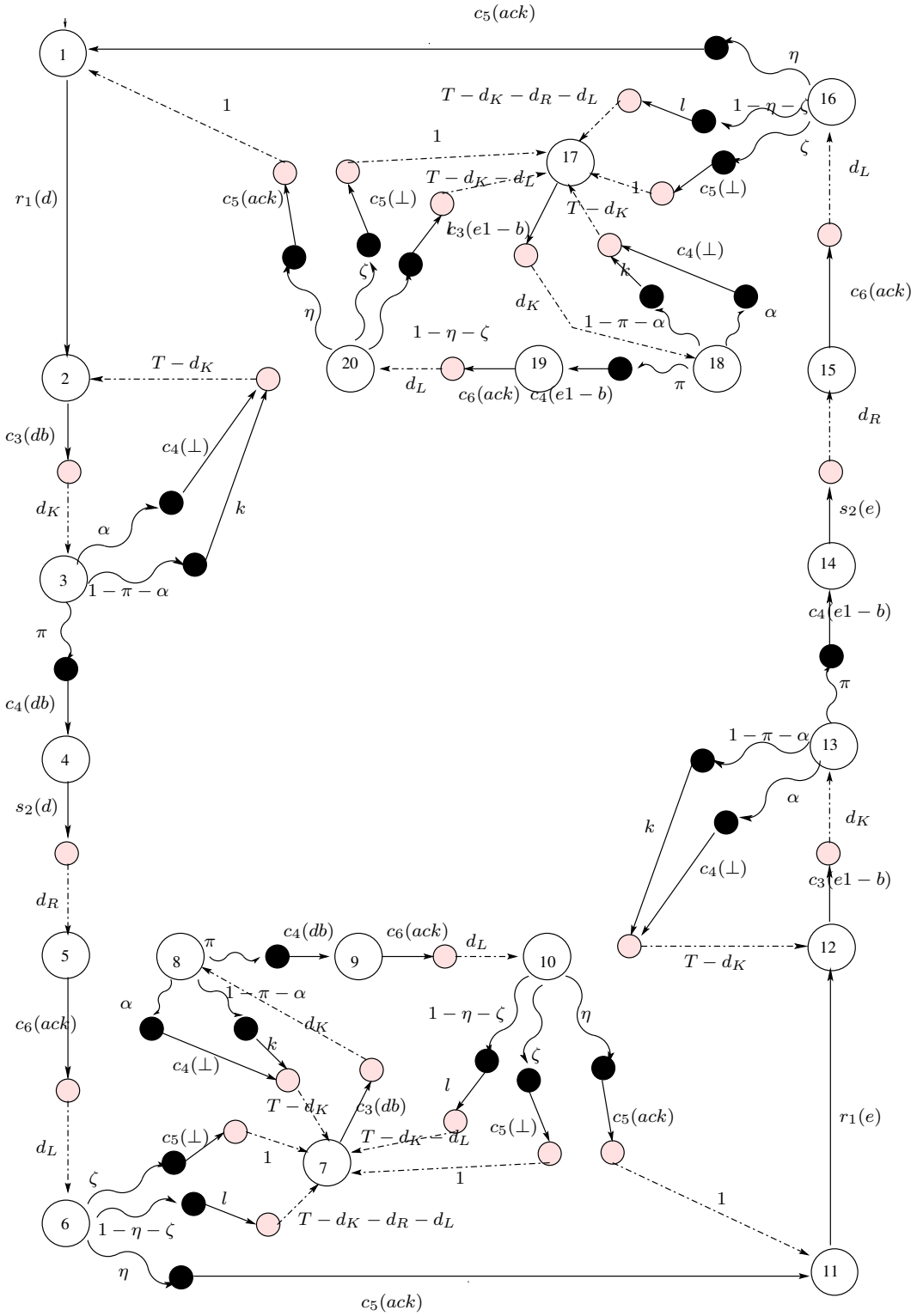


Figure 7.11: Process describe by the specification in Figure 7.10.

$$
\begin{aligned}
X &= X_1^0\\
X_1^b &= \sum_{d\in D} r_1(d)\cdot X_2^{db}\\
X_2^{db} &= \underline{\underline{c_3(db)}}\cdot \sigma_{rel}^{d_K}(X_3^{db})\\
X_3^{db} &= \underline{\underline{c_4(db)}}\cdot X_4^{db} \between_\pi \underline{\underline{c_4(\bot)}}\cdot \sigma_{rel}^{T-d_K}(X_2^{db}) \between_\alpha \underline{\underline{k}}\cdot \sigma_{rel}^{T-d_K}(X_2^{db})\\
X_4^{db} &= \underline{\underline{s_2(d)}}\cdot \sigma_{rel}^{d_R}(X_5^{db})\\
X_5^{db} &= \underline{\underline{c_6(ack)}}\cdot \sigma_{rel}^{d_L}(X_6^{db})\\
X_6^{db} &= \underline{\underline{c_5(ack)}}\cdot \sigma_{rel}(X_1^{(1-b)}) \between_\eta \underline{\underline{c_5(\bot)}}\cdot \sigma_{rel}(X_7^{db}) \between_\zeta \underline{\underline{l}}\cdot \sigma_{rel}^{T-d_K-d_R-d_L}(X_7^{db})\\
X_7^{db} &= \underline{\underline{c_3(db)}}\cdot \sigma_{rel}^{d_K}(X_8^{db})\\
X_8^{db} &= \underline{\underline{c_4(db)}}\cdot X_9^{db} \between_\pi \underline{\underline{c_4(\bot)}}\cdot \sigma_{rel}^{T-d_K}(X_7^{db}) \between_\alpha \underline{\underline{k}}\cdot \sigma_{rel}^{T-d_K}(X_7^{db})\\
X_9^{db} &= \underline{\underline{c_6(ack)}}\cdot \sigma_{rel}^{d_L}(X_{10}^{db})\\
X_{10}^{db} &= \underline{\underline{c_5(ack)}}\cdot \sigma_{rel}(X_1^{1-b}) \between_\eta \underline{\underline{c_5(\bot)}}\cdot \sigma_{rel}(X_7^{db}) \between_\zeta \underline{\underline{l}}\cdot \sigma_{rel}^{T-d_K-d_L}(X_7^{db})
\end{aligned}
$$

Figure 7.12: Specification obtained from the specification in Figure 7.10.

Time abstraction Next, we will show that the protocol behaves as a one-place buffer. But since we do not have a technique to work with internal actions in a timed setting we will derive a time free specification from the one obtained above by using a method called *time abstraction* [42, 23]. It is achieved by the time free projection operator π_{tf} which renames an undelayable action $\underline{\underline{a}}$ into a delayable action a and removes all occurrences of the delay operator σ_{rel}. In fact, π_{tf} embeds $pACP^+_{drt}$ into $pACP^+$ in a way that every delayable action becomes an untimed action. The axioms for π_{tf} operator are shown in Table 7.5 where a ranges over A_δ.

$\pi_{tf}(\underline{\underline{a}})$	=	a	$DRTFP1$
$\pi_{tf}(\sigma_{rel}(x))$	=	$\pi_{tf}(x)$	$DRTFP2$
$\pi_{tf}(x+y)$	=	$\pi_{tf}(x)+\pi_{tf}(y)$	$DRTFP3$
$\pi_{tf}(x\cdot y)$	=	$\pi_{tf}(x)\cdot\pi_{tf}(y)$	$DRTFP4$
$\pi_{tf}(x\between_\rho y)$	=	$\pi_{tf}(x)\between_\rho\pi_{tf}(y)$	$PrDRTFP$

Table 7.5: Axioms for the time free operator.

Back to our specification, the next step is to derive a time free specification $\pi_{tf}(X)$ for X. The recursive specification after the π_{tf} operator is applied on X_i^{db} consists of the following equations:

$$
\begin{aligned}
Y &= Y_1^0\\
Y_1^b &= \sum_{d\in D} r_1(d)\cdot Y_2^{db}\\
Y_2^{db} &= c_3(db)\cdot Y_3^{db}\\
Y_3^{db} &= c_4(db)\cdot Y_4^{db} \between_\pi c_4(\bot)\cdot Y_2^{db} \between_\alpha k\cdot Y_2^{db}\\
Y_4^{db} &= s_2(d)\cdot Y_5^{db}\\
Y_5^{db} &= c_6(ack)\cdot Y_6^{db}\\
Y_6^{db} &= c_5(ack)\cdot Y_1^{d(1-b)} \between_\eta c_5(\bot)\cdot Y_7^{db} \between_\zeta l\cdot Y_7^{db}\\
Y_7^{db} &= c_3(db)\cdot Y_8^{db}\\
Y_8^{db} &= c_4(db)\cdot Y_5^{db} \between_\pi c_4(\bot)\cdot Y_7^{db} \between_\alpha k\cdot Y_7^{db}
\end{aligned}
$$

If we abstract from atomic actions $I' = \{c_4(x), c_5(x) \ : \ x \in D \times B\} \cup \{c_7(st), c_7(to), k, l\}$ exactly the recursive specification (1) on page 230 (with the root variable Y) is obtained. Hence, any further investigation will be superfluous.

7.4 Verification rules - revisited

In this section, we discuss once again the issue of verification rules for probabilistic systems. We believe that the rules we proposed in Chapter 6 can be applied on a large number of real processes . But still, they are not applicable on probabilistic systems that contain non-determinism. Here we will try to answer some questions, but also we will pose some more questions that are still open. So, this section can be seen as some ideas for future research directions.

Basically the initial ideas arose when we did a probabilistic specification of the Concurrent Alternating Bit Protocol (CABP). Since the main intention of this section is to give the reader an insight to our concept of dealing with non-determinism in probabilistic processes, we do not aim to give a complete description of the protocol. We refer the reader to [109] for more details. The CABP is a more complicated variant of the well-known Alternating Bit Protocol (ABP). While in the ABP one a message is sent, and it is not re-transmitted until a "negative" acknowledgment is received (saying that something wrong has happened during the transmission), in the CABP a stream of frames is sent continuously until a positive acknowledgment arrives confirming a correct delivery of the datum sent.

In [109], the protocol is specified by six processes (as shown in Figure 7.13): sender S, receiver R, acknowledgment sender AS, acknowledgment receiver AR and two channels K and L, the first one used to transmit data and the second one used to transmit acknowledgments. The six components are divided into two modules: one module formed by S, K and R and another module consisting of AS, L and AR. In the first module, the stream of frames flows from S to R. The second module contains the stream of acknowledgments from AS to AR. Let us focus on the first module. In Figure 7.14, we give the recursive equations that define the behaviour of these three processes. Our (probabilistic) specification of these processes resembles the specification in [109]. The only difference is the specification of the channel which in our case is modeled by the means of the probabilistic choice operator (as Section 7.2 and 7.3).

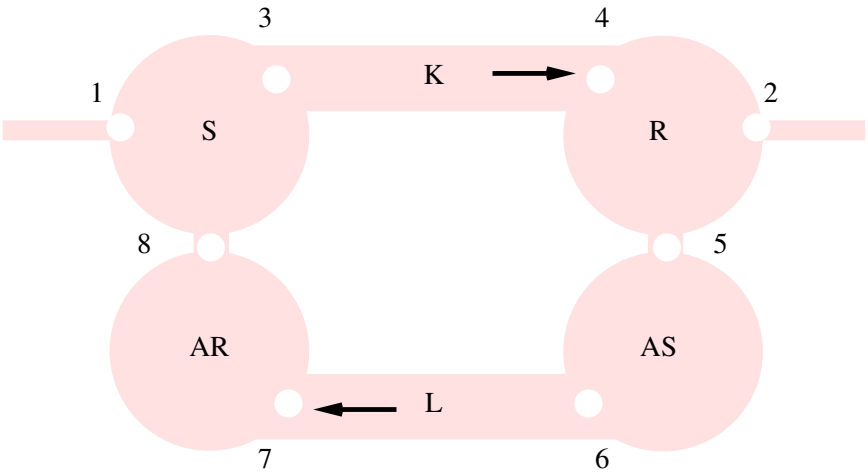


Figure 7.13: Components of the CABP.

$Sender$:

$$\begin{array}{lcll} S & = & RM(0) & \\ RM(b) & = & \sum_{d\in D} r_1(d)\cdot SF(db), & b\in\{0,1\} \\ SF(db) & = & s_3(db)\cdot SF(db)+r_8(ac)\cdot RM(1-b), & db\in D\times\{0,1\} \end{array}$$

$Receiver$:

$$\begin{array}{lcll} R & = & RF(0) & \\ RF(b) & = & \sum_{d\in D} r_4(db)\cdot RS(b) & \\ & & +\sum_{d\in D} r_4(d,1-b)\cdot RF(b) & \\ & & +r_4(\bot)\cdot RF(b), & b\in\{0,1\} \\ RS(b) & = & s_2(d)\cdot s_5(ac)\cdot RF(1-b) & \end{array}$$

$Channel$:

$$\begin{array}{lcll} K_r & = & \sum_{d\in D,b\in\{0,1\}} r_3(db)\cdot K_s(db) & \\ K_s(db) & = & (s_4(db)\between_\pi s_4(\bot)\between_\rho k\,)\cdot K_r, & db\in D\times\{0,1\} \end{array}$$

Figure 7.14: Specification of the sender, the receiver and the channel.

D denotes a finite set of data elements. Communication actions $c_3(db)$, $c_4(db)$ and $c_3(\bot)$ as well as action k are internal actions for this module. Therefore, we take $I=\{c_3(db),c_4(db),c_3(\bot),k\ :\ db\in D\times\{0,1\}\}$. Also we encapsulate send and receive actions and take $H=\{s_3(db),s_4(db),s_3(\bot),r_3(db),r_4(db),r_3(\bot)\ :\ db\in D\times\{0,1\}\}$. Moreover, with a slight modification, the technique introduced in [109] called "language matching" can be adapted for our probabilistic process algebra.

Briefly we describe the idea of the language matching technique. In process specification and verification in process algebra it often happens that a term p has "redundancies in a context $\partial_H(q)(\_\,\|\,q)$". This means that p has certain subterms that are eliminated in the context $\partial_H(q)(\_\,\|\,q)$ due to encapsulation ∂_H. For instance, redundancy can simply occur when some subterms of p are always encapsulated, and they do not communicate with subterms of q. The language matching is a method that is used to find and label possible redundancies at an early stage of a verification. It is used to find and label redundant terms in a given context, given some information about the expected behaviour of the total system in the form of a collection of process traces. The labelling technique used in language matching consists of a mechanism for replacing terms that do not match some given set of traces Z, by a special atomic action r. The language matching operator introduced in [109] is denoted by $\triangle_Z$.

Back to our specification, next, we investigate the following expression:

$$\tau_I\circ\triangle_Z\circ\partial_H(S\,\|\,K\,\|\,R),$$

where Z contains all traces that do not match the language containing concatenation of trace $r_1(d)s_2(d)s_5(ac)r_8(ac)$.

We will not give the complete specification derived for the expression above, but we will point out some equations from the recursive specification that lead us to the desired goal.

Consider parallel composition $SF(db)\,\|\,K\,\|\,RS(b)$. Informally, it corresponds to the moment that a frame has been successfully delivered to R but since S has not received an acknowledgment yet it still can send the same frame to R via K. At the same time S is ready to communicate at port 8 waiting for the acknowledgment. We derive that

$$\triangle_Z\circ\partial_H(SF(db)\,\|\,K\,\|\,RS(b))=r_8(ac)\cdot r+s_2(d)\cdot U+c_3(db)\cdot\triangle_Z\circ\partial_H(SF(db)\,\|\,K_s(db)\,\|\,RS(b)),$$

for some process U not of our interest at this point. r is a process obtained by applying the $\triangle_Z$ operator. Also we consider the parallel composition $SF(db) \parallel K_s(db) \parallel RS(b)$ which corresponds to the situation similar to the one above, with the difference that a frame from S to R is in transit. For this expression we obtain:

$$\begin{aligned}\triangle_Z \circ \partial_H(SF(db) \parallel K_s(db) \parallel RS(b)) \;\; = \;\; r_8(ac) \cdot r \;\; & + s_2(d) \cdot U \\ & + (\delta \leftthreetimes_{\pi+\rho} k) \cdot \triangle_Z \circ \partial_H(SF(db) \parallel K \parallel RS(b))\end{aligned}$$

By abstraction we obtain the following equations:

$$\begin{aligned}&\tau \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K \parallel RS(b)) \\ &\qquad = \tau \cdot \tau_I\Big(r_8(ac) \cdot r + s_2(d) \cdot U + c_3(db) \cdot \triangle_Z \circ \partial_H(SF(db) \parallel K_s(db) \parallel RS(b)\Big) \\ &\qquad = \tau \cdot \Big(r_8(ac) \cdot r + s_2(d) \cdot \tau_I(U) + \tau \cdot \big(r_8(ac) \cdot r + s_2(d) \cdot \tau_I(U) \\ &\qquad\qquad + (\delta \leftthreetimes_{\pi+\rho} \tau) \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K \parallel RS(b))\big)\Big) \\ &\qquad = \tau \cdot (y + \tau \cdot (y + z)),\end{aligned}$$

for $y \equiv r_8(ac) \cdot r + s_2(d) \cdot \tau_I(U)$ and $z \equiv (\delta \leftthreetimes_{\pi+\rho} \tau) \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K \parallel RS(b))$. On the other side, we transform the second expression as:

$$\begin{aligned}&\tau \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K_s(db) \parallel RS(b)) \\ &\qquad = \tau \cdot \Big(r_8(ac) \cdot r + s_2(d) \cdot \tau_I(U) + (\delta \leftthreetimes_{\pi+\rho} \tau) \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K \parallel RS(b)\Big) \\ &\qquad = \tau \cdot (y + z).\end{aligned}$$

To resume, we have obtained that

$$\tau \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K \parallel RS(b)) = \tau \cdot (x + \tau \cdot (x + y))$$

and

$$\tau \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K_s(db) \parallel RS(b)) = \tau \cdot (x + y).$$

We argue that these two processes should be considered equivalent. First, let us note that by our transformation we have reached processes that by their structure resemble the left-side and the right-side expressions of axiom $B2$ (see Chapter 6). Second, consider the processes in Figure 7.15. The left process corresponds to a term $\tau \cdot (y + \tau \cdot (y + (z_1 \leftthreetimes_\pi z_2)))$ and the right one corresponds to $\tau \cdot (y + (z_1 \leftthreetimes_\pi z_2))$, similar to the expression we have obtained above. One can notice that in both processes (after the initial action τ is performed), no matter what activity it does, it always reaches a state in which y can be chosen non-deterministically. On the other side, if y is not performed, then z_1 or z_2 is performed according to the same probability distribution in both processes. This gives us an idea that the axiom $B2$ should hold for probabilistic processes too. However, we have to make one restriction about processes y, namely, it is required to be a trivial static process. Thus, we suggest that in the probabilistic setting we should have the following conditional axiom:

$$y = y + y \Rightarrow x \cdot (\tau \cdot (y + z) + y) = x \cdot (y + z), \qquad (PrB2).$$

Consequently, we obtain that

$$\tau \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K \parallel RS(b)) = \tau \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K_s \parallel RS(b)),$$

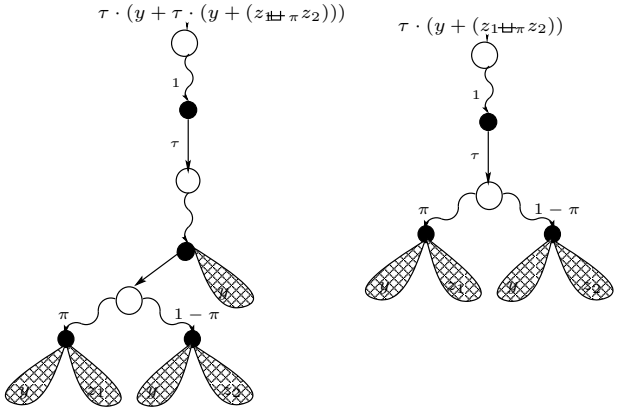


Figure 7.15: Processes that should be related.

that leads us to the conclusion that $\tau \cdot \tau_I \circ \triangle_Z \circ \partial_H(SF(db) \parallel K_s \parallel RS(b))$ is a solution of the following recursive equation:

$$X = \tau \cdot (r_8(ac) \cdot r + s_2(d) \cdot \tau_I(U) + (\delta \leftthreetimes\!\!\sqcup_{\pi+\rho} \tau) \cdot X).$$

If we replace the process $r_8(ac) \cdot r + s_2(d) \cdot \tau_I(U)$ by some arbitrary process, say z, then the left

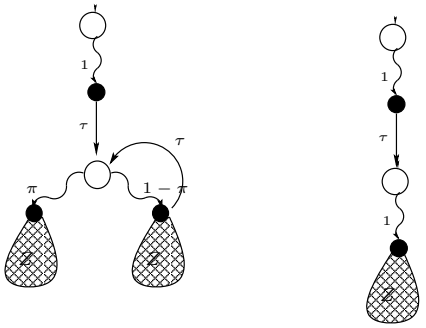


Figure 7.16: Processes that should be related.

process in Figure 7.16 corresponds to the solution of equation $X = Z \leftthreetimes\!\!\sqcup_\pi (Z + i \cdot X)$, where i is an internal action. Informally, it is a process that chooses to behave as Z with probability π. With probability $1 - \pi$ it reaches a state at which it chooses non-deterministically to behave as Z or it makes an internal step to the initial state. Clearly, this process will eventually reach sub-process Z. In other words, it behaves like Z with probability 1. Therefore, it should be considered equivalent to the second process given in Figure 7.16. Thus, we are inclined to consider the following verification rule:

$$\frac{Y = Z \leftthreetimes\!\!\sqcup_\pi (Z + i \cdot Y), i \in I}{\tau \cdot \tau_I(Y) = \tau \cdot \tau_I(Z)} \quad (PVR)$$

under the assumption that Z represents a trivial static process. One can notice that in order to state this rule we do not need the fairness assumption. Even if the non-deterministic choice $Z + i \cdot Y$ will unfairly be resolved in the favour of the summand $i \cdot Y$ the result will still be the same. This situation actually is already captured by the rule PVR_1.

It turned out that $PrB2$ and PVR are sufficient to do the verification of the ABP. Of course, here we mean about possible directions for this verification: still we cannot talk about a completely formal proof, since we do not have a formally developed theory that can provide a formal proof. Basically, we lack a definition of an appropriate equivalence relation that will constitute a model or our rules. The equivalence relation we have in mind should be an extension f the probabilistic branching bisimulation relation defined in Chapter refchapterabstraction. In [100], the author defines a weak probabilistic bisimulation that relates the kind of processes we have talked bout. Even more, in [32] the authors propose an axiom system for a weak probabilistic bisimulation and one of the axioms coincides with $PrB2$ axiom. However, this definition of weak bisimulation does not elate processes we discussed in Chapter 6. We believe hat the weak probabilistic bisimulations in [100, 32] are good points to explore, in order to obtain an equivalence relation that is an extension of the bisimulation defined in Chapter 6 and at the same time it makes a model for the axiom $PrB2$ and the rule PVR.

Chapter 8

Conclusion

This chapter is an overview of the contributions of this thesis. In more details we explain our achievements shortly discussed in Chapter 1 and give several directions and ideas for future work.

8.1 Achievements

The objective of this thesis is to introduce a probabilistic version of *ACP* where non-determinism and probability co-exist. In Chapter 3 and 4 the presented probabilistic process algebra $pACP^+$ improves the variant of probabilistic process algebra proposed in [8]. In order to get a more effective axiom system we have proposed a new variant of an extension of *pBPA* with parallel composition. Following the idea of *ACP*-like process algebras for the interleaving model we have given the axiom system where only parallel dynamic processes are merged. In order to realise this concept we have added an extra quaternary operator, $\between$ called merge with memory. The operational semantics of $pACP^+$ is based on the alternating model of Hansson [71] and it has been defined by a term deduction system. The signature of this system contains an extended set of constants (each atomic action has a dynamic counterpart) and its deduction rules include two transition types: probabilistic and action transitions. Instead of labelling probabilistic transitions we have defined the probability distribution function which gives a probability with which a probabilistic transition may occur. In the construction of the term models we have used probabilistic bisimulation and we have shown soundness and completeness of the term model with respect to the proposed axiom systems. $pACP^+$ is a theory for structured specification of probabilistic systems. We give an example in Chapter 7 where we discuss the PAR protocol with unreliable channels. Here we also discuss the possibility to extend our theory with the priority operator needed for the verification of the protocol. The main contribution of this part is a new method for description of probabilistic systems that keeps the flexibility of *ACP* and can be extended with new features if it is necessary.

In Chapter 5 we have introduced time in the probabilistic theories from the previous two chapters. Timing is introduced in the discrete-time manner which basically is modelled by the time unit delay operator. We distinguish between two types of processes: processes that have to start their execution in the same time slice they are initialized and processes that can delay their activities for an arbitrary number of time slices. For the time extension of the basic process algebra from Chapter 3 no additional operators were needed apart from the operators that are used for the discrete time extension of *ACP*. But in order to model a time variant of the asynchronous parallel composition as defined in Chapter 4 a new operator has been inevitable. This operator is necessary for maintaining time consistency. For the discrete time algebras we have defined operational semantics and probabilistic timed

bisimulation. We proved soundness and completeness results. The main contribution of this part is a new method that is suitable for describing quantitative and qualitative behaviour of probabilistic timed systems.

In the thesis we also presented a version of fully probabilistic process algebra with abstraction which contains, in addition to the axioms for the basic operators, a set of verification rules. These rules tie in successfully the idea of abstraction in process algebra with the results from discrete time Markov chain analysis. Furthermore, we proposed a probabilistic branching bisimulation relation which corresponds to this process algebra in the sense that it gives a model for it. In such a way we obtain a model for the verification rules. We provide several examples of probabilistic processes that are related by our bisimulation but are not related by any other existing weak or branching bisimulation. We show that the branching bisimulation can be decided in polynomial time with respect to the number of states of the considered system.

In Chapter 7 we could prove the correctness of the PAR protocol by combining the methods presented earlier. Actually we reduced the process expression for the parallel composition of the protocol components to an expression of a fully probabilistic process on which the verification technique from Chapter 6 has been applied.

8.2 Future research

We believe that the specification methods we have proposed are powerful enough to model a broad class of probabilistic system behaviours. However, there are many aspects that have to be considered regarding the algebraic verification techniques for probabilistic systems.

In Section 7.4 we have mentioned that one of the main directions of our future interest is the extension of the probabilistic branching bisimulation defined in Chapter 6 to the class of probabilistic processes with non-determinism. The main aspect in our definition is that not every state has to be considered but only those states that are entered after an observable action or the states from one equivalence class that are first entered from a state from some other equivalence class. Thus, some states that cannot be observed do not have to be related since they are only involved when probability distributions for observable states - entries - are composed.

The new extended definition should also be based on the notion of entries. Besides, a "big internal" transition consisting of a sequence of internal transitions between states of the same equivalence class should be defined that takes non-determinism into account. Clearly, it is desirable for such a bisimulation to be compositional. We have realized that branching bisimulation taken as the underlying concept can be too strong in the sense that no probabilistic branching bisimulation that preserves the parallel composition operator can be defined. Thus we believe that the underlying equivalence relation should be weaker than branching bisimulation, e.g. as the relations described in [57].

While sufficient verification rules have been proposed for the standard *ACP*-like process algebras, this is not the case with its time extensions. The attempt to define a timed variant of $KFAR$ rules in [44] was unsuccessful. But in the recent paper [23] new verification rules and an equivalence relation for timed systems have been proposed. This may open another prospect in the research of verification of probabilistic timed systems. Therefore, combining the approach in [23] together with our probabilistic approach with its possible extension with non-determinism should be investigated.

List of axioms

$x + y$	=	$y + x$		$A1$
$(x + y) + z$	=	$x + (y + z)$		$A2$
$x + x$	=	x		$A3$
$a + a$	=	a		$AA3$
$\underline{\underline{a}} + \underline{\underline{a}}$	=	$\underline{\underline{a}}$		$DRTAA3$
$(x + y) \cdot z$	=	$x \cdot z + y \cdot z$		$A4$
$(x \cdot y) \cdot z$	=	$x \cdot (y \cdot z)$		$A5$
$x \parallel y$	=	$x \between y + y \between x + x \mid y$		$CM1$
$a \between x$	=	$a \cdot x$		$CM2$
$a \cdot x \between y$	=	$a \cdot (x \parallel y)$		$CM3$
$(x + y) \between z$	=	$x \between z + y \between z$		$CM4$
$a \mid b$	=	$\gamma(a, b)$		CF
$a \mid b \cdot x$	=	$(a \mid b) \cdot x$		$CM5$
$a \cdot x \mid b$	=	$(a \mid b) \cdot x$		$CM6$
$a \cdot x \mid b \cdot y$	=	$(a \mid b) \cdot (x \parallel y)$		$CM7$
$(x + y) \mid z$	=	$x \mid z + y \mid z$		$CM8$
$z \mid (x + y)$	=	$z \mid x + z \mid y$		$CM9$
$\partial_H(a)$	=	a	if $a \notin H$	$D1$
$\partial_H(a)$	=	δ	if $a \in H$	$D2$
$\partial_H(x + y)$	=	$\partial_H(x) + \partial_H(y)$		$D3$
$\partial_H(x \cdot y)$	=	$\partial_H(x) \cdot \partial_H(y)$		$D4$
$\Pi_n(a)$	=	a		$PR1$
$\Pi_1(a \cdot x)$	=	a		$PR2$
$\Pi_{n+1}(a \cdot x)$	=	$a \cdot \Pi_n(x)$		$PR3$
$\Pi_n(x + y)$	=	$\Pi_n(x) + \Pi_n(y)$		$PR4$
$\tau_I(a)$	=	a	if $a \notin I$	$TI1$
$\tau_I(a)$	=	τ	if $a \in I$	$TI2$
$\tau_I(x + y)$	=	$\tau_I(x) + \tau_I(y)$		$TI3$
$\tau_I(x \cdot y)$	=	$\tau_I(x) \cdot \tau_I(y)$		$TI4$
$x \cdot \tau$	=	x		$B1$
$x \cdot (\tau \cdot (y + z) + y)$	=	$x \cdot (y + z)$		$B2$

$\sigma_{rel}(x) + \sigma_{rel}(y)$	=	$\sigma_{rel}(x + y)$		$DRT1$
$\sigma_{rel}(x) \cdot y$	=	$\sigma_{rel}(x \cdot y)$		$DRT2$
$x + \underline{\underline{\delta}}$	=	x		$DRT3$
$\underline{\underline{\delta}} \cdot x$	=	$\underline{\underline{\delta}}$		$DRT4$
$\nu_{rel}(\underline{\underline{a}})$	=	$\underline{\underline{a}}$		$DCS1$
$\nu_{rel}(x + y)$	=	$\nu_{rel}(x) + \nu_{rel}(y)$		$DCS2$
$\nu_{rel}(x \cdot y)$	=	$\nu_{rel}(x) \cdot y$		$DCS3$
$\nu_{rel}(\sigma_{rel}(x))$	=	$\underline{\underline{\delta}}$		$DCS4$
$\underline{\underline{a}} \mid \underline{\underline{b}}$	=	$\underline{\underline{\gamma(a,b)}}$		$DRTCF$
$\underline{\underline{a}} \mid \underline{\underline{b}} \cdot x$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot x$		$DRTCM2$
$\underline{\underline{a}} \cdot x \mid \underline{\underline{b}}$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot x$		$DRTCM3$
$\underline{\underline{a}} \cdot x \mid \underline{\underline{b}} \cdot y$	=	$(\underline{\underline{a}} \mid \underline{\underline{b}}) \cdot (x \parallel y)$		$DRTCM4$
$\sigma_{rel}(x) \mid \nu_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTCM5$
$\nu_{rel}(x) \mid \sigma_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTCM6$
$\sigma_{rel}(x) \mid \sigma_{rel}(y)$	=	$\sigma_{rel}(x \mid y)$		$DRTCM7$
$\underline{\underline{a}} \lfloor\!\lfloor x$	=	$\underline{\underline{a}} \cdot x$		$DRTM2$
$\underline{\underline{a}} \cdot x \lfloor\!\lfloor y$	=	$\underline{\underline{a}} \cdot (x \parallel y)$		$DRTM3$
$(x + y) \lfloor\!\lfloor z$	=	$x \lfloor\!\lfloor z + y \lfloor\!\lfloor z$		$DRTM4$
$\sigma_{rel}(x) \lfloor\!\lfloor \nu_{rel}(y)$	=	$\underline{\underline{\delta}}$		$DRTM5$
$\sigma_{rel}(x) \lfloor\!\lfloor (\nu_{rel}(y) + \sigma_{rel}(z))$	=	$\sigma_{rel}(x \lfloor\!\lfloor z)$		$DRTM6$
$\partial_H(\underline{\underline{a}})$	=	$\underline{\underline{a}}$	if $a \notin H$	$DRTD1$
$\partial_H(\underline{\underline{a}})$	=	$\underline{\underline{\delta}}$	if $a \in H$	$DRTD2$
$\partial_H(\sigma_{rel}(x))$	=	$\sigma_{rel}(\partial_H(x))$		$DRTD5$
$x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y$	=	$y \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_{1-\pi} x$		$PrAC1$
$x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi (y \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\rho z)$	=	$(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_{\frac{\pi}{\pi+\rho-\pi\rho}} y) \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_{\pi+\rho-\pi\rho} z$		$PrAC2$
$x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi x$	=	x		$PrAC3$
$(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y) \cdot z$	=	$x \cdot z \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y \cdot z$		$PrAC4$
$(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y) + z$	=	$(x + z) \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi (y + z)$		$PrAC5$
$\Pi_n(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\rho y)$	=	$\Pi_n(x) \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\rho \Pi_n(y)$		$prPR$
$x \parallel y$	=	$(x, x) \left[\!\left[(y, y)\right.\right.$		$PrMM1$
$(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi x', z) \left[\!\left[(y, w)\right.\right.$	=	$(x, z) \left[\!\left[(y, w) \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi (x', z) \left[\!\left[(y, w)\right.\right.\right.\right.$		$PrMM2$
$(x, z) \left[\!\left[(y \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y', w)\right.\right.$	=	$(x, z) \left[\!\left[(y, w) \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi (x, z) \left[\!\left[(y', w)\right.\right.\right.\right.$		$PrMM3$
$(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y) \lfloor\!\lfloor z$	=	$x \lfloor\!\lfloor z \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y \lfloor\!\lfloor z$		$PrCM1$
$(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y) \mid z$	=	$x \mid z \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y \mid z$		$PrCM2$
$x \mid (y \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi z)$	=	$x \mid y \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi x \mid z$		$PrCM3$
$\partial_H(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y)$	=	$\partial_H(x) \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi \partial_H(y)$		$PrD5$
$\sigma_{rel}(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y)$	=	$\sigma_{rel}(x) \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi \sigma_{rel}(y)$		$PrDRT1$
$\nu_{rel}(x \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi y)$	=	$\nu_{rel}(x) \leftarrow\!\!\!\shortmid\!\!\!\rightarrow_\pi \nu_{rel}(y)$		$PrDCS1$

$\sigma_{rel}(x) \between (\nu_{rel}(y) \leftplus_\pi z) = \sigma_{rel}(x) \between z$ $PrDRTM7$

$\sigma_{rel}(x) \between ((\nu_{rel}(y) + \sigma_{rel}(z)) \leftplus_\pi w) = \sigma_{rel}(x) \between (\sigma_{rel}(z) \leftplus_\pi w)$ $PrDRTM8$

$x = x + x, y = y + y \Rightarrow (x, z) \between (y, w) = x \between w + y \between z + x \mid y$ $PrMM4$

$z = z + z \Rightarrow (x + y) \mid z = x \mid z + y \mid z$ $PrCM4$

$z = z + z \Rightarrow z \mid (x + y) = z \mid x + z \mid y$ $PrCM5$

$a = \underline{\underline{a}} + \sigma_{rel}(a)$ $RSPDA1$

$y = \underline{\underline{a}} + \sigma_{rel}(y) \Rightarrow y = a$ $RSPDA2$

$y = \underline{\underline{a}} \cdot x + \sigma_{rel}(y) \Rightarrow y = a \cdot x$ $RSPDA3$

$z = z + z \;\&\; y = \underline{\underline{a}} + \nu_{rel}(z) + \sigma_{rel}(y) \;\&\; y_1 = \nu_{rel}(z) + \sigma_{rel}(y_1) \Rightarrow$ $RSPDA4$
$y = a + y_1$

$z = z + z \;\&\; y = \underline{\underline{a}} \cdot x + \nu_{rel}(z) + \sigma_{rel}(y) \;\&\; y_1 = \nu_{rel}(z) + \sigma_{rel}(y_1) \Rightarrow$ $RSPDA5$
$y = a \cdot x + y_1$

$x'' = x'' + x'', y'' = y'' + y'' \Rightarrow$ $PrDRTMM4$
$(\nu_{rel}(x') + \sigma_{rel}(x''), z) \between (\nu_{rel}(y') + \sigma_{rel}(y''), w) =$
$(\nu_{rel}(x'), z) \between (\nu_{rel}(y'), w)) + \big(\sigma_{rel}(x'') \between w + \sigma_{rel}(y'') \between z + \sigma_{rel}(x'') \mid \sigma_{rel}(y'')\big)$

$x = x + x, y = y + y \Rightarrow$ $PrDRTMM5$
$(\nu_{rel}(x), z) \between (\nu_{rel}(y), w) = \nu_{rel}(x) \between w + \nu_{rel}(y) \between z + \nu_{rel}(x) \mid \nu_{rel}(y)$

$(\nu_{rel}(x) + \sigma_{rel}(x'), z) \between (\nu_{rel}(y), w) =$ $PrDRTMM6$
$(\nu_{rel}(x), z) \between (\nu_{rel}(y), w) + \sigma_{rel}(x') \between w$

$(\nu_{rel}(x), z) \between (\nu_{rel}(y) + \sigma_{rel}(y'), w) =$ $PrDRTMM7$
$(\nu_{rel}(x), z) \between (\nu_{rel}(y), w) + \sigma_{rel}(y') \between w$

$\overline{\boldsymbol{\sigma}}(\nu_{rel}(x)) = \underline{\delta}$ $PrRN1$

$\overline{\boldsymbol{\sigma}}(\nu_{rel}(x) + \sigma_{rel}(y)) = y$ $PrRN2$

$\overline{\boldsymbol{\sigma}}(\nu_{rel}(x) \leftplus_\pi y) = \overline{\boldsymbol{\sigma}}(y)$ $PrRN3$

$\overline{\boldsymbol{\sigma}}((\nu_{rel}(x) + \sigma_{rel}(y)) \leftplus_\pi z) = \overline{\boldsymbol{\sigma}}(\sigma_{rel}(y) \leftplus_\pi z)$ $PrRN4$

$y = y + y \Rightarrow x \cdot (\tau \cdot (y + z) + y) = x \cdot (y + z)$ $PrB2$

Summary

Every day we witness the fast development of the hardware and software technology. This, of course, is the reason that new and more complex systems controlled by some kind of computational-based devices become an unseparated part of our daily life. As more as the system complexity increases, as more the reasoning about its correct behaviour becomes difficult. A variety of consequences may occur as a result of a failure, ranging from simple annoying to life threatening ones. Thus for some systems it is crucial that they exhibit a correct functioning. However, for systems with an extremely complex construction it is almost impossible to give an absolute guarantee for their correctness. In this case, it is still satisfactory to know that the possibility for a system to fail is low enough.

Formal methods have been developed for establishing correctness of computer systems. They provide rigorous methods with which one can formally specify properties of a systems's intended behaviour, and also can check if the system conforms to that specification. In case of complex systems we need a formal method that allows us to reason in compositional way, it provides us with techniques that can be used to build larger systems from the composition of smaller ones. Process algebra carries exactly this idea; it provides operators that allow to compose processes in order to obtain a more complex process. Besides, every process algebra contains a set of axioms. Every axiom is an algebraic equation that carries our intuition and insight in process behaviour, it expresses which two processes behaviour we consider equal. In such a way, manipulation with processes becomes manipulation with equations in the algebraic sense.

But, equations and operators do not have any meaning unless we place them in a certain real "world" and match the terms of the process algebra with the entities of the real world. This step is traditionally called "giving a semantic of the syntax". The structure constructed in this way is called a model of the considered process algebra. For every given process algebra we can construct an infinite number of models, but only several of them are interesting for the purpose process algebra was developed as a formal method. However, there is a tendency always to use so-called a bisimulation model. In this thesis we propose several process algebras and construct their models based on the notion of bisimulation.

Probabilities

When using traditional formal methods to model a concurrent system designers are mostly interested in the functional behaviour of that system. But in real-life systems not only functionality but also quantitative aspects of the system behaviour are important. Even more due to the physical implementation of the system and its interaction with the environment one cannot expect a perfect system without a possibility to fail. Naturally, the designer wants to be certain that the probability for this to happen is sufficiently small.

In this thesis we turn our attention to probabilistic phenomena and propose methods for specifying and verifying systems that exhibit probabilistic behaviour - probabilistic systems. Probabilistic

behaviour of processes in the framework of process algebra is captured by an operator, called probabilistic choice operator. This operator allows the explicit specification of probabilistic aspects in a way that it expresses (quantitatively) a probability distribution over a set of possible events/behaviours.

In this thesis we focus on two instances where probabilistic aspects have to be considered.

First, in the case of an unreliable system where the whole system or some of its components are subject to failure. Usually, failures of system (components) are probabilistic in nature or can be approximated y some probabilistic process and clearly in these cases probabilities should be used for the sake of obtaining a more accurate model of the system. In Chapter 3 and Chapter 4 we propose a process algebra that can be used for specification of concurrent processes with probabilistic behaviour. Traditional results in process algebra such as congruence, elimination, soundness and completeness are studied.

The second application of probabilities is that they can be used to model fairness. In the presence of probabilities, a fairness assumption for probabilistic choice is superfluous as it is implicitly expresses by assigning non-zero probabilities to every alternative in the probabilistic choice. In Chapter 6 we investigate the following scenario: if a system can executes an external action with a non-zero probability, then abstraction from internal steps will yield the external step with probability 1 after a sequence of finitely many internal steps. In case of more possible external activities, the behaviour of the process, after the internal cycle is left, is governed by a probability distribution function. Using the concept of absorption probabilities from discrete time Markov chain theory, we formulate several algebraic verification rules applicable on fully probabilistic processes. The main contribution of this part is the definition of a probabilistic branching bisimulation and the construction of a model for our probabilistic process algebra with abstraction based on it. We also define an algorithm that decides the probabilistic branching bisimulation.

Another quantitative aspect that should be taken into account when modelling a system behaviour is time. Simultaneously introducing time and probability in formal methods provides a new aspect to the specification and verification of (concurrent) systems. Certainly, it allows more accurate modelling of time behaviour and unreliability which in standard methods usually are encoded by alternative composition. In Chapter 5 we consider discrete-time extensions of the probabilistic process algebras defined in Chapter 3 and Chapter 4. Besides, we define a timed variant of the probabilistic bisimulation and construct the bisimulation models of the discrete-time probabilistic process algebras. Like for the untimed process algebras, we study results such as elimination, soundness and completeness in the context of the timed process algebras.

In Chapter 7 we report three case studies analyzed by the methods defined in the previous chapters. All three case studies are examples of communication protocols that use an unreliable channel. By the last example we report several observations we have made regarding verification methods for process that exhibit both probabilistic and non-deterministic behaviour. Here, mainly we discuss some ideas left for further investigation.

Samenvatting

De ontwikkeling van software en hardware systemen is de afgelopen decennia in een stroomversnelling geraakt. De steeds grotere beschikbaarheid van omvangrijke en complexe, computer gestuurde systemen heeft tot gevolg dat we steeds afhankelijker worden van zulke systemen. Zoals veel hulpmiddelen, gemaakt door mensenhanden, kunnen dit soort systemen falen. Het falen van dergelijke systemen heeft vaak gevolgen die in ernst kunnen variëren van vervelend tot levensbedreigend. Het is daarom, zeker voor een klasse van systemen, van levensbelang dat ze correct functioneren. Voor veel systemen geldt echter dat het bouwen ervan vaak extreem complex is; derhalve is een absolute zekerheid op de correctheid van het gebouwde systeem niet altijd te geven. In deze gevallen is het van belang om te weten dat de kans op falen klein genoeg is.

Voor het vaststellen van de correctheid van een computer systeem zijn verscheidene *Formele Methoden* ontwikkeld. Deze stellen gebruikers in staat om op een precieze, eenduidige wijze vast te leggen wat de gewenste eigenschappen van een systeem zijn. Bovendien is het vaak mogelijk om met behulp van dit soort methoden vast te stellen dat een gegeven systeem aan een gewenste specificatie voldoet, en dat gewenste eigenschappen daadwerkelijk aanwezig zijn. De grootte van complexe systemen is echter in veel gevallen een belemmering voor dit soort beschrijvingen en analyses. Daarom is het noodzakelijk dat de methode gebruikers in staat stelt om systemen op een *compositionele* wijze te beschrijven en te analyseren. Met andere woorden, zulk soort methoden stellen gebruikers in staat om grote, complexe systemen samen te stellen uit kleinere, behapbare systemen. *Proces algebra* is een van de formele methoden die aan deze eisen beantwoord; de manier waarop complexe systemen kunnen worden samengesteld uit kleinere systemen is door middel van (wiskundige) operatoren. Kenmerkend voor een proces algebra zijn de axioma's die in vergelijkingen de intuïtie achter het samenspel van systeemgedragingen en operatoren vastleggen. Op die manier beschrijft het eenduidig welke systemen we *equivalent* kunnen beschouwen. Deze vergelijkingen stellen ons bovendien in staan om te rekenen aan systemen op een algebraïsche wijze.

Vergelijkingen en operatoren zijn echter weinig zinvol als we niet precies begrijpen wat we ermee bedoelen. Derhalve is het noodzakelijk om termen van de proces algebra te relateren aan entiteiten uit de echte wereld. Het vastleggen van deze relaties staat bekend als het geven van een *semantiek* aan de syntaxis. De objecten uit de echte wereld vormen een zogenaamd *model* voor een proces algebra. Voor elke proces algebra kan in wezen een oneindige hoeveelheid modellen gegeven worden; echter, maar enkele modellen hiervan zijn interessant, daar de meerderheid van de modellen het idee achter de proces algebra niet juist vertegenwoordigt. Een veelgebruikt model is het zogenaamde *bisimulatie* model. De in dit proefschrift bestudeerde proces algebras worden allen voorzien van een model dat gestoeld is op bisimulatie.

Kansen

Bij het gebruik van traditionele formele methoden om systemen te beschrijven is men vaak beperkt tot het het beschrijven en analyseren van het functionele gedrag van dat systeem. De realiteit leert echter dat kwantitatieve eigenschappen van een systeem vaak minstens zo belangrijk zijn als het functionele gedrag van een systeem. Door de vaak imperfecte omgeving waarmee een systeem interacties heeft en waarin een systeem dient te functioneren, kan men een foutloos functioneren van een systeem redelijkerwijs niet verwachten. Een gedegen inzicht in de kans op het falen van een systeem is vaak van groot belang voor zowel de ontwerper als voor gebruikers van een systeem. Door het meenemen van kwantitatieve informatie over de omgeving alsmede over het systeem zelf in de beschrijving van een systeem is een ontwerper in staat om betere inschattingen te maken in het functioneren van een systeem.

In dit proefschrift bestuderen we het fenomeen van *kansen*. We stellen methoden voor die gebruikers in staat stellen om een systeem waarin kans een rol speelt — zogenaamde *probabilistische systemen* — te beschrijven en te verifiëren. In de proces algebra wordt het probabilistische gedrag van een systeem beschreven middels een operator, genaamd *probabilistische keuze*. Deze operator stelt gebruikers in staat om (kwantitatieve) kans distributies te koppelen aan een verzameling mogelijke systeemgedragingen.

In dit proefschrift bestuderen we twee instanties waarin probabilistische aspecten moeten worden beschouwd. Een gebruik van kansen is in het modelleren van onbetrouwbare (mogelijk parallelle) systemen. Het falen van een dergelijke systeem is vaak terug te voeren op (de kans op) het falen van een of meerdere deelcomponenten van het systeem. Het falen van componenten kan in veel gevallen beschreven worden door het meenemen van kanstechnische informatie over het gedrag; het algehele systeem falen is daarmee vaak eveneens kanstechnisch te beschrijven. Een functionele *en* kwantitatieve beschrijving van een systeem en zijn componenten is derhalve wenselijk als het doel is een zo natuurgetrouw beeld te krijgen van een systeem. De proces algebra die we beschrijven en bestuderen in Hoofdstuk 3 en Hoofdstuk 4 kan gebruikt worden om zulke onbetrouwbare systemen te beschrijven en analyseren. Met name bestuderen we in deze hoofdstukken de voor proces algebra traditionele resultaten zoals congruentie, eliminatie, en volledigheid.

Het tweede gebruik van het toepassen van kansen dat we bestuderen in dit proefschrift omvat het modelleren van *fairness* eigenschappen van een systeem. Door de aanwezigheid van kansen zijn aannames over fairness voor de probabilistische keuze overbodig. De fairness van een probabilistische keuze volgt namelijk impliciet uit het toekennen van strikt positieve kansen aan ieder alternatief in een probabilistische keuze. In Hoofdstuk 6 onderzoeken we het volgende scenario: als een systeem een *externe actie* a met strikt positieve kans kan uitvoeren, dan zal door het abstraheren van interne acties, de kans op de actie a na een eindig aantal interne acties, gelijk zijn aan 1. In het geval dat meerdere externe acties mogelijk zijn, zal het verdere gedrag van het systeem, zodra de interne lus verlaten wordt, bepaald worden door een kansdistributie functie. Gebruik makend van het concept van *absorbing probabilities*, bekend uit de Markov chain theorie, zijn we in staat om verscheidene algebraïsche verificatie regels te formuleren die ons in staat stellen om met abstractie in puur probabilistische systemen te rekenen. De belangrijkste contributie van dit hoofdstuk is de definitie van een *probabilistic branching* bisimulatie en de constructie van een model voor onze probabilistische proces algebra met abstractie. Bovendien tonen we aan dat de probabilistic branching bisimulatie beslisbaar is en definieren we hiervoor een algoritme.

Kansen vormen niet de enige kwantitatieve aspecten van een systeem. Het verstrijken van tijd is een belangrijk ander kwantitatief aspect dat veelal het gedrag van een systeem kan beïnvloeden. Een systeembeschrijving waarin zowel de kanstechnische informatie alsmede de tijdsafhankelijkhe-

den zijn opgenomen stelt een ontwerper in staat om de invloed van beide aspecten op het systeem en op elkaar grondig te analyseren. In Hoofdstuk 5 beschouwen we een discrete-tijd uitbreiding van de probabilistische proces algebras die we in Hoofdstuk 3 en Hoofdstuk 4 reeds eerder hebben gedefinieerd. De toevoeging van tijd als concept aan onze proces algebras heeft tot gevolg dat een aanpassing van het bisimulatie model van de oorspronkelijke probabilistische proces algebras aangepast dient te worden. Daartoe definieren we een tijds-variant op de probabilistische bisimulatie en construeren we het bisimulatie model voor de discrete-tijd probabilistische proces algebras. De resultaten die we reeds eerder bestudeerden voor de probabilistische proces algebras, zoals eliminatie en volledigheid, worden opnieuw bestudeerd voor de discrete-tijd probabilistische proces algebras.

Hoofdstuk 7 beschrijft, aan de hand van drie casussen, de toepassingen van de methoden die we onderzocht en beschreven hebben in de voorgaande hoofdstukken. Alle beschreven casussen zijn voorbeelden van communicatie protocollen waarbij gebruik wordt gemaakt van een onbetrouwbaar kanaal. Bij het laatste voorbeeld gaan we dieper in op diverse observaties die we maken met betrekking tot methoden voor het verifiëren van systemen die zowel probabilistisch als non-deterministisch gedrag vertonen. De ideeën die hier beschreven staan zijn suggesties voor verder onderzoek.

Bibliography

[1] L. Aceto, W. Fokkink, C. Verhoef, *Conservative extension in structural operational semantics*, In Current Trends in Theoretical Computer Science - Entering the 21st Century, World Scientific, G. Paun, G. Rozenberg, A. Salomaa eds., pp. 504-524, 2001.

[2] L. Aceto, W. Fokkink, C. Verhoef, *Structural operational semantics*, In [38], pp. 197-292, 2001.

[3] L. Aceto, Z. Ésik, A. Ingólfsdóttir, *Equational axioms for probabilistic bisimilarity*, Proc, of the 9th International Conference on Algebraic Methodology And Software Technology, AMAST '2002, St. Gilles les Bains, Reunion Island, France. Lecture Notes in Computer Science 2422, pp. 239-253, 2002. Also appears as technical report BRICS RS-02-6, 2002.

[4] A. Aho, J. Hopcroft, J. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley Publishing Company, 1974.

[5] A. Aldini, R. Gorrieri, *Security analysis of a probabilistic non-repudiation protocol*, Proc. of the 2nd Joint Int. Workshop on Process Algebra and Performance Modelling, Probabilistic Methods in Verification (PAPM-PROBMIV'02), H. Hermanns, R. Segala eds., Springer LNCS 2399, pp. 17-36, Copenhagen, Denmark, July 2002

[6] S. Andova, *Vremenski procesni algebri*, MSc. thesis, University "Sts. Cyril and Methodious", Institute of Informatics, 1997.

[7] S. Andova, *Process algebra with probabilistic choice (extended abstract)*, Proc. 5th International AMAST Workshop, ARTS'99, Bamberg, Germany, J.-P. Katoen, ed., LNCS 1601, Springer-Verlag, pp. 111-129, 1999. (Full version report CSR 99-12, Eindhoven University of Technology, 1999.)

[8] S. Andova, *Process algebra with interleaving probabilistic parallel composition*, Eindhoven University of Technology, CSR 99-04, 1999.

[9] S. Andova, *Process algebra with time and probabilities*, Proc. of International Conference on Algebraic Methodology and Software Technology (AMAST'00), Iowa City, USA, T. Rus, ed., LNCS 1816, Springer-Verlag, pp.323-338, 2000.

[10] S. Andova, J. C. M. Baeten *Abstraction in probabilistic process algebra*, Proc. Tools and Algorithms for the Construction and Analysis of Systems, 7th International Conference, TACAS 2001 Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2001 Genova, Italy, T. Margaria, Wang Yi, eds., LNCS 2031 Springer Verlag, pp. 204-219, 2001.

[11] S. Andova, J. C. M. Baeten *Alternative composition does not imply non-determinism*, Bulletin of the European Association for Theoretical Computer Science 76, EATCS, pp. 125-127, Feb. 2002.

[12] J. C. M. Baeten, J. A. Bergstra, J. W. Klop, *Syntax and defining equations for and interrupt mechanism in process algebra*, Fundamenta Informaticæ, IX(2):127-168, 1986.

[13] J. C. M. Baeten, J. A. Bergstra, J. W. Klop, *On the consistency of Koomen's fair abstraction rule*, Theor. Comp. Sci. 51, pp.129-176, 1987.

[14] J. C. M. Baeten, R. J. van Glabbeek, *Merge and termination in process algebra*, Proc. of Foundations of Software Technology and Theoretical Computer Science (FSTTCS), Pune, India, K.V. Nori, ed., LNCS 287, Springer-Verlag, pp.153-172, 1987.

[15] J. C. M. Baeten, J. A. Bergstra, *Global renaming operators in concrete process algebra*, Information and Computation 78, pp. 205-245, 1988.

[16] J. C. M. Baeten, J. A. Bergstra, *Real time process algebra*, Formal Aspects of Computing, 3(2):142-188, 1991.

[17] J. C. M. Baeten, J. A. Bergstra, S. A. Smolka, *Axiomatizing probabilistic processes: ACP with generative probabilities*, Information and Computation 121(2), pp. 234-255, Sep. 1995.

[18] J. C. M. Baeten, J. A. Bergstra, *Process algebra with partial choice*, Proc. CONCUR '94, Uppsala, B. Jonsson & J. Parrow, eds., LNCS 836, Springer Verlag, pp. 465-480, 1994.

[19] J. C. M. Baeten, J. A. Bergstra, *Discrete time process algebra*, Formal Aspects of Computing, 8(2):188-208, 1996.

[20] J. C. M. Baeten, J. A. Bergstra, *Discrete time process algebra: Absolute time, relative time and parametric time*, Fundamenta Informaticæ, 29(1,2):51-76, 1997.

[21] J. C. M. Baeten, R. van Glabbeek, *Another look at abstraction in process algebra*, Proc. ICALP'87, Karlsruhe, Th. Ottman ed., LNCS 267, Springer Verlag, pp. 84-94, 1987.

[22] J. C. M. Baeten, C. A. Middelburg, *Process algebra with timing: Real time and discrete time*, Eindhoven University of Technology, CSR 99-11, 1999. In J.A. Bergstra, A. Ponse and S.A. Smolka, eds., Handbook of Process Algebra, Elsevier, 2001.

[23] J. C. M. Baeten, C. A. Middelburg, M. A. Reniers, *A new equivalence for processes with timing – with an application to protocol verification*, Eindhoven University of Technology, CSR 2002.

[24] J. C. M. Baeten, C. A. Middelburg, *Process algebra with timing*, EATCS Monographs Series, Springer-Verlag, 2002.

[25] J. C. M. Baeten, J. J. Vereijken, *Discrete time process algebra with empty process*, Technical report CSR 97/05, Eindhoven University of Technology, Computing Science Department, 1997.

[26] J. C. M. Baeten, C. Verhoef, *Concrete process algebra*, In: Handbook of logic in computer science , S. Abramsky, D.M. Gabbay, T.S.E. Maibaum, eds., Vol. 4, Syntactical Methods, Chapter 2, Oxford University Press 1995, pp. 149 - 268.

[27] J.C.M. Baeten, W. P. Weijland, *Process algebra*, Cambridge University Press, 1990.

[28] C. Baier, *On algorithmic verification methods for probabilistic systems*, Habilitation thesis, Univ. Mannheim, 1998.

[29] C. Baier, H. Hermanns, *Weak bisimulation for fully probabilistic processes*, Proc. CAV'97, O. Grumberg, ed., LNCS 1254, pp. 119-130, 1997.

[30] C. Baier, M. Stoelinga, *Norm functions for probabilistic bisimulations with delays*, Proc. FOSSACS'00, J. Tiuryn, ed., Berlin, Germany, LNCS 1784, Springer Verlag, pp. 1-16, 2000.

[31] J. W. de Bakker, J. I. Zucker, *Processes and the denotational semantics of concurrency*, Information and Control 54(1/2), pp. 70-120, 1982.

[32] E. Bandini, R. Segala, *Axiomatizations for probabilistic bisimulation*, Proc. ICALP'01, F. Orejas, P.G. Spirakis, J. van Leeuwen, eds., Crete, Greece, LNCS 2076, Springer Verlag, pp. 370-381, 2001.

[33] J. A. Bergstra, *Put and gets, primitives for synchronous unreliable message passing*, Rep. LGPS3, Department of Philosophy, University of Utrecht, 1985.

[34] J. A. Bergstra, J. W. Klop, *Process algebra for synchronous communication*, Information and Control 60, pp. 109-137, 1984.

[35] J. A. Bergstra, J. W. Klop, *The algebra of recessively defined processes and the algebra of regular processes*, Proc. 11th ICALP, Antwerpen, J. Paredaens ed., LNCS 172, Springer Verlag, pp. 82-95, 1984.

[36] J. A. Bergstra, J. W. Klop, *Algebra of communicating processes with abstraction*, Theoret. Comput. Sci., 37(1), pp. 77-121, 1985.

[37] J. A. Bergstra, J. W. Klop, *Verification of an alternating bit protocol by means of process algebra*, Mathematical Methods of Specification and Synthesis of Software Systems '85, W. Bibel and K.P.Jantke, eds., Mathematical research 31, Akademie-Verlag, Berlin, pp. 8-23, 1986.

[38] J. A. Bergstra, A. Ponse, S. Smolka, eds, *Handbook of process algebra*, North-Holland, 2000.

[39] M. Bernardo, R. Gorrieri, *A tutorial on EMPA: A theory of concurrent processes with nondeterminism, priorities, probabilities and time*, Theoretical Computer Science, 202(1-2):1-54, 1998.

[40] M. Bernardo, *Theory and application of extended Markovian process algebra*, Ph.D. thesis, Dottorato di Ricerca in Informatica, Università di Bologna, Padova, Venezia, 1999.

[41] S. L. Bloom, Z. Ésik, *Iteration theories*, Springer-Verlag, Berlin, 1993.

[42] S. H. J. Bos, M. A. Reniers, *The I^2C-bus in discrete-time process algebra*, Science of Computer Programming, 29(1-2):235-285, 1997.

[43] R. Bol, J. F. Groote, *The meaning of negative premises in transition system specification*, In Journal of the ACM, 43(5):863-914, 1996.

[44] D. Bošnački, *PAR protocol in discrete time process algebra*, unpublished paper, 1996.

[45] M. Bravetti, R. Gorrieri *The theory of interactive generalized semi-Markov processes*, Theoretical Computer Science, 286, 2002.

[46] E. Brinksma, H. Hermanns, J.-P. Katoen eds. *Lectures on formal methods and performance analysis*, First EEF/Euro Summer School on Trends in Computer Science, LNCS 2090, Berg en Dal, The Netherlands, 2000.

[47] Dagstuhl seminar, *Probabilistic methods in verification*, Schloss Dagstuhl, Germany, http://www.cs.bham.ac.uk/~mzk/Dagstuhl, 2000.

[48] P.R. D'Argenio, C. Verhoef, *A general conservative extension theorem in process algebra with inequalities*, Theoretical Computer Science 177, pp. 351-380, 1997.

[49] P.R. D'Argenio, H. Hermanns, J.-P. Katoen, *On generative parallel composition*, Proc. of Workshop on Probabilistic Methods in Verification, (PROBMIV'98), Indianapolis, USA, C. Baier & M. Huth & M Kwiatkowska & M. Ryan ed., ENTCS 22, pp. 105-121, 1998.

[50] P.R. D'Argenio, *Algebras and automata for timed and stochastic systems*, Ph.D. Thesis, University of Twente, 1999.

[51] E. W. Dijkstra, *A discipline of programming*, Prentice-Hall, 1976.

[52] R. W. Floyd, *Assigning meanings to programs*, Proc. of Symposia in Applied Mathematics: Mathematical Aspects of Computer Science, vol. 19, pp. 19-31, 1967.

[53] W. Fokkink, *Introduction to process algebra*, Springer-Verlag, 2000.

[54] A. Giacalone, C. Jou, S. A. Smolka *Algebraic reasoning for probabilistic concurrent systems*, Proc. IFIP TC2 Working conference on Programming Concepts and Methods, M. Broy, C. B. Jones, eds., Sea of Galilee, Israel, pg. 443-458, North-Holland, 1990

[55] R. J. van Glabbeek, *Comparative concurrency semantics, with refinement of actions*, Ph.D. Thesis, Free University, Amsterdam, 1990.

[56] R. J. van Glabbeek, S. A. Smolka, B. Steffen, C. M. N. Tofts, *Reactive, generative and stratified models of probabilistic processes*, Proc. of 5th Annual IEEE Symp. on Logic in Computer Science, Philadelphia, PA, pp. 130-141, 1990.

[57] R. J. van Glabbeek, *The linear time - branching time spectrum II (the semantics of sequential systems with silent moves)*, Extended abstract in: Proc. CONCUR '93, Hildesheim, Germany, E. Best, ed., LNCS 715, Springer-Verlag, 1993, pp. 66-81

[58] R. J. van Glabbeek, *What is branching time semantics and why to use it?*, The Concurrency Column, M. Nielsen, ed., Bulletin of the EATCS 53, pp. 190-198, June, 1994.

[59] R. J. van Glabbeek, P. Weijland, *Branching time and abstraction in bisimulation semantics*, JACM, 43(3): 555-600, 1996.

[60] R. J. van Glabbeek, *The meaning of negative premises in transition system specification II*, in: *Automata, Languages and Programming*, Proc. 23th International Colloquium, ICALP'96, Paderborn, Germany, F. Meyer auf der Heide, B. Monien eds., LNCS 1099, Springer Verlag, pp. 502-513, 1996.

[61] R. J. van Glabbeek, *The linear time - branching time spectrum I*, in [38], pp. 3-99.

[62] N. Götz, U. Herzog, M. Rettelbach, *Multiprocessor and distributed system design: The integration of functional specification and performance analysis using stochastic process algebras*, Performance Evaluation of Computer and Communication Systems, L. Donatiello and R. Nelson eds., LNCS 729, pp. 121-146, Springer Verlag, 1993.

[63] W.O.D. Griffioen, F. Vaandrager, *Normed simulation*, Proc. CAV'98, Vancouver, BC, Canada, A.J. Hu, M.Y. Vardi eds., LNCS 1427, pp. 332-344, Springer Verlag, 1998.

[64] J.F. Groote, F. Vaandrager, *An efficient algorithm for branching bisimulation and stuttering equivalence*, Proc. ICALP'90, LNCS 443, M.S. Paterson, ed., Warwick, England, pp. 626-638, 1990.

[65] J. F. Groote, *Process algebra and structured operational semantics*, Ph.D. thesis, University of Amsterdam, 1991.

[66] J. F. Groote, J.J. van Wamel, *Analysis of three hybrid systems in timed μCRL*, Science of Computer Programming 39:215-247, 2001. Also available as Technical Report SEN-R9815, CWI, Amsterdam, 1998.

[67] R.L. Grossman, A. Nerode, A. Ravn, H. Rischel, editors, *Hybrid Systems*, LNCS 736, Springer-Verlag, 1993.

[68] P. Halmos, *Measure theory*, Springer Verlag, 1950.

[69] H. Hansson, B. Jonsson, *A framework for reasoning about time and reliability*, Proc. 10-th IEEE Real-Time Systems Symposium, IEEE Computer Society Press, 1989.

[70] H. Hansson, B. Jonsson, *A calculus for communicating systems with time and probabilities*, Proc. IEEE Real-Time Systems Symposium, IEEE Computer Society Press, pp 278-287, 1990.

[71] H. Hansson, *Time and probability in formal design of distributed systems*, Ph.D. thesis, DoCS 91/27, University of Uppsala, 1991.

[72] J. I. den Hartog, E. P. de Vink, *Mixing up nondeterminism and probability*, A preliminary report, Proc. LICS'98 workshop on Probabilistic Methods in Verification, C. Baier, M. Huth, M. Kwiatkowska, M. Ryan (eds.), ENTCS 22, 1998. (Full version report IR-449, Vrije Universiteit, Amsterdam, 1998.)

[73] J. I. den Hartog, *Probabilistic extensions of semantical models*, Ph.D. thesis, Vrije Universiteit, October 2002.

[74] H. Hermanns, *Interactive Markov chains*, Ph.D. thesis, University of Erlangen-Nürnberg, 1998.

[75] J. Hillston, *A compositional approach to performance modelling*, Distinguished Dissertation in Computer Science, Cambridge University Press, 1996.

[76] C. A. R. Hoare, *An axiomatic basis for computer programming*, Communications of the ACM 12:576-580, 1969.

[77] C. A. R. Hoare, *Communicating sequential processes*, Communications of the ACM 21(8):666-677, 1978.

[78] C. A. R. Hoare, *Communicating sequential processes*, International Series in Computer Science, Prentice Hall, 1985.

[79] R.A. Howard, *Dynamic probabilistic systems*, New York, Wiley, 1971.

[80] C.-C. Jou, *Aspects of probabilistic process algebra*, Ph.D.Thesis, State University of New York at Stony Brook, 1990.

[81] C.-C. Jou, S. A. Smolka *Equivalences, congruences and complete axiomatizations for probabilistic processes*, Proc. CONCUR '90, LNCS 458, J.C.M. Baeten, J. W. Klop, eds. Springer Verlag, Amsterdam, pp. 367-383, 1990.

[82] J. G. Kemeny, L. J. Snell *Finite Markov chains*, Springer Verlag, 1976.

[83] J. W. Klop *Term rewriting systems*, in *Handbook of Logic and Computer Science, vol. 2: "Background:Computational Structures"*, Oxford University Press, S. Abramsky, D. M. Gabbay, T. S. E. Maibaum eds., pp. 1-116, 1992.

[84] J. L. M. Vrancken, *The algebra of communicating processes with empty process*, Theoretical Computer Science, 177(2):287-328, 1997.

[85] V. Kulkarni, *Modeling and Analysis of Stochastic Systems*, Chapman & Hall, 1995.

[86] K. G. Larsen, A.Skou, *Bisimulation through probabilistic testing*, Information and Computation, 94:1-28, 1991.

[87] N. Lopez, M. Núñez, *NMSPA: A non-Markovian model for stochastic processes*, Proc. of 1st Int. Workshop on Distributed System Validation and Verification, IEEE CS Press, 2000.

[88] N. Lynch, F. Vaandrager, *Forward and backward simulations, II: timing-based systems*, Information and Computation 128(1): 1-25 (1996)

[89] R. Milner, *A calculus of communicating systems*, LNCS 92, Springer, 1980.

[90] R. Milner, *A modal characterisation of observable machine-behaviour*, CAAP'81, G. Astesiano, C. Böhm, eds., LNCS 112, Springer Verlag, pp. 25-34, 1980.

[91] R. Milner, *Calculi for synchrony and asynchrony*, Theoretical Computer Science 25, pp. 267-310, 1983.

[92] R. Milner, *Communication and concurrency*, International Series in Computer Science, Prentice Hall, 1989.

[93] D. M. R. Park, *Concurrency and automata on infinite sequences*, 5^{th} GI Conference, P. Deussen, ed., LNCS 104, Springer, 1981.

[94] C. A. Petri, *Introduction to general net theory*, Proc. Advance Course on General Net Theory of Processes and Systems, LNCS 84, 1980.

[95] A. Philippou, O. Sokolsky, I. Lee, *Weak bisimulation for probabilistic systems*, Proc. CONCUR'98, D. Sangiorgi, R. de Simone, eds., Nice, France, LNCS 1466, Springer Verlag, 1998.

[96] G. D. Plotkin, *A structural approach to operational semantics*, Report DAIMI FN-19, Computer Science Department, Aarhus University, 1981.

[97] A. Pnueli, *The temporal logic of programs*, Proc. 18th IEEE Symposium Foundation of Computer Science - FOCS, pg. 46-57, 1977.

[98] P. Panangaden, *Does combining nondeterminism and probability make sense?*, in Bulletin of the EATCS 72, The Concurrency Column, pp. 182-189, October 2001.

[99] Y. A. Rozanov, *Introductory probability theory*, Prentice Hall, Englewood Cliffs, 1969.

[100] R. Segala, *Modeling and verification of randomized distributed real-time systems*, Ph.D. thesis, Massachusetts Institute of Technology, 1995.

[101] R. Segala, N. A. Lynch, *Probabilistic simulations for probabilistic processes*, Nordic Journal of Computing, 2(2):250-273,1995.

[102] E.W. Stark, S. A. Smolka, *A complete axiom system for finite-state probabilistic processes*, in Proof, Language and Interaction: Essays in Honour of Robin Milner, Plotkin G., Stirling C., Tofte M. (eds.), MIT Press, Cambridge, MA, pp. 571-595,2000.

[103] M. Stoelinga, *Alea jacta est: Verification of probabilistic, real-time and parametric systems*, Ph.D. thesis, Katholieke Universiteit Nijmegen, 2002.

[104] A. S. Tanenbaum, *Computer networks*, Prentice-Hall International, 1981.

[105] F. W. Vaandrager, *Two simple protocols*, In: *Applications of Process algebra*, Cambridge University Press, J.C.M. Baeten ed., pp. 23-44, 1990.

[106] M.Y. Vardi, *Automatic verification of probabilistic concurrent finite state programs*, Proc. of 26th Symp. on Foundations of Com. Sc., IEEE Comp. Soc. Press, pp. 327-338, 1985.

[107] C. Verhoef, *A general conservative extension theorem in process algebra*, Proc. of PROCOMET'94, IFIP 2 Working Conference, San Miniato, E.-R. Olderog ed., pp. 149-168, 1994.

[108] J. J. Vereijken, *Discrete-time process algebra*, Ph.D. thesis, Eindhoven University of Technology, 1997.

[109] J. van Wamel, *Verification techniques for elementary data types and retransmission protocols*, Ph.D. thesis, University of Amsterdam, 1995.

[110] T.A.C. Willemse, *A process algebraic approach to hybrid systems*, PROGRESS 2000, Proc. of Workshop on Embedded Systems, J.P. Veaen ed., pp. 165-170, 2000.

Titles in the IPA Dissertation Series

J.O. Blanco. *The State Operator in Process Algebra*. Faculty of Mathematics and Computing Science, TUE. 1996-1

A.M. Geerling. *Transformational Development of Data-Parallel Algorithms*. Faculty of Mathematics and Computer Science, KUN. 1996-2

P.M. Achten. *Interactive Functional Programs: Models, Methods, and Implementation*. Faculty of Mathematics and Computer Science, KUN. 1996-3

M.G.A. Verhoeven. *Parallel Local Search*. Faculty of Mathematics and Computing Science, TUE. 1996-4

M.H.G.K. Kesseler. *The Implementation of Functional Languages on Parallel Machines with Distrib. Memory*. Faculty of Mathematics and Computer Science, KUN. 1996-5

D. Alstein. *Distributed Algorithms for Hard Real-Time Systems*. Faculty of Mathematics and Computing Science, TUE. 1996-6

J.H. Hoepman. *Communication, Synchronization, and Fault-Tolerance*. Faculty of Mathematics and Computer Science, UvA. 1996-7

H. Doornbos. *Reductivity Arguments and Program Construction*. Faculty of Mathematics and Computing Science, TUE. 1996-8

D. Turi. *Functorial Operational Semantics and its Denotational Dual*. Faculty of Mathematics and Computer Science, VUA. 1996-9

A.M.G. Peeters. *Single-Rail Handshake Circuits*. Faculty of Mathematics and Computing Science, TUE. 1996-10

N.W.A. Arends. *A Systems Engineering Specification Formalism*. Faculty of Mechanical Engineering, TUE. 1996-11

P. Severi de Santiago. *Normalisation in Lambda Calculus and its Relation to Type Inference*. Faculty of Mathematics and Computing Science, TUE. 1996-12

D.R. Dams. *Abstract Interpretation and Partition Refinement for Model Checking*. Faculty of Mathematics and Computing Science, TUE. 1996-13

M.M. Bonsangue. *Topological Dualities in Semantics*. Faculty of Mathematics and Computer Science, VUA. 1996-14

B.L.E. de Fluiter. *Algorithms for Graphs of Small Treewidth*. Faculty of Mathematics and Computer Science, UU. 1997-01

W.T.M. Kars. *Process-algebraic Transformations in Context*. Faculty of Computer Science, UT. 1997-02

P.F. Hoogendijk. *A Generic Theory of Data Types*. Faculty of Mathematics and Computing Science, TUE. 1997-03

T.D.L. Laan. *The Evolution of Type Theory in Logic and Mathematics*. Faculty of Mathematics and Computing Science, TUE. 1997-04

C.J. Bloo. *Preservation of Termination for Explicit Substitution*. Faculty of Mathematics and Computing Science, TUE. 1997-05

J.J. Vereijken. *Discrete-Time Process Algebra*. Faculty of Mathematics and Computing Science, TUE. 1997-06

F.A.M. van den Beuken. *A Functional Approach to Syntax and Typing*. Faculty of Mathematics and Informatics, KUN. 1997-07

A.W. Heerink. *Ins and Outs in Refusal Testing*. Faculty of Computer Science, UT. 1998-01

G. Naumoski and W. Alberts. *A Discrete-Event Simulator for Systems Engineering*. Faculty of Mechanical Engineering, TUE. 1998-02

J. Verriet. *Scheduling with Communication for Multiprocessor Computation*. Faculty of Mathematics and Computer Science, UU. 1998-03

J.S.H. van Gageldonk. *An Asynchronous Low-Power 80C51 Microcontroller*. Faculty of Mathematics and Computing Science, TUE. 1998-04

A.A. Basten. *In Terms of Nets: System Design with Petri Nets and Process Algebra*. Faculty of Mathematics and Computing Science, TUE. 1998-05

E. Voermans. *Inductive Datatypes with Laws and Subtyping – A Relational Model*. Faculty of Mathematics and Computing Science, TUE. 1999-01

H. ter Doest. *Towards Probabilistic Unification-based Parsing*. Faculty of Computer Science, UT. 1999-02

J.P.L. Segers. *Algorithms for the Simulation of Surface Processes*. Faculty of Mathematics and Computing Science, TUE. 1999-03

C.H.M. van Kemenade. *Recombinative Evolutionary Search*. Faculty of Mathematics and Natural Sciences, Univ. Leiden. 1999-04

E.I. Barakova. *Learning Reliability: a Study on Indecisiveness in Sample Selection*. Faculty of Mathematics and Natural Sciences, RUG. 1999-05

M.P. Bodlaender. *Schedulere Optimization in Real-Time Distributed Databases*. Faculty of Mathematics and Computing Science, TUE. 1999-06

M.A. Reniers. *Message Sequence Chart: Syntax and Semantics*. Faculty of Mathematics and Computing Science, TUE. 1999-07

J.P. Warners. *Nonlinear approaches to satisfiability problems*. Faculty of Mathematics and Computing Science, TUE. 1999-08

J.M.T. Romijn. *Analysing Industrial Protocols with Formal Methods*. Faculty of Computer Science, UT. 1999-09

P.R. D'Argenio. *Algebras and Automata for Timed and Stochastic Systems*. Faculty of Computer Science, UT. 1999-10

G. Fábián. *A Language and Simulator for Hybrid Systems*. Faculty of Mechanical Engineering, TUE. 1999-11

J. Zwanenburg. *Object-Oriented Concepts and Proof Rules*. Faculty of Mathematics and Computing Science, TUE. 1999-12

R.S. Venema. *Aspects of an Integrated Neural Prediction System*. Faculty of Mathematics and Natural Sciences, RUG. 1999-13

J. Saraiva. *A Purely Functional Implementation of Attribute Grammars*. Faculty of Mathematics and Computer Science, UU. 1999-14

R. Schiefer. *Viper, A Visualisation Tool for Parallel Progam Construction*. Faculty of Mathematics and Computing Science, TUE. 1999-15

K.M.M. de Leeuw. *Cryptology and Statecraft in the Dutch Republic*. Faculty of Mathematics and Computer Science, UvA. 2000-01

T.E.J. Vos. *UNITY in Diversity. A stratified approach to the verification of distributed algorithms*. Faculty of Mathematics and Computer Science, UU. 2000-02

W. Mallon. *Theories and Tools for the Design of Delay-Insensitive Communicating Processes*. Faculty of Mathematics and Natural Sciences, RUG. 2000-03

W.O.D. Griffioen. *Studies in Computer Aided Verification of Protocols*. Faculty of Science, KUN. 2000-04

P.H.F.M. Verhoeven. *The Design of the MathSpad Editor*. Faculty of Mathematics and Computing Science, TUE. 2000-05

J. Fey. *Design of a Fruit Juice Blending and Packaging Plant*. Faculty of Mechanical Engineering, TUE. 2000-06

M. Franssen. *Cocktail: A Tool for Deriving Correct Programs*. Faculty of Mathematics and Computing Science, TUE. 2000-07

P.A. Olivier. *A Framework for Debugging Heterogeneous Applications*. Faculty of Natural Sciences, Mathematics and Computer Science, UvA. 2000-08

E. Saaman. *Another Formal Specification Language*. Faculty of Mathematics and Natural Sciences, RUG. 2000-10

M. Jelasity. *The Shape of Evolutionary Search Discovering and Representing Search Space Structure*. Faculty of Mathematics and Natural Sciences, UL. 2001-01

R. Ahn. *Agents, Objects and Events a computational approach to knowledge, observation and communication*. Faculty of Mathematics and Computing Science, TU/e. 2001-02

M. Huisman. *Reasoning about Java programs in higher order logic using PVS and Isabelle*. Faculty of Science, KUN. 2001-03

I.M.M.J. Reymen. *Improving Design Processes through Structured Reflection*. Faculty of Mathematics and Computing Science, TU/e. 2001-04

S.C.C. Blom. *Term Graph Rewriting: syntax and semantics*. Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2001-05

R. van Liere. *Studies in Interactive Visualization*. Faculty of Natural Sciences, Mathematics and Computer Science, UvA. 2001-06

A.G. Engels. *Languages for Analysis and Testing of Event Sequences*. Faculty of Mathematics and Computing Science, TU/e. 2001-07

J. Hage. *Structural Aspects of Switching Classes*. Faculty of Mathematics and Natural Sciences, UL. 2001-08

M.H. Lamers. *Neural Networks for Analysis of Data in Environmental Epidemiology: A Case-study into Acute Effects of Air Pollution Episodes*. Faculty of Mathematics and Natural Sciences, UL. 2001-09

T.C. Ruys. *Towards Effective Model Checking*. Faculty of Computer Science, UT. 2001-10

D. Chkliaev. *Mechanical verification of concurrency control and recovery protocols*. Faculty of Mathematics and Computing Science, TU/e. 2001-11

M.D. Oostdijk. *Generation and presentation of formal mathematical documents*. Faculty of Mathematics and Computing Science, TU/e. 2001-12

A.T. Hofkamp. *Reactive machine control: A simulation approach using χ*. Faculty of Mechanical Engineering, TU/e. 2001-13

D. Bošnački. *Enhancing state space reduction techniques for model checking*. Faculty of Mathematics and Computing Science, TU/e. 2001-14

M.C. van Wezel. *Neural Networks for Intelligent Data Analysis: theoretical and experimental aspects*. Faculty of Mathematics and Natural Sciences, UL. 2002-01

V. Bos and J.J.T. Kleijn. *Formal Specification and Analysis of Industrial Systems*. Faculty of Mathematics and Computer Science and Faculty of Mechanical Engineering, TU/e. 2002-02

T. Kuipers. *Techniques for Understanding Legacy Software Systems*. Faculty of Natural Sciences, Mathematics and Computer Science, UvA. 2002-03

S.P. Luttik. *Choice Quantification in Process Algebra*. Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2002-04

R.J. Willemen. *School Timetable Construction: Algorithms and Complexity*. Faculty of Mathematics and Computer Science, TU/e. 2002-05

M.I.A. Stoelinga. *Alea Jacta Est: Verification of Probabilistic, Real-time and Parametric Systems*. Faculty of Science, Mathematics and Computer Science, KUN. 2002-06

N. van Vugt. *Models of Molecular Computing*. Faculty of Mathematics and Natural Sciences, UL. 2002-07

A. Fehnker. *Citius, Vilius, Melius: Guiding and Cost-Optimality in Model Checking of Timed and Hybrid Systems*. Faculty of Science, Mathematics and Computer Science, KUN. 2002-08

R. van Stee. *On-line Scheduling and Bin Packing*. Faculty of Mathematics and Natural Sciences, UL. 2002-09

D. Tauritz. *Adaptive Information Filtering: Concepts and Algorithms*. Faculty of Mathematics and Natural Sciences, UL. 2002-10

M.B. van der Zwaag. *Models and Logics for Process Algebra*. Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2002-11

J.I. den Hartog. *Probabilistic Extensions of Semantical Models*. Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2002-12

L. Moonen. *Exploring Software Systems*. Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2002-13

J.I. van Hemert. *Applying Evolutionary Computation to Constraint Satisfaction and Data Mining*. Faculty of Mathematics and Natural Sciences, UL. 2002-14

S. Andova. *Probabilistic Process Algebra*. Faculty of Mathematics and Computer Science, TU/e. 2002-15