

# Isomorphisms between Predicate and State Transformers

Marcello Bonsangue<sup>1\*</sup> and Joost N. Kok<sup>2</sup>

<sup>1</sup> CWI, P.O. Box 4079, 1009 AB Amsterdam, The Netherlands. [marcello@cwi.nl](mailto:marcello@cwi.nl)

<sup>2</sup> Utrecht University, Department of Computer Science, P.O. Box 80.089, 3508 TB Utrecht, The Netherlands. [joost@cs.ruu.nl](mailto:joost@cs.ruu.nl)

**Abstract.** We study the relation between state transformers based on directed complete partial orders and predicate transformers. Concepts like ‘predicate’, ‘liveness’, ‘safety’ and ‘predicate transformers’ are formulated in a topological setting. We treat state transformers based on the Hoare, Smyth and Plotkin power domains and consider continuous, monotonic and unrestricted functions. We relate the transformers by isomorphisms thereby extending and completing earlier results and giving a complete picture of all the relationships.

## 1 Introduction

In this paper we give a full picture of the relationship between state transformers and predicate transformers. For the state transformers we consider the Hoare, Smyth and Plotkin power domains. We give a full picture in the sense that we consider algebraic directed complete partial orders (with a bottom element) (and not only flat domains), we consider not only continuous state transformers, but also the monotonic ones and the full function space, we do not restrict to bounded nondeterminism, and we treat all the three power domains with or without empty set. The first item is important when we want to use domains for concurrency semantics. The second and third item give more freedom in the sense that we can use these transformations also for specification purposes without constraints on computability. Having the empty set in a power domain can be important to treat deadlock. Our treatment includes the Plotkin power domain.

For state transformers we use an extension of the standard power domains. For predicate transformers we start from the (informal) classification of predicates in liveness and safety predicates of Lamport [Lam77]. Later Smyth [Smy83] followed by [AS85, Kwi91] used topology to formalize this classification. Also we use topology for defining predicates and safety and liveness predicate transformers. We consider predicate transformers with predicates that are the intersection of safety and liveness predicates.

---

\* The research of this author was supported by a grant of the Consiglio Nazionale delle Ricerche (CNR), Italy, announcement no. 203.15.3 of 15/2/90.

We prove that the Hoare state transformers are isomorphic to safety predicate transformers, the Smyth state transformers are isomorphic to the liveness predicate transformers, and that the Plotkin state transformers are isomorphic to the “intersection” predicate transformers. So for the first time we are able to give a full picture of all the relationships filling several gaps that were present in the literature.

Next we discuss how this paper is related to previous work. Power domains for dcpo’s were introduced in [Plo76], [Smy78] and [Plo81]. Our power domains are slightly more general in the sense that we do not restrict to non-empty (Scott-) compact sets. Besides the standard ways of adding the empty set to the Smyth [Smy83] and to the Plotkin [MM79, Plo81, Abr91] power domains, we also add the empty set in all the three power domains as a separate element, comparable only with itself and with the bottom.

Predicate transformers were introduced in [Dij76] with a series of healthiness conditions. Back and von Wright [Bac80, vW90] use only the monotonicity restriction on predicate transformers. They use predicate transformers for refinement and provide a nice lattice theoretical framework. Nelson [Nel89] has (for the flat case) used “compatible” pairs of predicate transformers for giving semantics to a language with backtracking. Smyth [Smy83] introduced predicate transformers (with the Dijkstra healthiness conditions) for non-flat domains. Our definition of predicate transformers is parametric with respect to the collection of predicates (observable, liveness and safety). Furthermore, a new (generalization) of the multiplicativity restriction is introduced and a generalization of “compatible” pairs of predicate transformers is given.

Isomorphisms between state and predicate transformers have been given for the flat case of the Smyth power domain in [Plo79] (and for countable nondeterminism in [AP86]), and for the flat case of the Hoare power domain in [Plo81]. Also De Bakker and De Roever [Bak80, Roe76] studied (from a semantical point of view) for the flat case the relation between state transformer and predicate transformer semantics. Moreover, for the flat case of the Plotkin power domain we have proposed an isomorphism in [BK92].

For the general case of the compact Smyth power domain in the paper [Smy83] an isomorphism is given for continuous state transformers. He uses a topological technique which Plotkin later used in [Plo81] for the continuous Hoare state transformers. A recent work includes an operational point of view in Van Breugel [Bre93]. In the present paper we give some new isomorphisms for the Hoare and the Smyth power domains, showing also how the previous ones can be obtained as combinations of the new isomorphisms. Our definition of multiplicativity for predicate transformers permits us to use a technique similar to that used for the flat case. Furthermore we give isomorphisms for the Plotkin power domain. As far as we know no isomorphism was known for the non-flat Plotkin power domain (as for example is remarked in [Plo81] and in [Smy83]).

For reasons of space, proofs are not given in this paper. They can be found in [BK93].

## 2 Mathematical Preliminaries

We introduce some basic notions on domain theory and topology. For a more detailed discussion on domain theory consult for example [Plo81], and for topology we refer to [Eng77].

Let  $P$  be a set ordered by  $\sqsubseteq_P$ ,  $x \in P$  and let  $A$  be a subset of  $P$ . Define  $x \uparrow = \{y \mid y \in P \wedge x \sqsubseteq y\}$  and  $A \uparrow = \bigcup \{x \uparrow \mid x \in A\}$ . A set  $A$  is called upper-closed if  $A = A \uparrow$ . A subset  $A$  of a partially ordered set  $P$  is said to be *directed* if it is non empty and every finite subset of  $A$  has an upper bound in  $A$ .  $P$  is a (pointed) *directed complete partially order set* (dcpo) if there exists a least element  $\perp_P$  and every directed subset  $A$  of  $P$  has least upper bound (lub)  $\bigsqcup A$ . A directed set  $A$  is *eventually constant* if  $\bigsqcup A \in A$ .

An element  $b$  of a dcpo  $P$  is *finite* if for every directed set  $A \subseteq P$ ,  $b \sqsubseteq \bigsqcup A$  implies  $b \sqsubseteq x$  for some  $x \in A$ . The set of all finite elements of  $P$  is denoted by  $B_P$  and is called *base*. A dcpo  $P$  is *algebraic* if for every element  $x \in P$  the set  $\{b \mid b \in B_P \wedge b \sqsubseteq x\}$  is directed and has least upper bound  $x$ ; it is  $\omega$ -*algebraic* if it is algebraic and its base is denumerable.

Let  $P, Q$  be two partially ordered sets. A function  $f : P \rightarrow Q$  is *monotone* (denoted by  $f : P \rightarrow_m Q$ ) if for all  $x, y \in P$  with  $x \sqsubseteq_P y$  we have  $f(x) \sqsubseteq_Q f(y)$ . If  $P$  is a dcpo we say  $f$  is *continuous* (denoted by  $f : P \rightarrow_c Q$ ) if  $f(\bigsqcup A) = \bigsqcup f(A)$  for each directed set  $A \subseteq P$ ; moreover  $f$  is *stabilizing* (denoted by  $f : P \rightarrow_{c_s} Q$ ) if it is continuous and for every directed set  $A \subseteq P$   $f(A)$  is an eventually constant directed set in  $Q$ . If  $f : P \rightarrow_c Q$  is continuous then  $f$  is monotone. Given a set  $\beta \subseteq Q$ , a continuous function  $f : P \rightarrow_c Q$  is said  $\beta$ -*algebraic* (denoted by  $f : P \rightarrow_{a(\beta)} Q$ ) if for every directed set  $S \subseteq P$  and for every  $q \in \beta$  such that  $q \sqsubseteq f(\bigsqcup S)$  there exists an  $x \in S$  such that  $q \sqsubseteq f(x)$ . Clearly, for  $Q$  an algebraic dcpo with base  $B_Q$ , a function  $f : P \rightarrow Q$  is continuous if and only if  $f$  is  $B_Q$ -algebraic. A function  $f$  is *strict* (denoted by  $f : P \rightarrow_s Q$ ) if  $f(\perp_P) = \perp_Q$ ; dually  $f$  is *top preserving* (denoted by  $f : P \rightarrow_t Q$ ) if and only if  $f(\top_P) = \top_Q$ .

Let  $P$  be a dcpo and  $f : P \rightarrow P$ . We denote by  $\mu.f$  the *least fixed point* of  $f$ , that is,  $f(\mu.f) = \mu.f$  and for every other  $x \in P$  such that  $f(x) = x$  then  $\mu.f \sqsubseteq x$ . For a monotone function  $f : P \rightarrow_m P$ , where  $P$  is a dcpo, the least fixed point of  $f$  always exists and can be calculated by iteration, that is, there exists an ordinal  $\lambda$  such that  $\mu.f = f^\lambda$ , where the  $\alpha$ -iteration of  $f$  is defined by  $f^\alpha = f(\bigsqcup_{k < \alpha} f^k)$  for every ordinal  $\alpha$  [HP72]. If  $f$  is also continuous then  $\lambda \leq \omega$ . It can be of interest to consider also non-monotonic functions, at least when they are representation as quotient of some monotonic functions between dcpo, as shown in the following transfer lemma [BK92]: let  $P$  be a dcpo and  $Q$  be a partially ordered set,  $f : P \rightarrow_m P$  be a monotone function,  $h : P \rightarrow_c Q$  be an onto and continuous function and  $g : Q \rightarrow Q$  be a (possibly non monotone) function such that  $g \circ h = h \circ f$ . Then for every ordinal  $\alpha$  the  $\alpha$ -iteration from the bottom element  $g^\alpha$  exists. Moreover, if for each  $y \in Q$  the partially ordered set  $h^{-1}(y) \subseteq P$  is finite or has either the bottom or the top element then the smallest fixed point  $\mu.g$  exists and  $\mu.g = h(\mu.f)$ .

We now introduce some basic topological notions. A *topology*  $\mathbf{O}(X)$  on a set  $X$  is a collection of subsets of  $X$  that is closed under finite intersections and

arbitrary unions. The pair  $(X, \mathbf{O}(X))$  is called *topological space* and the elements of  $\mathbf{O}(X)$  are the *open sets* of the space  $X$ . A *base* of a topology  $\mathbf{O}(X)$  on  $X$  is a subset  $\mathbf{B} \subseteq \mathbf{O}(X)$  such that every open set is the union of elements of  $\mathbf{B}$ . A set  $S \subseteq X$  is *dense* if and only if  $X \setminus S$  contains no non-empty open sets. A  $G_\delta$ -set is a countable intersection of open sets.

For example, given a partially ordered set  $X$ , its *discrete* topology is  $\mathbf{O}_d(X) = \mathcal{P}(X)$  while its *Alexandroff topology*  $\mathbf{O}_{A1}(X)$  consists of all the upper-closed subsets of  $X$ . If  $X$  is a dcpo, a finer topology of  $X$  is the Scott topology  $\mathbf{O}_{Sc}(X)$ , where  $o \in \mathbf{O}_{Sc}(X)$  if and only if  $o$  is upper-closed and for any directed set  $S \subseteq X$  if  $\bigsqcup S \in o$  then  $S \cap o \neq \emptyset$ . Let  $A$  be a collection of subsets of  $X$ ; the closure under arbitrary intersection of  $A$  is denoted by  $A^\cap = \{Q \mid Q = \bigcap A' \wedge A' \subseteq A\}$ .

We can describe a topology by its closed sets instead of its open sets. A subset of a set  $X$  is *closed* if and only if it is the complement of an open set of a given topology on  $X$ . The collection of closed sets of a topological space is denoted by  $\mathbf{C}(X)$  and, dually to the case of open sets, is closed under finite unions and arbitrary intersections. For every  $A \subseteq X$  there exists a closed set  $c$  and a dense set  $d$  such that  $A = c \cap d$ .

For example, given a dcpo  $P$  the closed sets of the Alexandroff topology are all the lower closed sets, while a set  $c \subseteq P$  is closed with respect to the Scott topology if  $c$  is lower closed and for every directed set  $S \subseteq P$  if  $S \subseteq c$  then  $\bigsqcup S \in c$ .

Let  $\mathbf{O}(X)$  be a topology on a set  $X$ . A subset  $A \subseteq X$  is *compact* in  $\mathbf{O}(X)$  if and only if for every collection of open sets  $o_i \in \mathbf{O}(X)$  with  $i \in I$  such that  $A \subseteq \bigcup_I o_i$  there exists a finite subcollection  $o_j$  such that  $A \subseteq \bigcup_J o_j$ . For example  $A \subseteq X$  is compact in  $\mathbf{O}_d(X)$  if and only if it is a finite set. The intersection of a closed set with a compact one is always compact.

### 3 Predicates and Predicate Transformers

A *predicate*  $P$  is a function from a set  $X$  to the boolean set  $\mathbf{Bool} = \{tt, ff\}$  or, equivalently, is a subset of  $X$ . Topology provides an elegant way of expressing predicates of programs (see [Smy83], [Kwi91]) in which the open sets of a topological space  $X$  are seen as the *computable predicates*. Taking different topologies corresponds to different restrictions on the function space. For example, with  $ff \sqsubseteq tt$  we have that  $\mathbf{O}_d(X)$  is isomorphic to the set of all the predicates from  $X$  to  $\mathbf{Bool}$ ,  $\mathbf{O}_{A1}(X)$  is isomorphic to the set of all the monotone predicates from  $X$  to  $\mathbf{Bool}$  and  $\mathbf{O}_{Sc}(X)$  is isomorphic to the set of all the continuous predicates from  $X$  to  $\mathbf{Bool}$ .

In [Lam77] two classes of predicates were introduced: *safety* and *liveness predicates*. In the topological view of Smyth [Smy83, Smy92] closed sets represent *safety predicates* while *liveness predicates* are  $G_\delta$  sets. We take arbitrary intersections of open sets as liveness predicates (saturated sets). This differs also from [AS85] where liveness predicates are dense sets (the complement does not contain non-empty open sets). In [Kwi91] liveness predicates are also  $G_\delta$ -sets.

In this paper we consider algebraic dcpo's together with the Scott topology. The Scott-closed sets are the safety predicates and are ordered by  $\supseteq$ . The Scott-open sets of a dcpo  $Y$  represent the computable (observable) predicates and are ordered by  $\subseteq$ . They are *finitary* in the sense that  $y \in o$  if and only if there exists a  $b \in B_Y$  such that  $b \in o$  and  $b \sqsubseteq y$ . In other words, a predicate  $P$  is finitary if we can test whether  $P$  holds for  $y$  by testing only the finite elements smaller than  $y$ . Liveness predicates are the arbitrary intersection of Scott-open sets (that is Alexandroff open sets) and are ordered by  $\subseteq$ .

Consider for example the set of sequences (finite and infinite) over an alphabet  $\Sigma$  ordered by the prefix ordering (for more examples see [Kwi91]).

- Safety predicate: *always*  $a = \{x \mid x = a^* \vee x = a^\omega\}$  (Scott closed),
- Observable predicate: *eventually*  $a = \{xa \mid x \in \Sigma^*\} \uparrow$  (Scott open),
- Observable predicate: *start with*  $x = x \uparrow$  (Scott open), where  $x \in \Sigma^*$ ,
- Liveness predicate: *infinitely often*  $a = \bigcap_{n \in \mathbb{N}} \{x \mid x \in \Sigma^* \wedge |x|_a = n\} \uparrow$  (Alexandroff open but not Scott open),
- Neither safety nor liveness predicate: *always*  $a$  but *starting with*  $x = \text{always } a \wedge \text{start with } x$ .

Let  $P(Y)$  and  $P(X)$  be two collections of predicates on the space  $Y$  and  $X$ , respectively. We define *predicate transformers* as the monotone functions from  $P(Y)$  to  $P(X)$ . Another natural restriction (besides monotonicity) in the case that  $Y \in P(Y)$  is to require that a predicate transformer must be top-preserving. Predicate transformers mapping observable predicates to observable predicates are denoted by  $P(Y) \rightarrow_O P(X)$ .

A predicate transformer  $\pi : P(Y) \rightarrow P(X)$  is *multiplicative* (denoted by  $\pi : P(Y) \rightarrow_M P(X)$ ) if and only if for collections of predicates  $P, Q \subseteq P(Y)$  if  $\bigcap P \subseteq \bigcap Q$  then  $\bigcap_{p \in P} \pi(p) \subseteq \bigcap_{q \in Q} \pi(q)$ . If  $P(Y)$  is closed under arbitrary intersection then  $\pi$  is multiplicative if and only if  $\bigcap_{p \in P} \pi(p) = \pi(\bigcap P)$  for every collection of predicates  $P \subseteq P(Y)$ . If  $Y \in P(Y)$  then  $\pi$  multiplicative implies  $\pi$  top preserving. Given a predicate transformer  $\pi : P(Y) \rightarrow P(X)$  its *dual*  $\pi^\circ : P(Y)^\circ \rightarrow P(X)^\circ$  is given by  $\pi^\circ(p) = X \setminus \pi(Y \setminus p)$ , for every  $p \in P(Y)^\circ = \{Y \setminus q \mid q \in P(Y)\}$ . A predicate transformer is *additive* (denoted by  $\pi : P(Y) \rightarrow_A P(X)$ ) if and only if its dual is multiplicative.

A predicate transformer  $\pi : P(Y) \rightarrow P(X)$  is *intersection extensible* (denoted by  $\pi : P(Y) \rightarrow_I P(X)$ ) if  $\bigcap_{p \in P} \pi(p) \in P(X)$  for every collection of predicates  $P \subseteq P(Y)$ . Dually, if  $\bigcup_{p \in P} \pi(p) \in P(Y)$  then  $\pi$  is called *union extensible* (denoted by  $\pi : P(Y) \rightarrow_U P(X)$ ).

Intuitively, multiplicative predicate transformers  $\pi : P(Y) \rightarrow P(X)$  preserve the logical ' $\forall$ ' on predicates on  $Y$ , while the additive ones preserve the logical ' $\exists$ ' (even if they are not  $\exists$  predicates in  $P(Y)$  or  $P(X)$ ). If  $\pi$  is also intersection (union) extensible then the logical ' $\forall$ ' (' $\exists$ ') of  $\pi$  of an arbitrary collection of predicates on  $Y$  is always a predicate in  $P(X)$ .

We now define a restricted version of the Cartesian product on (multiplicative) predicate transformers by requiring (multiplicativity) monotonicity on the intersection.

**Definition 1.** Let  $P_1(Y), P_2(Y)$  be two collections of predicates on  $Y$  and  $Q_1(X), Q_2(X)$  be two collections of predicates on  $X$ . Define  $(P_1(Y) \rightarrow_m Q_1(X)) \otimes (P_2(Y) \rightarrow_m Q_2(X))$  as the subset of  $(P_1(Y) \rightarrow_m Q_1(X)) \times (P_2(Y) \rightarrow_m Q_2(X))$  given by:

$$\{(\pi, \rho) \mid \forall p, p' \in P_1(Y), q, q' \in P_2(Y) : p \cap q \subseteq p' \cap q' \Rightarrow \pi(p) \cap \rho(q) \subseteq \pi(p') \cap \rho(q')\}.$$

Similarly, define  $(P_1(Y) \rightarrow_M Q_1(X)) \otimes_M (P_2(Y) \rightarrow_M Q_2(X))$  as

$$\begin{aligned} \{(\pi, \rho) \mid \forall P, P' \subseteq P_1(Y), Q, Q' \subseteq P_2(Y) : \bigcap P \cap \bigcap Q \subseteq \bigcap P' \cap \bigcap Q' \\ \Rightarrow \bigcap_{p \in P} \pi(p) \cap \bigcap_{q \in Q} \rho(q) \subseteq \bigcap_{p' \in P'} \pi(p') \cap \bigcap_{q' \in Q'} \rho(q')\}. \end{aligned}$$

They are ordered pointwise.

Now we come to the definition of safety and liveness predicate transformers used in this paper. Let  $X$  and  $Y$  be algebraic dcpo's. The liveness predicate transformers are functions in  $\mathbf{O}_{Sc}(Y)^\cap \rightarrow_{OM} \mathbf{O}(X)^\cap$  for some topology  $\mathbf{O}(X)$  on  $X$ . They are ordered pointwise by subset inclusion. The safety predicate transformers are functions in  $\mathbf{C}_{Sc}(Y) \rightarrow_M \mathbf{C}(X)$  for some collection of closed set  $\mathbf{C}(X)$  on  $X$ . They are ordered pointwise by superset inclusion.

We can define liveness and safety predicate transformers in terms of observable predicate transformers since  $(\mathbf{O}_{Sc}(Y)^\cap \rightarrow_{OM} \mathbf{O}(X)^\cap) \cong (\mathbf{O}_{Sc}(Y) \rightarrow_M \mathbf{O}(X))$  and  $(\mathbf{C}_{Sc}(Y) \rightarrow_M \mathbf{C}(X)) \cong (\mathbf{O}_{Sc}(Y) \rightarrow_A \mathbf{O}(X))$ . We can also change the subset order of the liveness predicate transformers to the deadlock order of [BK92], where for every  $\pi_1, \pi_2 \in \mathbf{O}_{Sc}(Y) \rightarrow_M \mathbf{O}(X)$ ,  $\pi_1 \sqsubseteq_{LD} \pi_2$  if

$$(\pi_1(\emptyset) \subseteq \pi_2(\emptyset)) \wedge (\forall o \in \mathbf{O}_{Sc}(Y) : o \neq Y \Rightarrow \pi_1(o) \setminus \pi_1(\emptyset) \subseteq \pi_2(o) \setminus \pi_2(\emptyset)).$$

and for safety predicate transformers  $\rho_1, \rho_2$ ,  $\rho_1 \sqsubseteq_{SD} \rho_2$  if

$$(\rho_1(\emptyset) \subseteq \rho_2(\emptyset)) \wedge (\forall c \in \mathbf{C}_{Sc}(Y) : c \neq \emptyset \Rightarrow \rho_1(c) \supseteq \rho_2(c) \setminus \rho_1(\emptyset)).$$

## 4 State Transformers

In this section we give generalizations of the three 'classical' power domains on  $\omega$ -algebraic dcpo's, the so-called Hoare, Smyth and Plotkin power domains ([Plo76], [Smy78] and [Plo81]).

Let  $X$  be an algebraic dcpo and  $A \subseteq X$ . Define  $\bar{A} = \{x \mid \forall b \in B_X : b \sqsubseteq x \Rightarrow \exists x_b \in A : b \sqsubseteq x_b\}$  and  $A^* = \{x \mid (\exists x' \in A : x' \sqsubseteq x) \wedge (\forall b \in B_X : b \sqsubseteq x \Rightarrow \exists x_b \in A : b \sqsubseteq x_b)\}$ . We have  $\bar{A} = A$  if and only if  $A \in \mathbf{C}_{Sc}(X)$ . Further  $A \subseteq A^*$ ,  $(A^*)^* = A^*$ , and  $A = A^* \Leftrightarrow A = A \uparrow \cap \bar{A}$ . Next we define the power domains:

**Definition 2.** Let  $X$  be an algebraic dcpo. Define

- the Hoare power domain  $\mathcal{H}(X) = \langle \{A \mid A \subseteq X \wedge A = \bar{A}\}, \sqsubseteq_H \rangle$ , where  $A \sqsubseteq_H B$  if  $A \subseteq B$ ,
- the Smyth power domain  $\mathcal{S}(X) = \langle \{A \mid A \subseteq X \wedge A = A \uparrow\}, \sqsubseteq_S \rangle$ , where  $A \sqsubseteq_S B$  if  $A \supseteq B$ ,

- the Plotkin power domain  $\mathcal{P}(X) = \langle \{A \mid A \subseteq X \wedge A = A^*\}, \sqsubseteq_P \rangle$ , where  $A \sqsubseteq_P B$  if  $A \uparrow \sqsubseteq_S B \uparrow$  and  $\bar{A} \sqsubseteq_H \bar{B}$ .

If we consider only bounded nondeterminism then we can restrict the power domains to those sets that are compact in the Scott topology (denoted by the subscript *co*). Since every Scott closed set of a dcpo is compact in the Scott topology we have  $\mathcal{H}_{co}(X) = \mathcal{H}(X)$ . The standard definitions of the Hoare, Smyth and Plotkin power domains are  $\mathcal{H}^+(X)$ ,  $\mathcal{S}_{co}^+(X)$  and  $\mathcal{P}_{co}^+(X)$ , where the superscript  $+$  denotes that the power domains should be taken without the empty set. The same domains but with a slight different order are denoted by  $\mathcal{H}\delta(X)$ ,  $\mathcal{S}\delta(X)$  and  $\mathcal{P}\delta(X)$ . Their ordering are respectively given by

- $A \sqsubseteq_{H\delta} B$  if  $(A = \{\perp\}) \vee (A = \emptyset \Rightarrow B = \emptyset) \vee (A \neq \emptyset \wedge A \sqsubseteq_H B)$ ,
- $A \sqsubseteq_{S\delta} B$  if  $(A = X) \vee (A = \emptyset \Rightarrow B = \emptyset) \vee (B \neq \emptyset \wedge A \sqsubseteq_S B)$ ,
- $A \sqsubseteq_{P\delta} B$  if  $(A = \{\perp\}) \vee (A = \emptyset \Rightarrow B = \emptyset) \vee (A \neq \emptyset \wedge A \sqsubseteq_P B)$ .

Most of the usual operations (such as the sequential composition) are not monotone w.r.t.  $\sqsubseteq_{S\delta}$ . However, we can use the transfer lemma given in the Mathematical Preliminaries for calculating least fixed points [BK92]. For an algebraic dcpo  $X$ , the Hoare power domain is a complete lattice. Furthermore it is also an algebraic dcpo with as finite elements the Scott closure of finite subsets of  $B_X$ . Also the Smyth power domain is a complete lattice, but in general not an algebraic dcpo. However its restriction  $\mathcal{S}_{co}(X)$  is an algebraic dcpo with finite elements the upper closure of finite subsets of  $B_X$  [Smy78]. In general, the Plotkin power domain is neither a complete lattice nor a dcpo (there is no bottom element because the empty set is related only with itself and  $\{\perp\}$  is less than any other set different from empty set). However if  $X$  is algebraic then  $\mathcal{P}_{co}^+(X)$  is an algebraic dcpo with finite elements the \*-closure of finite subsets of  $B_X$  (see [Plo76] and extensions in [Hrb87],[Hrb89]). Furthermore,  $\mathcal{P}\delta_{co}(X)$  coincides with the standard way of adding the empty set to the Plotkin power domain [MM79], [Plo81] and also [Abr91].

*State transformers* are functions (ordered pointwise) from an algebraic dcpo  $X$  to one of the power domains over an algebraic dcpo  $Y$ .

## 5 Relations

In this section we give the isomorphisms between the state transformers and predicate transformers domains. We start with the relation between safety predicate transformers and the Hoare state transformers:

**Theorem 3.** *Let  $X$  and  $Y$  be two algebraic dcpo's. We have the following order-isomorphisms:*

1.  $X \rightarrow \mathcal{H}(Y) \cong \mathbf{C}_{S_c}(Y) \rightarrow_M \mathbf{C}_d(X)$ ,
2.  $X \rightarrow \mathcal{H}^+(Y) \cong \mathbf{C}_{S_c}(Y) \rightarrow_{sM} \mathbf{C}_d(X)$ ,
3.  $X \rightarrow_m \mathcal{H}(Y) \cong \mathbf{C}_{S_c}(Y) \rightarrow_M \mathbf{C}_{At}(X)$ ,
4.  $X \rightarrow_c \mathcal{H}(Y) \cong \mathbf{C}_{S_c}(Y) \rightarrow_M \mathbf{C}_{S_c}(X)$ ,

$$5. X \rightarrow_{c_s} \mathcal{H}(Y) \cong \mathbf{C}_{S_c}(Y) \rightarrow_{UM} \mathbf{C}_{S_c}(X).$$

In all cases the isomorphism is given by the function  $\gamma: \gamma(m)(c) = \{x | m(x) \subseteq c\}$

The function  $\gamma$  is the generalization of the weakest liberal precondition and its inverse is given by  $\gamma^{-1}(\rho)(x) = \bigcap \{c | x \in \rho(c)\}$ . Because the isomorphism is always the same we can combine cases of the theorem (for example combining 2. and 4. we get the result of [Plo81]:  $X \rightarrow_c \mathcal{H}^+(Y) \cong \mathbf{C}_{S_c}(Y) \rightarrow_{sM} \mathbf{C}_{S_c}(X)$ ). Theorem 3 holds also if we substitute  $\mathcal{H}\delta(Y)$  for  $\mathcal{H}(Y)$  and we take  $\sqsubseteq_{SD}$  as order for the safety predicate transformers.

Now we relate liveness predicate transformers and Smyth state transformers:

**Theorem 4.** *Let  $X$  and  $Y$  be two algebraic dcpo's. We have the following order-isomorphisms:*

1.  $X \rightarrow \mathcal{S}(Y) \cong \mathbf{O}_{S_c}(Y) \rightarrow_M \mathbf{O}_d(X),$
2.  $X \rightarrow \mathcal{S}^+(Y) \cong \mathbf{O}_{S_c}(Y) \rightarrow_{sM} \mathbf{O}_d(X),$
3.  $X \rightarrow \mathcal{S}_{co}(Y) \cong \mathbf{O}_{S_c}(Y) \rightarrow_{cM} \mathbf{O}_d(X),$
4.  $X \rightarrow_m \mathcal{S}(Y) \cong \mathbf{O}_{S_c}(Y) \rightarrow_M \mathbf{O}_{Ai}(X),$
5.  $X \rightarrow_{a(\beta)} \mathcal{S}(Y) \cong \mathbf{O}_{S_c}(Y) \rightarrow_M \mathbf{O}_{S_c}(X),$
6.  $X \rightarrow_{c_s} \mathcal{S}(Y) \cong \mathbf{O}_{S_c}(Y) \rightarrow_{IM} \mathbf{O}_{S_c}(X),$

where  $\beta = \{B \uparrow \in \mathcal{S}(Y) | B \subseteq B_Y\}$ . In all cases the isomorphism is given by the function  $\omega: \omega(m)(o) = \{x | m(x) \subseteq o\}$

The function  $\omega$  is a generalization of the weakest precondition and its inverse is given by  $\omega^{-1}(\pi)(x) = \bigcap \{o | x \in \pi(o)\}$ . Also in this case we can combine 2., 3. and 5. to obtain the result of [Smy83], because  $\mathcal{S}_{co}(Y)$  is an algebraic dcpo with finite elements the upper closure of finite subset of  $B_Y$ , thus every continuous function from  $X$  to  $\mathcal{S}_{co}(Y)$  is also  $\beta$ -algebraic. Theorem 4 holds also if we substitute  $\mathcal{S}\delta(Y)$  for  $\mathcal{S}(Y)$  and we order of the liveness predicate transformer by  $\sqsubseteq_{LD}$ .

To prove these theorems we need the following extension of the *stability lemma* of Plotkin [Plo79, AP86]:

**Lemma 5.** *Let  $\pi: P(Y) \rightarrow_M P(X)$  be a multiplicative predicate transformer. Then  $x \in \pi(\hat{p}) \Leftrightarrow \bigcap \{p | x \in \pi(p)\} \subseteq \hat{p}$  for every  $\hat{p} \in P(Y)$  and  $x \in X$ .*

Finally we relate the Plotkin state transformers with pairs of safety and liveness predicate transformers:

**Theorem 6.** *Let  $X$  and  $Y$  be two algebraic dcpo's. We have the following order-isomorphisms:*

1.  $X \rightarrow \mathcal{P}(Y) \cong (\mathbf{O}_{S_c}(Y) \rightarrow_M \mathbf{O}_d(X)) \otimes_M (\mathbf{C}_{S_c}(Y) \rightarrow_M \mathbf{C}_d(X))$
2.  $X \rightarrow \mathcal{P}^+(Y) \cong (\mathbf{O}_{S_c}(Y) \rightarrow_{sM} \mathbf{O}_d(X)) \otimes_M (\mathbf{C}_{S_c}(Y) \rightarrow_{sM} \mathbf{C}_d(X)),$
3.  $X \rightarrow \mathcal{P}_{co}(Y) \cong (\mathbf{O}_{S_c}(Y) \rightarrow_{cM} \mathbf{O}_d(X)) \otimes_M (\mathbf{C}_{S_c}(Y) \rightarrow_M \mathbf{C}_d(X)),$
4.  $X \rightarrow_m \mathcal{P}(Y) \cong (\mathbf{O}_{S_c}(Y) \rightarrow_M \mathbf{O}_{Ai}(X)) \otimes_M (\mathbf{C}_{S_c}(Y) \rightarrow_M \mathbf{C}_{Ai}(X)),$

5.  $X \rightarrow_c \mathcal{P}_{co}(Y) \cong (\mathbf{O}_{Sc}(Y) \rightarrow_{cM} \mathbf{O}_{Sc}(X)) \otimes_M (\mathbf{C}_{Sc}(Y) \rightarrow_M \mathbf{C}_{Sc}(X))$ ,
6.  $X \rightarrow_{c_s} \mathcal{P}(Y) \cong (\mathbf{O}_{Sc}(Y) \rightarrow_{IM} \mathbf{O}_{Sc}(X)) \otimes_M (\mathbf{C}_{Sc}(Y) \rightarrow_{UM} \mathbf{C}_{Sc}(X))$ .

In all cases the isomorphism is given by the function  $\eta$ :

$$\eta(m)(o, c) = (\{x|m(x) \uparrow \subseteq o\}, \{x|\overline{m(x)} \subseteq c\})$$

The inverse of  $\eta$  is given by  $\eta^{-1}((\pi, \rho))(x) = \bigcap \{o|x \in \pi(o)\} \cap \bigcap \{c|x \in \rho(c)\}$ . Theorem 6 holds also if we substitute  $\mathcal{P}\delta(Y)$  for  $\mathcal{P}(Y)$  and we order the safety and the liveness predicate transformer respectively by  $\sqsubseteq_{SD}$  and  $\sqsubseteq_{LD}$ .

To prove this theorem we need a different *stability lemma*:

**Lemma 7.** *Let  $(\pi, \rho) : (P_1(Y) \rightarrow_M Q_1(X)) \otimes_M (P_2(Y) \rightarrow_M Q_2(X))$ . Then for every  $x \in X$ ,  $\hat{p} \in P_1(Y)$ , and  $\hat{q} \in P_2(Y)$  we have:*

1.  $x \in \pi(\hat{p}) \Leftrightarrow \bigcap \{p|x \in \pi(p)\} \cap \bigcap \{q|x \in \rho(q)\} \subseteq \hat{p}$ ,
2.  $x \in \rho(\hat{q}) \Leftrightarrow \bigcap \{p|x \in \pi(p)\} \cap \bigcap \{q|x \in \rho(q)\} \subseteq \hat{q}$ .

## 6 Conclusions and Future Work

We have proposed a formal definition of safety and liveness predicates and of predicate transformers following the line of [Smy83, Kwi91]. Furthermore we have give generalizations of the standard definitions of power domains and of state transformers, and which give us a complete series of isomorphisms between predicate and state transformers (including the Plotkin state transformers).

Future work includes: a generalization of the results to arbitrary topological spaces and applications of predicate transformers to non-flat domains for concurrency and communication.

**Acknowledgements:** We wish to thanks all the members of the Amsterdam Concurrency Group especially Jaco de Bakker, Jan Rutten, Daniele Turi, and Franck van Breugel, for discussions and suggestions about the contents of this paper. Thanks also to Peter Knijnenburg of Utrecht University and the anonymous referees for their helpful comments.

## References

- [Abr91] S. Abramsky. A domain equation for bisimulation. *Information and Computation*, 92:161–218, 1991.
- [AP86] K. R. Apt and G. Plotkin. Countable nondeterminism and random assignment. *Journal of the ACM*, 33(4):724–767, October 1986.
- [AS85] B. Alpern and F.B. Schneider. Defining liveness. *Information Processing Letters*, 21:181–185, 1985.
- [Bac80] R.-J.R. Back. *Correctness Preserving Program Refinements: Proof Theory and Applications*, volume 131 of *Mathematical Centre Tracts*. Mathematical Centre, Amsterdam, 1980.
- [Bak80] J. W. de Bakker. *Mathematical Theory of Program Corretness*. Prentice-Hall, 1980.

- [BK92] M. Bonsangue and J. N. Kok. Semantics, orderings and recursion in the weakest precondition calculus. Technical Report CS-R9267, Centre for Mathematics and Computer Science, Amsterdam, 1992. Extended abstract to appear in the proceedings of the Rex Workshop '92 'Semantics: Foundations and Applications' LNCS 666, 1993.
- [BK93] M. Bonsangue and J. N. Kok. Isomorphisms between state and predicate transformers. Technical report, Centre for Mathematics and Computer Science, Amsterdam, 1993. Available through anonymous ftp from ftp.cwi.nl.
- [Bre93] F. van Breugel. Relating state transformation semantics and predicate transformer semantics for parallel programs. To appear, 1993.
- [Dij76] E.W. Dijkstra. *A Discipline of Programming*. Prentice-Hall, 1976.
- [Eng77] R. Engelking. *General Topology*. Polish Scientific Publishers, 1977.
- [HP72] P. Hitchcock and D. Park. Induction rules and termination proofs. In *International Conference on Automata, Languages and Programming*, 1972.
- [Hrb87] K. Hrbacek. Convex Powerdomains I. *Information and computation*, 74:198–225, 1987.
- [Hrb89] K. Hrbacek. Convex Powerdomains II. *Information and computation*, 81:290–317, 1989.
- [Kwi91] M.Z. Kwiatowska. On topological characterization of behavioural properties. In G.M. Reed, A.W. Roscoe, and R.F. Wachter, editors, *Topology and Category Theory in Computer Sciences - Proc. Oxford Topology Symposium, June 1989*, pages 153–177. Oxford Science Publications, 1991.
- [Lam77] L. Lamport. Proving the correctness of a multiprocess programs. *IEEE Transaction on Software Eng.*, SE-3:125–143, 1977.
- [MM79] G. Milne and R. Milner. Concurrent processes and their syntax. *J. ACM*, 26, 2:302–321, 1979.
- [Nel89] G. Nelson. A generalization of Dijkstra's calculus. *ACM Transaction on Programming Languages and Systems*, 11 - 4:517–561, 1989.
- [Plo76] G. D. Plotkin. A powerdomain construction. *SIAM J. Comput.*, 5:452–487, 1976.
- [Plo79] G. D. Plotkin. Dijkstra's predicate transformer and Smyth's powerdomain. In *Proceedings of the Winter School on Abstract Software Specification*, volume 86 of *Lecture Notes in Computer Science*, pages 527–553. Springer-Verlag, Berlin, 1979.
- [Plo81] G.D. Plotkin. Post-graduate lecture notes in advanced domain theory (incorporating the "Pisa Notes"). Department of Computer Science, Univ. of Edinburgh, 1981.
- [Roe76] W.P. de Roever. Dijkstra's predicate transformer, non-determinism, recursion, and terminations. In *Mathematical foundations of computer science*, volume 45 of *Lecture Notes in Computer Science*, pages 472–481. Springer-Verlag, Berlin, 1976.
- [Smy78] M.B. Smyth. Power domains. *J. Comput. Syst. Sci.*, 16,1:23–36, 1978.
- [Smy83] M.B. Smyth. Power domains and predicate transformers: A topological view. In *Proceedings of ICALP '83 (Barcelona)*, volume 154 of *Lecture Notes in Computer Science*, pages 662–675. Springer-Verlag, Berlin, 1983.
- [Smy92] M.B. Smyth. Topology. In S. Abramsky, D.M. Gabbay, and T.S.E. Malbaum, editors, *Handbook of Logic in Computer Science*, volume I - Background: Mathematical Structures. Oxford University Press, 1992.
- [vW90] J. von Wright. *A Lattice-theoretical Basis for Program Refinement*. PhD thesis, Abo Akademi, 1990.