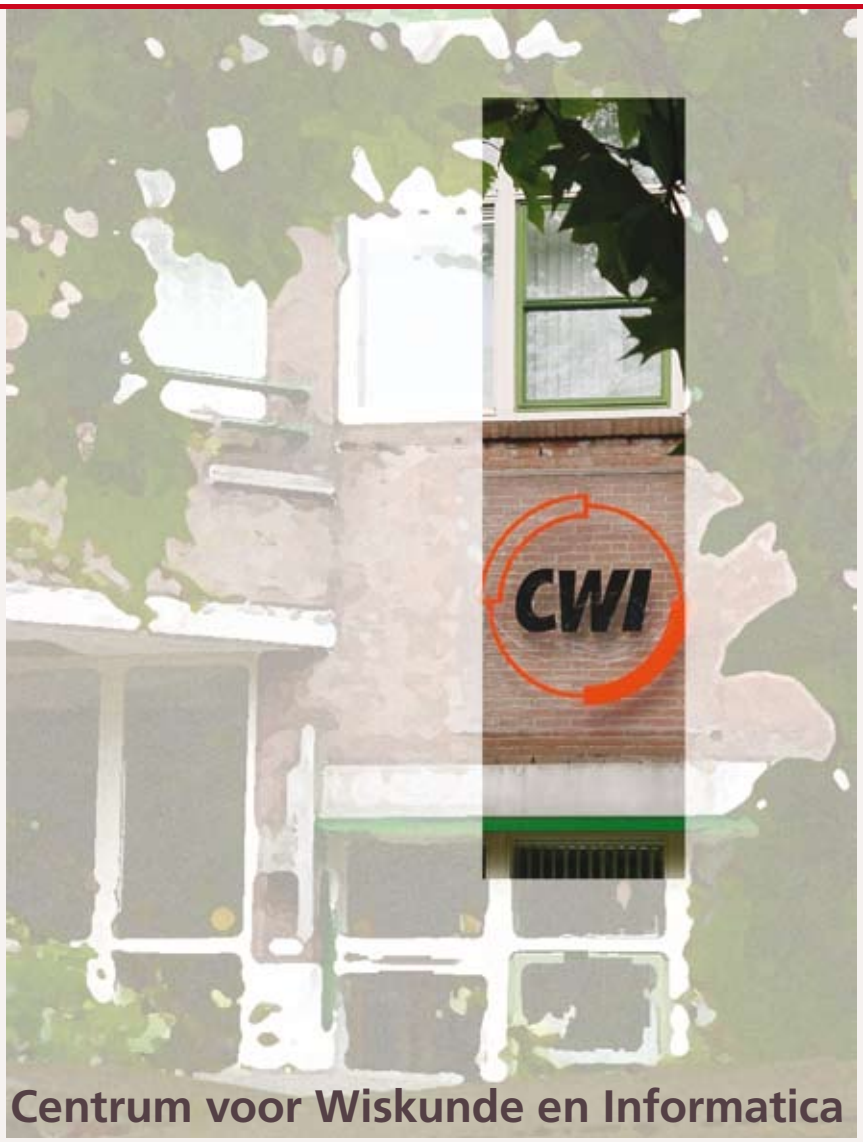
Centrum voor Wiskunde en Informatica

Annual Report 2006

Contents



Centrum voor Wiskunde en Informatica

Visiting Address	Kruislaan 413 1098 SJ Amsterdam The Netherlands
Postal Address	P.O. Box 94079 1090 GB Amsterdam The Netherlands
Telephone	+31 20 592 9333
Fax	+31 20 592 4199
Website	www.cwi.nl

Centrum voor Wiskunde en Informatica (CWI) is the national research institute for mathematics and computer science. It is supported by the Netherlands Organisation for Scientific Research (NWO).
CWI is a founding member of ERCIM, the European Research Consortium for Informatics and Mathematics. The institute is a member of the World Wide Web Consortium (W3C) and it manages the W3C Office in the Benelux. CWI is located at Science Park Amsterdam.

CONTENTS

Introduction 5

Overview 6
1. To conduct advanced research of societal and scientific relevance 8
2. To act as a 'breeding ground' for academic staff 13
3. To train young researchers 15
4. To transfer knowledge to society 21
5. To play a leading role in the Dutch and European mathematics and computer science scene 24
6. To increase public interest in mathematics and computer science 30

Research Highlights 34
Efficient health care 35
Models for better ships 39
Quantum information processing 43
Larger diamonds thanks to discrete mathematics 47

Appendices 50
Organization 51
Facts and figures 52
CWI clusters and themes 55
International and national research programmes 62

The CWI annual report series consists of:

- Annual Report (English), a full colour document giving a general overview of CWI's activities
- Overview Research Activities (English), a comprehensive enumeration of CWI's research
- Jaarverslag (Dutch), a supplement containing the social and financial report and the works council report

Copies can be ordered at the Communication and Information Department (C&I): info@cwi.nl

Introduction

This year of our 60th anniversary was not only festive, it was successful: successful in realizing scientific breakthroughs and successful in acquiring external projects.

Breakthroughs included our work on phytoplankton research, published in Nature. New upper bounds were determined for the Kissing Number using semidefinite optimization. Personal Space Technologies, one of our spin-off companies, developed new immersible techniques for its desktop virtual reality systems.

Among the external projects acquired this year were an NWO Vici grant for Ronald Cramer, an EU CREDO grant for Frank de Boer and an EU EC-MOAN grant for Jaco van de Pol. In line with CWI's tradition, the grants will be spent for leading-edge research, inspired by practical problems. Peter Boncz won the national ICTRegie Award 2006 for his data-mining techniques, which were used by another CWI spin-off company, Data Distilleries.
In December, the final design was approved for our new 4000 m^2 wing and for the renovation of our existing 6500 m^2 offices. We expect that when the work is completed in 2009, the result will be a stimulating environment that – after a period of cramped quarters and construction inconveniences – will signal the start of a new period of creative light (and enlightenment!) for our researchers. We are confident that CWI's offices will be the pearl of the Amsterdam Science Park!

2006 was not only a year of physical developments, but of strategic ones as well. Our plan *A Fundamental Difference* outlines the Institute's research programme for the coming five years. The plan articulates our vision of CWI's future, the contours of our scientific agenda, and our methods for maintaining – and improving – our track record of research excellence. The strategic plan will be used to position CWI in our discussions with governmental, business and other funding partners. The one-time financial bonus that we received from NWO in connection with the Institute's evaluation of 2005 will be spent in accordance with the plan.

In addition to this all, 2006 was a festive year for CWI. The celebrations of our 60th birthday included a lively soiree where the first Van Wijngaarden Awards were presented, a particularly active staff outing, a well-attended reunion, and the requisite meals that accompany this milestone. All of these framed a successful review of our past accomplishments and our confidence in CWI's future. The book *Opgelost* (Solved!), with its collection of stories on the practical and inspirational applications of mathematics and computer science, was our present to the Dutch society that has supported CWI's work throughout our history. The goal of this book was not only to inspire our continued firm financial future, but also to draw young talent to the scientific areas that we study. In this way, we hope that when CWI celebrates its 100th anniversary, it remains a vibrant institute with resilient and respected researchers.

Jan Karel Lenstra
General Director

Overview

CWI Research Clusters

Probability, Networks and Algorithms (PNA)
1 - Algorithms, Combinatorics and Optimization
2 - Advanced Communication Networks
3 - Stochastics
4 - Signals and Images
5 - Cryptology and Information Security

Software Engineering (SEN)
1 - Interactive Software Development and Renovation
2 - Specification and Analysis of Embedded Systems
3 - Coordination Languages
4 - Evolutionary Systems and Applied Algorithmics
5 - Convergent Media Infrastructures

Modelling, Analysis and Simulation (MAS)
1 - Non-linear PDEs – Analysis and Scientific Computing
2 - Computing and Control
3 - Nonlinear Dynamics and Complex Systems

Information Systems (INS)
0 - Standardization and Knowledge Transfer
1 - Database Architectures and Information Access
2 - Multimedia and Human/Computer Interaction
3 - Visualization and 3D Interfaces
4 - Quantum Computing and Advanced Systems Research

CWI

Founded in 1946, the Centrum voor Wiskunde en Informatica (CWI) is the Netherlands' national research institute for mathematics and computer science.
CWI conducts pioneering research in mathematics and computer science, generating new knowledge in these fields and conveying it to broader society, and to trade and industry in particular. CWI obtains around 60% of its funding from the Netherlands Organisation for Scientific Research (NWO). The remaining 40% is obtained through national and international programmes and contract research commissioned by industry.

To achieve its mission, CWI has formulated the following goals:

1. To conduct advanced research of societal and scientific relevance
2. To act as a 'breeding ground' for academic staff
3. To train young researchers
4. To transfer knowledge to society
5. To play a leading role in the Dutch and European mathematics and computer science scene
6. To increase public interest in mathematics and computer science

I To conduct advanced research of societal and scientific relevance

The primary goal of CWI is to conduct relevant advanced and fundamental scientific research. Both science and society should benefit from our work. In this section, we report on the influence our work has had.

Search techniques for a new company

The setting of new standards in high-speed analysis of complex databases constitutes a major challenge. In 2006, when CWI researcher Peter Boncz won the ICTRegie Award for his search techniques, the jury commented that the challenges of complex database analysis are not merely scientific – the real art lies in using research results to compile a convincing business model. And that is precisely what Peter Boncz and his colleagues did. Thanks to their new search techniques, they were able to launch the successful spin-off company Data Distilleries, which later merged with SPSS.
Data Distilleries specialized in the development of data-mining software, an analysis technique used to discover hidden strategic information in very large databases. This kind of information is not easily disclosed by conventional analysis techniques, such as statistical tools. "Boncz showed that the actual application of scientific knowledge in the field of computer science can lead to impressive results," the jury reported.

Atomic structures as revealed by mathematics

Thanks to the computational techniques developed by Joost Batenburg, physicists can now obtain 3D images of individual atoms within nano-crystals. This research will help us understand material properties, such as superconductivity or the behaviour of semiconductors. His new discrete tomography technology focuses on 3D image reconstruction from a small number of X-ray photos. Batenburg's techniques can also be used to detect osteoporosis, but also impurities in diamonds. For his presentation of these techniques, Joost Batenburg, PhD student at CWI, won the first Philips Mathematics Prize for PhD students. He was also awarded the C.J. Kok jury prize by Leiden University. See page 46.

Joost Batenburg

Peter Boncz with the ICTRegie Award during the 'National ICT Awards 2006' event.
(picture: Gerrit Serne)

Strategy 2007-2012

Towards the end of 2006, CWI prepared its strategy for the 2007-2012 period, laid down in the memo *A Fundamental Difference*.
Active research institutes play an essential role in the realization of national and European aims and objectives, in that they are breeding grounds for professors and generators of knowledge. This is particularly true for CWI, which operates successfully at the interface between mathematics and computer science, and between pure and applied research.
In order to consolidate its status as a centre of excellence, CWI has clustered its research into four social themes: Earth and Life Sciences; the Data Explosion; Societal Logistics; and Software as service. CWI will pursue national and international collaboration, and will continue to invest in researchers and the free exchange of knowledge and ideas.
A Fundamental Difference also addresses a number of new social challenges. In this regard, CWI will foster research into the problem of creating effective work and school timetables, and into the technology facilitating à-la-carte arrangements of available internet services.
The memo is the product of an intensive and absorbing year-long process that addressed numerous questions. What makes CWI unique? What is its value for society? How will it develop? By answering these questions, an image of CWI was compiled – a profile in which we could recognize ourselves. This served as a foundation for developing a vision of the future, adopted and supported by our entire organization. The memo *A Fundamental Difference* was published in the spring of 2007.

New computer science research

Grants from the Netherlands Organisation for Scientific Research (NWO) have enabled CWI to initiate three new research projects.

Distributed Implementations of Adaptive Collective Decision Making focuses on collective decision-making mechanisms in economics. Such mechanisms are increasingly influenced by grid computing and electronic commerce. Krzysztof Apt is project coordinator.

The second project, *Cracking a Scientific Database*, deals with the development of better database management systems for very large – petabyte – databases and complex distributed searches. Examples include the gigantic databases of Sloan Digital Sky-Server and Astro-Wise. This project is coordinated by Martin Kersten.

These two grants form part of the FOCUS programme (part of BRICKS) developed by NWO Physical Sciences to stimulate fundamental computer science research.

The third grant was awarded to the project *Workflow Management for Large Parallel and Distributed Applications*, coordinated by Natalia Sidorova of the Eindhoven University of Technology. This project aims to bridge the gap between two key areas in which complex software systems are applied: workflow management and grid computing. This grant is part of GLANCE, one of NWO's computer science programmes.

Optimization of complex schedules

Research conducted at CWI has set the tone for an entire field: discrete optimization. Mathematical insight generated in this field has become indispensable for planning in certain sectors, such as the allocation of frequencies for mobile phones and the distribution of available carriages among trains.

Martin Grötschel (Berlin University of Technology), László Lovász (Eötvös Loránd University Budapest) and Alexander Schrijver conducted pioneering work in the field of discrete optimization. This was acknowledged by the Institute for Operations Research and the Management Science (INFORMS), which awarded them the John Von Neumann Theory Prize for their collective and individual efforts.

The prize specifically recognized their work on the ellipsoid method. The three researchers showed, in the early 1980s, that a geometrical approach is essential when dealing with a large group of discrete optimization problems. This geometrical approach subsequently became the conventional method for tackling problems of this kind. In fact, it lies at the heart of almost all software for discrete optimization.

The link between industry and mathematics

Scientific computing for industrial applications is of great economic importance to our country. In recent decades, Piet Hemker has made significant contributions to this field. He has conducted key studies on the numerical-mathematical multi-grid method. This technique has proved crucial in many large-scale industrial computational problems. For instance, in the fields of aerodynamics and hydrodynamics.

Piet Hemker retired in 2006, on which occasion he was awarded with a Royal decoration "Ridder in de Orde van de Nederlandse Leeuw". The international scientific journal Applied Numerical Mathematics will mark his retirement with a special issue, featuring articles written by his colleagues. Throughout his career, Piet Hemker worked to forge links between mathematics and industry. He was also instrumental in bringing together scientists from both sides of the Iron Curtain. After the curtain was raised, he strove to further foster that spirit of cooperation.

Piet Hemker

Searching for Vermeer

A new computer application will make it possible to search the web for, say, Jan Vermeer's paintings or wooden masks from a specific region, while making sense of how the results are related. This application is the result of the E-Culture project, in which CWI is participating.

Online access to even the most important aspects of our past is still limited and highly fragmented. The new search applications demonstrate the integration of resources that were developed using different vocabularies and different perspectives on the data. They also show how information about the nature of data can be accessed and how context-specific presentations may be generated. This project applies insight from computer science for

Kissing in higher dimensions

Scientists have identified new limits for kissing in higher dimensions. 'Kissing' is the term for touching. On a table, seven similar coins can be arranged in such a way that six of them touch one central coin – and no others. The kissing number is six. But kissing is only this simple in two dimensions. Add another dimension and the kissing problem becomes very difficult to solve.

As far back as 1694, Isaac Newton and David Gregory debated how many balls one central ball would be able to touch. Gregory argued that thirteen balls could be touched, while Newton believed the maximum number was twelve. It was not until 1953 that Schütte and Van der Waerden were able to prove Newton right.

In the 1970s, Delsarte developed a method of determining upper bounds for the kissing number based on linear programming. For example, in four dimensions, the Delsarte bound is 25. In 2003, Musin proved that the actual value is 24. Until recently, the exact kissing number was only known for the dimensions 1, 2, 3, 4, 8 and 24.

Christine Bachoc (University of Bordeaux) and Frank Vallentin have calculated upper bounds for other dimensions. They developed a new method to determine these upper bounds, based on representation theory and semi-definite optimization. They found new or better values for all dimensions up to dimension 10. They refined the upper bound for dimension 5 from 45 to 44. And in dimension 10, they discovered that 27 fewer balls were able to kiss.

Kissing is not just fun for mathematicians. Research on kissing numbers has applications in geometry, error correcting codes in telecommunications, and string theory.

3D Kissing. Picture: F. Vallentin

BRICKS in progress

BRICKS is at midterm. This research consortium, financed with Dutch Bsik funds, has completed three years of intensive work. Hosted by CWI, the BRICKS organization comprises 22 projects. The main aim of the programme is to strengthen the Dutch knowledge society with higher standards and a lasting infrastructure for computer science and mathematics. Project topics include future networks consisting of a heterogeneous mix of broadband, wireless and personal area networks, but also novel paradigms for advanced computing algorithms based on quantum theory, as well as new algorithms for bio-informatics and breakthroughs in biotechnology. Other projects are working on formal verification and theorem proving, and developing new approaches to scientific computing, visualization, gaming and other virtual environments. BRICKS is also a breeding ground for a new generation of database technology for ambient intelligence and data mining on a peta-byte scale, and for intelligent decision-support systems for societal logistics.

In 2006, BRICKS scientist Michael Weber won the Best Paper Award of the European Association of Software Science and Technology (EASST). Written in collaboration with Moritz Hammer (Ludwig-Maximilians University, Munich), *To Store or Not To Store' Reloaded: Reclaiming Memory on Demand* describes techniques for handling extremely large state spaces in model checking of computer systems. In addition, BRICKS scientist Pascal Lieshout won the Sigmetrics/Performance Outstanding Student Paper Award.

BRICKS

the purposes of semantic web technology, multimedia indexing and searching, and web interfacing and data visualization, with a view to facilitating the display of our cultural heritage.

This project won the 2006 International Semantic Web Challenge, which acknowledges projects that extract information from distributed sources in an open environment where user queries cannot be predicted.
The winning application was built by an Amsterdam-based team of researchers from CWI and Amsterdam's two universities, working in close cooperation with the Dutch cultural heritage organizations DEN and ICN. The prize was presented to two members of the E-Culture team, Guus Schreiber (VU University, Amsterdam) and Jacco van Ossenbruggen.

Guus Schreiber (right) demonstrating the winning application to the inventor of the Web, Sir Tim Berners-Lee. Picture: Jacco van Ossenbruggen

A new link with the social sciences

The study of games, action and social software involves knowledge from very different disciplines. For almost six months, leading scientists from the fields of philosophy, logic, computer science, psychology and economics lived and worked together in a villa in Wassenaar, near the Dutch coast, participating a project headed by CWI scientist Jan van Eijck and Rineke Verbrugge of the University of Groningen. The aim of this intensive cooperation was to find a more unified view of social mechanisms.

A book on this subject is currently being written, and the team have also held workshops on various social mechanisms, to obtain feedback from people involved in the redesign of social protocols. Workshop topics included electoral reforms for an enlarged Europe, peace negotiations in the Middle East, auction design, and public tenders for contracts.

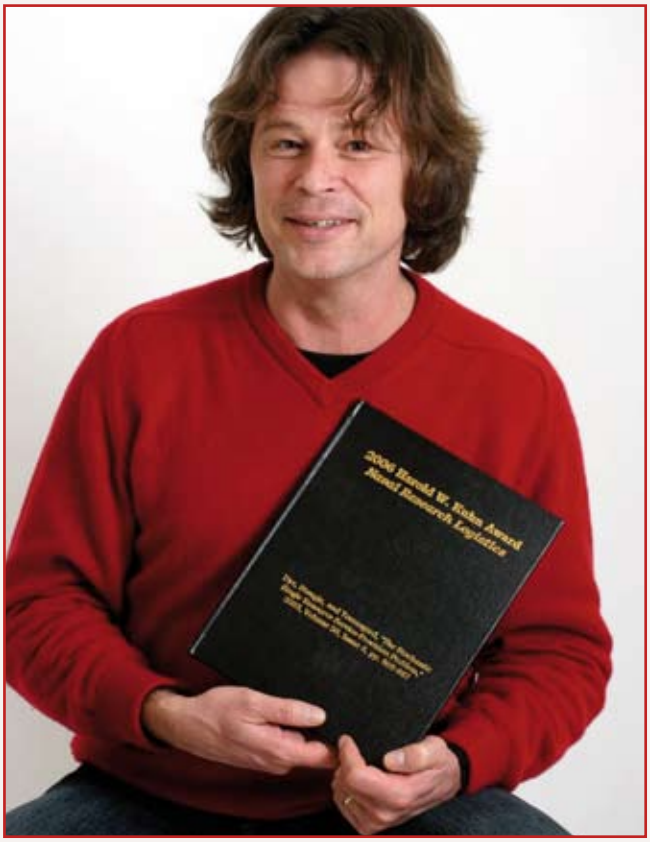
This think tank was made possible by grants from the Netherlands Institute for Advanced Study in the Humanities and Social Sciences (NIAS) and from the NWO Cognition Programme.

Destabilization of oceans

Global warming could destabilize the ocean's plankton. Temperature changes in the surface layers of oceans reduce the upward transport of nutrients. Computer simulations have shown that this causes chaos among plankton.
These findings were published in *Nature* by Nga Pham Thi and Ben Sommeijer, together with colleagues from the University of Amsterdam and the University of Hawaii. Their study demonstrated that a reduced supply of nutrients will cause plankton growth to fluctuate. This will endanger fish populations, as plankton forms the basis of the marine food chain. Moreover, this will reduce the uptake of carbon dioxide in the oceans, resulting in a higher concentration of this greenhouse gas in the atmosphere. These predictions were rather unexpected, because they contradict the conventional wisdom that deep plankton in oceans constitute a highly stable system.

Integer optimization

In telecommunications networks, stochastic integer optimization problems commonly arise in the area of distributed processing. Leen Stougie has designed efficient approximation algorithms with constant worst-case performance guarantees. This work was carried out together with Shane Dye (New Zealand) and Asgeir Tomasgard (Norway). This major step forward in stochastic optimization has attracted significant interest and generated follow-up work. Moreover, the three scientists jointly received the Harold W. Kuhn Award, which is presented for the best paper published in the journal in the previous three years.



Leen Stougie

2 To act as a 'breeding ground' for academic staff

Over the years, CWI has honed the skills and expertise of many talented young people. We can proudly claim that no less than 170 of them work as professors in many parts of the world. CWI has a distinguished reputation in that it enables scientists to really focus on their research. This makes it an excellent scientific breeding ground, attracting some of the world's leading scientists.

More scientists for privacy research

A recent grant served as a new impulse for research into the mathematical foundations of privacy. NWO awarded mathematician Ronald Cramer a Vici grant of EUR 1.25 million to expand his top-class research team to study secure computation techniques.
His team explored situations where standard cryptography methods, such as encryption or digital signatures, are insufficient. Secure computation techniques offer a solution in such instances. Ronald Cramer developed efficient techniques for secure computation, based on novel interconnections with algebraic number theory and algebraic geometry, which can be widely applied. For instance in secure electronic voting, anonymous electronic payments, electronic auctions, and privacy-protecting data processing. This technology can be used for the protection of passenger lists that airlines are required to submit to the authorities. Using cryptography, these lists may be compared with information stored in a secret service database, without revealing the identity of innocent passengers.

Ronald Cramer

Krzysztof Apt

Member of the Academia Europaea

Krzysztof Apt was invited to join the Informatics Section of the Academia Europaea. The Academia Europaea is a non-governmental association acting as an Academy. Its members are scientists and scholars who promote learning, education and research. Members of the Academy are selected on the basis of a comprehensive peer review procedure.

Ute Ebert

Member of the oldest academic society

Ute Ebert has been invited to become a member of the Koninklijke Hollandsche Maatschappij der Wetenschappen (Royal Holland Society of Sciences and Humanities) in Haarlem. Established in 1752, the oldest academic society in the Netherlands aspires to bridge the gap between science and society. Ute Ebert is well known for her theoretical research on the formation of lightning and sparks. She heads the Nonlinear Dynamics and Complex Systems research group and is professor at the Eindhoven University of Technology.

Mark van den Brand was appointed professor at the Eindhoven University of Technology.

Thesis nominated for award

Dion Gijswijt's thesis Matrix Algebras and Semidefinite Programming Techniques for Codes (2005) was devoted to error-corrections for CD players and other electronic data transfer. He studied the theoretically possible qualitative limits of error-correcting codes. His thesis was one of three nominated by the Mathematical Programming Society for the prestigious Tucker Prize, which is awarded once every three years. Dion Gijswijt is currently working as a post-doctoral researcher at the University of Amsterdam.

Dion Gijswijt (left) and Tom McCormick (UBC, Chair of the 2006 Tucker Prize Committee), congratulating Dion with his nomination for the Tucker Award. (picture: MPS)

Extra brains for quantum computing

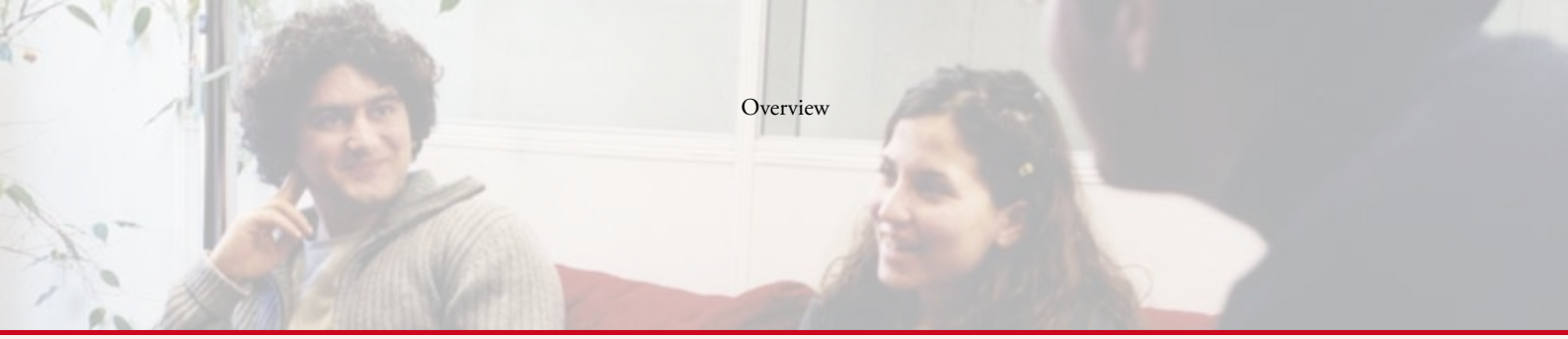
CWI has appointed computer scientist Nitin Saxena to conduct studies in the field of quantum computing. In 2002, Saxena, Manindra Agrawal and Neeraj Kayal of the Indian Institute of Technology (IIT) in Kanpur gained instant renown with their solution to one of the longest standing computational problems. They developed a polynomial-time algorithm to determine whether a given number is prime or not. The difficulty of finding the prime factors of very large numbers is one of the cornerstones of cryptography and data security. Their discovery was relayed around the globe within minutes, getting an immediate and enthusiastic response. Saxena's research is considered a masterpiece of mathematical reasoning. His work has inspired numerous researchers to work on the algebraic techniques involved.
Thanks to this work, Nitin Saxena became the youngest ever recipient of the prestigious Gödel Prize. He also won the 2006 Fulkerson Prize from the Mathematical Programming Society and the American Mathematical Society. His appointment at CWI was made possible by both Vici and BRICKS grants from NWO.

Nitin Saxena

New breeding ground

CWI is adding a new wing to its existing building and has also commissioned further alterations. This expansion is essential to accommodate the steady growth of our institute, which will have room for 350 employees in 2009.
The design is in the hands of Van Mourik Vermeulen Architects. Their mission is to inspire, motivate and surprise people, and to allow discovery. They also designed the Anton Philips Hall and the Royal Academy of Art in The Hague.
NWO is financing the building plans.

Artists impression of the new wing.



3 To train young researchers

CWI provides a stimulating environment for young researchers. They produced a number of exciting theses in 2006, and some of our students were awarded prestigious prizes and grants.

PhD theses

Probability, Networks & Algorithms Research Cluster

Fluid queues

Queueing theory addresses the problem of customers waiting for service. One important application revolves around the transmission of traffic at internet nodes, where data packets arrive and depart. Because these data packets are relatively small, their movement can be approximated by fluid streams. Consequently, internet nodes can be modelled as queues, fed by these fluid streams. One of the key issues here is the dramatic fluctuation in the rate at which these streams flow.

PhD student Ton Dieker studied several key problems relating to fluid queues. Insight into the performance of these queueing systems is crucial in designing systems that can guarantee a specified quality level to users of the network.

On 9 March, Ton Dieker received his PhD from the University of Amsterdam for his thesis *Extremes and Fluid Queues*. His supervisor was Prof. M.R.H. Mandjes (CWI, and University of Amsterdam).

Better train planning

PhD student Gabor Maróti designed mathematical models for train planning. He studied several optimization models for tactical and operational planning and maintenance routing. He looked at efficiency, immunity to failure, and the chance of clients obtaining a seat. His models allow planners to make a balanced choice between these often conflicting service requirements. Maróti found that the Dutch railway company NS could cut costs by a few million euros if it applied computational models developed at CWI in recent years.
CWI has a tradition in train scheduling. Spinoza Prize winner Alexander Schrijver developed software for several optimizing problems confronting NS. In late 2006, his research was used in a major overhaul of the Dutch railway timetable.
Gabor Maróti's project was funded by the European Union training network Algorithmic Methods for Optimizing the Railways in Europe (AMORE), as well as by NS Reizigers, the Bsik programme BRICKS and the Eindhoven University of Technology.
Maróti defended his thesis *Operations Research Models for Railway Rolling Stock Planning* in Eindhoven on 12 April. His supervisors were Prof. A.M.H. Gerards (CWI, Eindhoven University of Technology) and Prof. L.G. Kroon (NS Reizigers, Erasmus University).

Ton Dieker

Gabor Maróti

Software Engineering Research Cluster

Finitary coalgebraic logics

Modal logic and coalgebra are closely intertwined, reflecting the well-studied relationship between equational logic and algebra. PhD student Clemens Kupke has studied various types of modal languages in which coalgebras can be discussed. He argues that a logical language with which coalgebras can be meaningfully discussed must have a finite syntax. However, languages of this kind lack the so-called Hennessy-Milner property. Kupke therefore went in search of a class of coalgebras with logics that have finite syntaxes that also have the Hennessy-Milner property.

Clemens Kupke obtained his PhD for his thesis *Finitary Coalgebraic Logics* from the University of Amsterdam on 23 March. His supervisor was Prof. J.J.M.M. Rutten (CWI, and VU University Amsterdam), with associate supervisors Dr. A. Kurz (University of Leicester) and Dr. Y. Venema (University of Amsterdam).

Clemens Kupke

Modelling, Analysis & Simulation Research Cluster

Models for lightning

High-altitude lightning is a spectacular phenomenon. In a broad bundle, tens of thousands of individual discharges make their way parallel to one another. Other transient luminous events shoot straight up out of the clouds, as expanding rings, jets and a host of other formations.

PhD student Bernard Meulenbroek studied streamer propagation and branching that occurs in such phenomena. To this end, he derived a moving boundary approximation for the interface between ionized and nonionized regions and studied the boundary dynamics analytically and numerically.

Better internet connections: correctness beyond reasonable doubt

The reliability of many internet connections depends on TCP, one of the key protocols for internet applications. But can this protocol be improved? PhD student Bahareh Badban developed methods to mechanically verify several improvements.

The Transmission Control Protocol (TCP) is used in almost all internet applications, such as HTTP/HTTPS for the World Wide Web, SMTP/IMAP/POP3 for email, and FTP for file transfer. TCP implementations have been optimized for use in wired and wireless networks. Owing to the widespread use of TCP, it has been extensively researched. By tuning TCPs, more efficient use can be made of available bandwidth networks. Studies include enhancing TCP to reliably handle loss of data, minimize errors, and manage congestion, especially in very high-speed environments. Bahareh Badban conducted her research with the aid of theorem provers; computer programs that are able to prove mathematical rules or theorems by automatic reasoning. This is an important subfield in formal methods. Bahareh Badban extended existing theorem provers in order to be able to verify large distributed systems. She extended existing theorem provers to larger theories using different approaches. She then applied them to analyse the reliability of the existing TCP protocols. She verified a two-sided sliding window protocol (SWP). The SWP provides handling timeouts and also transmissions and retransmissions of data in TCP. Since TCP manages retransmission of data if it is not received within a reasonable round-trip time, a reliable and efficient SWP can produce a TCP with

a better use of the network bandwidth.
Bahareh Badban studied a version of the protocol that has the acknowledgements piggy-backed on data, ensuring them of a free ride in the channel. This allows the available bandwidth to be used more efficiently. Owing to this close coupling, however, verification was more complicated. She defended her thesis *Verification Techniques for Extensions of Equality* at the VU University Amsterdam on 7 September. Her supervisor was Prof. W.J. Fokkink (VU University Amsterdam, CWI), with associate supervisor Dr. J.C. van de Pol.

Bahareh Badban

Bernard Meulenbroek obtained his PhD for his thesis *Streamer Branching: Conformal Mapping and Regularisation* from the Eindhoven University of Technology on 13 April. His supervisor was Prof. U. Ebert (CWI, and Eindhoven University of Technology).

Bernard Meulenbroek

Hybrid control systems

Mathematical control theory relates to the control of natural and engineering systems, such as aeroplanes, conveyor belts, and systems for the automated injection of medicines. These systems commonly have components that exhibit continuous behaviour as well as those that exhibit discrete behaviour.

PhD student Mihály Petreczky studied these hybrid systems, combining differential equations and rule sets. The control of hybrid systems is important for engineering, where technology is often computer-controlled. In short, the study of hybrid systems is situated at the crossroads of control theory and computer science.

Mihály Petreczky obtained his PhD for his thesis *Realisation Theory of Hybrid Systems* from the VU University Amsterdam on 22 June. His supervisor was Prof. J.H. van Schuppen (CWI, VU University Amsterdam).

Mihály Petreczky

Information Systems Research Cluster

Noise for compression

Mathematical theory investigates how well one can compress music, photos and other digital information. The so-called Kolmogorov complexity of a word is the length of the shortest description of that word. It therefore describes the ultimate limit of compression. In practice, however, there are limitations that prevent this boundary being reached, owing to the restricted computational capacity of processors, for instance.

Troy Lee studied resource-limited variants of Kolmogorov complexity to map out a more realistic view. One of the most interesting results of his research is that pseudo-random generators can also be used for data compression.

Troy Lee obtained his PhD for his thesis *Kolmogorov Complexity and Formula Size Lower Bounds* from the University of Amsterdam on 11 January. His supervisor was Prof. H.M. Buhrman (CWI, and University of Amsterdam). Lee received a Rubicon grant from NWO.

Troy Lee

The power of quantum computing

Quantum computers make use of physical effects that take place at atomic level, allowing calculations to be conducted in a fundamentally different way. But only in theory, because only very small quantum computers have been built to date.

Robert Špalek explored the power of quantum computers. He presented a number of new quantum algorithms and developed new techniques for ascertaining the limitations of quantum computers. Špalek proved the first time-space trade-offs for quantum computers, offering insight into the relationship between computation time and computer memory required to solve a problem.

Robert Špalek obtained his PhD for his thesis *Quantum Algorithms, Lower Bounds, and Time-Space Tradeoffs* from the University of Amsterdam on 7 September. His supervisor was Prof. H.M. Buhrman (CWI, and University of Amsterdam), with associate supervisor Dr. R.M. de Wolf.

Robert Špalek

Make your own movie

Documentaries always feature a subjective selection from dozens of hours of footage. Stefano Bocconi designed the software system 'Vox Populi', which gives viewers access to all footage, enabling them to compile their own documentary, adopting a completely different angle, if they so desire.

Researcher and documentary maker Stefano Bocconi remarks that subjective choices define the nature of a documentary. And that tends to complicate matters. His own editorial team often found it difficult to select images and adopt a specific angle.

Online video repositories may contain several hours of documentary footage, but most users are only interested in a subset of that material. The aim of Bocconi's research was to provide an alternative authoring process for documentary makers, making all their material dynamically available to users, without having to edit a static final cut, which might result in informative footage being discarded. The Vox Populi system tests this approach, allowing users to specify topics as well as characters for rhetorical dialogue and rhetorical presentation formats.

Vox Populi ensures that viewers are not subject to the director's cut. Once the viewer has made his or her subjective selection, the software automatically edits the video fragments to form a

logical entity. With this production method, Stefano Bocconi has bridged the creative process of the documentary maker and the formal approach of the required software system.

Stefano Bocconi obtained his PhD for his thesis *Vox Populi: Generating Video Documentaries from Semantically Annotated Media Repositories* from the Eindhoven University of Technology on 30 November. His supervisor was Prof. L. Hardman (CWI, and Eindhoven University of Technology), with associate supervisor Dr. F. Nack.

Stefano Bocconi

Parsing context-free grammars

A parser is a tool that determines whether an input string is grammatically correct or not. An algorithm capable of parsing any context-free grammar is called a generalized parser.

Giorgios Economopoulos devoted his thesis to the theoretical analysis of generalized parsing algorithms. He described, analysed and compared several algorithms based on Knuth's LR parser. This work underpins the design and implementation of the Parser Animation Tool (PAT). Economopoulos used PAT to evaluate the asymptotic complexity of generalized parsing algorithms and to develop a new, cubic, worst-case parser.

Giorgios Economopoulos

Comparing several algorithms indicated that overheads of some parsing algorithms could have significant consequences on their behaviour.

Giorgios Economopoulos obtained his PhD for his thesis *Generalised LR Parsing Algorithms* from Royal Holloway, University of London in Egham, on 30 September. His supervisors were Dr. E. Scott and Dr. A. Johnstone (University of London).

More bright young minds

• Joost Batenburg obtained his PhD for his thesis *Network Flow Algorithms for Discrete Tomography* from the University of Leiden on 19 September. His supervisor was Prof. R. Tijdeman (University of Leiden), with associate supervisor Dr. H.J.J. te Riele. See pages 8 (picture) and 46.

• Nga Pham Thi defended her thesis *Numerical Analysis of Phytoplankton Dynamics* at the University of Amsterdam on 21 November. Her supervisors were Prof. J.G. Verwer (CWI, University of Amsterdam) and Prof. J. Huisman (University of Amsterdam); with associate supervisor Dr. B.P. Sommeijer.

Nga Pham Thi

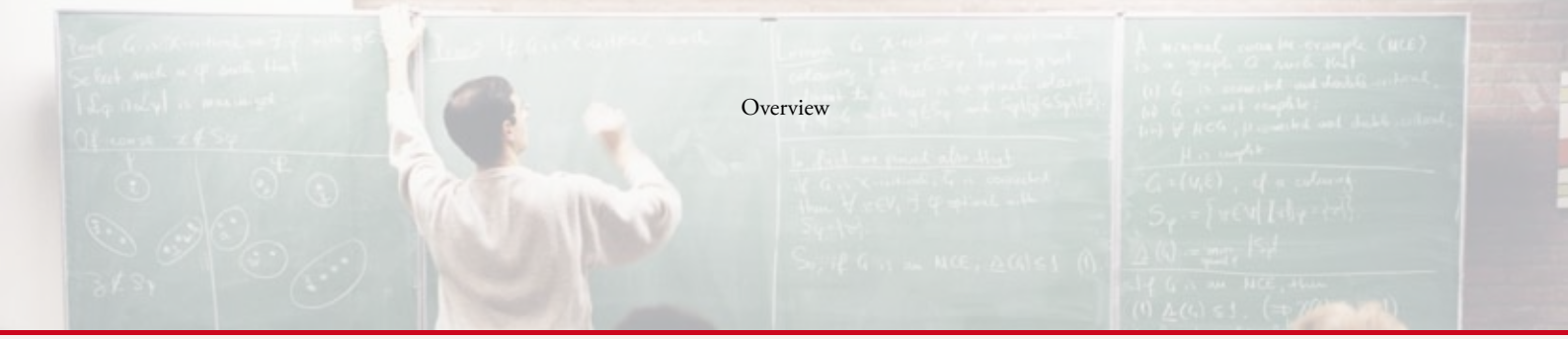
• Antonio Zagaris was awarded an NWO Veni grant for large-scale computer simulations. By developing new ways of identifying parts of complex systems, he aims to improve the efficiency and scope of microscopic and macroscopic studies.

Antonio Zagaris

• From a field of 175 theses, Jorick Naber's was selected as the best master's thesis of the year. He graduated from the Delft University of Technology and did his master's research at CWI, researching a method for unsteady compressible two-fluid flow.

Jorick Naber (picture: Aad Kluyt)

• Jeroen Wackers, CWI PhD student in the BRICKS Scientific Computing Project, completed two months of research in Japan at the invitation of the prestigious National Maritime Research Institute of Japan. Also see page 38.



4 To transfer knowledge to society

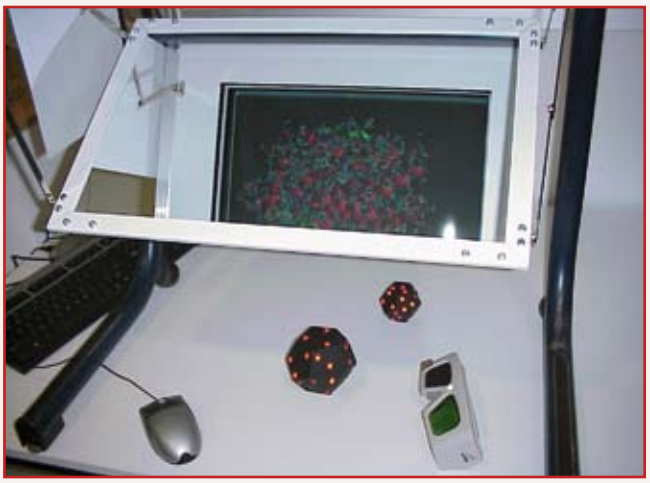
CWI pursues a policy of active knowledge transfer. For instance, by way of publishing licenses and establishing spin-off companies.

Virtual reality in the office

Personal Space Technologies is a CWI spin-off that specializes in visualization and 3D interaction. CWI staff and technology have been transferred to this young company, which is funded by CWI Incubator and other financiers.

The Personal Space Station (PSS)™ offers users interactive virtual-reality on their desktops. This technology gives users access to a virtual world within a normal office environment, allowing them to explore molecules, MRI-scans, equipment prototypes, and even entire star systems. These interactive simulations exploit eye-hand coordination, making them highly user-friendly. The user moves a marked pen, cube or thimble, while a specially developed optical tracking system enables wireless tracking of the interaction. The images calculated adapt to the hand movements in real time on the screen.

Personal Space Technologies has sold its products to universities and has joined hands with commercial partners. The technology is currently being used by biomedical technologists, cell biologists and virtual-reality labs.



Personal Space Station (PSS)™.

Intelligent cameras study buying behaviour

CWI and Innovista Security BV are collaborating on software modules for monitoring cameras. The intention is to automatically analyse the browsing and buying behaviour of customers in shops. Via this collaboration, CWI is making its knowledge of video intelligence available to the market and to society.

Together with Innovista, CWI is developing software to recognize people, objects and activities. The software can count the number of visitors to a shopping street or gauge how customers buy in supermarkets. It can also ascertain how long they look at a particular product and which routes they take through the shop.

Innovista has already developed an online surveillance platform. This is a suitable platform for CWI to test algorithms and codes for video intelligence. Innovista will then apply these in commercial products.

CWI also recently developed an advanced motion detection system, which was immediately put to good use in Eindhoven and Nuenen. CWI also plans to use this platform to test SenseNets. These are networks in which data streams from cameras and sensors can be combined and interpreted.

Solar sails and tsunamis for math teachers

Last years' summer school for math teachers dealt with topical mathematical issues, such as solar sails with photons and the origin of tsunamis. The aim was to give teachers material that would make pupils enthusiastic about mathematics. Held in collaboration with the Netherlands' society of mathematics teachers (NVvW), the very first summer school was organized back in 1946 by the Mathematical Centre, the predecessor of CWI.

Various other intriguing questions were also addressed at this year's gathering: How can mathematical techniques be used for the security of small devices like mobile phones? What techniques are applied in Geographical Information Systems? Why is the ABC Conjecture known as the 'last Holy Grail of mathematics'? What is the role of mathematics in the financial world, when it comes to the trading of options and other derivatives? How can mathematics help us access oil that until now has been difficult to extract?

Summer school for math teachers.

ICT Knowledge Congress

CWI was well represented at the ICT Knowledge Congress (ICT-Kenniscongres) in Amsterdam on 10 and 11 April. The congress aimed to promote knowledge exchange between scientific institutes and industry, addressing the needs of users and the social usefulness of ICT.
CWI was present at the knowledge fair, where it shared the NWO stand. BRICKS and the CWI spin-off Personal Space Technologies were also present. The congress also included a special youth programme, DizzizIT, aimed at 12 to 15 year olds, where CWI presented two demos. Elsewhere, CWI experts gave lectures on museum tours, error-free software, decentralized patient planning, and quantum computers.

CWI supports companies

At our annual industrial network day on 16 November, we demonstrated how our research is linked to industry. We presented four themes that will occupy a key position for CWI in the coming years, namely Earth and Life Sciences, the Data Explosion, Societal Logistics, and Software as service.

Prominent speakers and exciting demonstrations flavoured the day. Alexander Rinnooy Kan, chairman of the Dutch Social and Economic Council (SER) got the ball rolling with his vision on the role of science in the economy.
Leo Kroon of the Erasmus University and NS Reizigers explained how CWI scientific research had been used to improve Dutch railway timetables – a highly complex challenge, considering that the Dutch railway network is one of the busiest in the world. Consequently, thousands of interrelated constraints have to be taken into account, including desired frequencies, travel and transit times, the availability of rolling stock, and distances between trains. Furthermore, robustness and personnel schedules have to be optimized.

Back in the 1990s, CWI developed CADANS for Dutch Railways. This combinatorial algebraic timetable algorithm has been extended and improved over the years. CADANS enables Dutch Railways (NS) to qualitatively compare various factors and subsequently choose the desired balance. In 2007, CWI research helped produce a more robust timetable for Dutch Railways.

Frank Kelly of Cambridge University highlighted the challenges presented by road pricing. Kelly served as Chief Scientific Adviser to the UK Department for Transport. He explained the difficulties of traffic modelling in a system where not all roads are tolled. Both network topology and traffic patterns are important in such models. He also showed how to protect privacy in electronic toll systems. Presentations were also given by Hans Westerhoff (University of Manchester and both Amsterdam universities) and Mike Papazoglou (University of Tilburg).

CWI's annual industrial networkday.

Research gives Dutch aircraft stability

The Fokker F27 Friendship aircraft was voted Best Dutch Design of the 20th Century in a contest jointly organized by the Dutch newspaper NRC Handelsblad and the Premsela Foundation. The design was praised for its simple construction, robustness and efficiency.

The Mathematical Centre, forerunner of CWI, made an important contribution to the mechanical stability of the Fokker Friendship, calculating vibration levels that are a key factor in ascertaining required structural strength. A light buzz may be harmless, but heavier vibrations can seriously damage or even destroy an aircraft. These so-called flutter computations for the wings were performed on one of the first computers in the Netherlands. These computations can be used to alter the design of the wing to minimize flutter.

Greater knowledge exchange

• The third BRICKS Scientific Computing Meeting was held at Shell Research Centre in Amsterdam on 16 February, featuring lectures on the progress of BRICKS research.

Visitors at the Microsoft day.

• Dutch scientists engaged in direct dialogue with Microsoft for the first time at a one-day symposium on Agent Technology on 8 March, under the banner The Future of Software Development and Intellectual Property Rights.
• A delegation of 20 senior Chinese civil servants attended a CWI training programme on railway automation on 18 October, offering insight into the challenge of testing millions of combinations of signals and switches. They were also presented with calculations relating to carriages in the train schedule.

5 To play a leading role in the Dutch and European mathematics and computer science scene

CWI is an active participant in conferences, research consortia and international scientific forums.

Semantic Web

Ivan Herman was appointed 'Semantic Web Activity Lead' by the international World Wide Web Consortium (W3C), in which researchers, companies and authorities cooperate to develop standards for web formats that are directly understood by computers.

The Semantic Web is one of W3C's most important activities. It creates a universal medium for data exchange, enabling computer programs to automatically exchange facts via websites, even when these programs have been developed independently.

The World Wide Web Consortium combines the expertise of around 400 affiliated organizations in more than 40 countries. CWI runs the W3C Benelux Office and is contributing to development in various W3C Working Groups.

Ivan Herman

European research in mathematics and computer science

CWI is actively involved in the European Research Consortium for Informatics and Mathematics (ERCIM), which encompasses some 12,000 European researchers in mathematics and computer science. CWI's General Director Jan Karel Lenstra is vice president of ERCIM.

In 2006, CWI and others organized the Stelios Orphanoudakis ERCIM Memorial Seminar, in honour of ERCIM's former president, who passed away in March 2005.

ERCIM and W3C team in Nice, October 2006 . (picture: ERCIM)

ERCOM

Jan Karel Lenstra has been appointed chairman of ERCOM, a committee of the European Mathematical Society (EMS) consisting of directors of research centres for mathematics. Herman te Riele is the scientific secretary of ERCOM.

Dagstuhl and Oberwolfach

Paul Klint is member of the Scientific Directorate of the International Conference and Research Center for Computer Science (IBFI) in Schloss Dagstuhl, Germany. Following the tradition of the world-famous Mathematics Research Institute of Oberwolfach, IBFI regularly organizes specialized seminars for top researchers and promising young scientists. Jan Karel Lenstra is a member of the IBFI Scientific Advisory Board, and Alexander Schrijver has a seat on the scientific committee of the Mathematics Research Institute of Oberwolfach.

Process algebra and cryptography

On 9 March, our Process Algebra and Cryptography groups jointly held a seminar titled *Formal Methods and Cryptography*, the first in a series of joint PAM-RISC seminars. The significance of formal methods in both fields was discussed. Logical concepts,

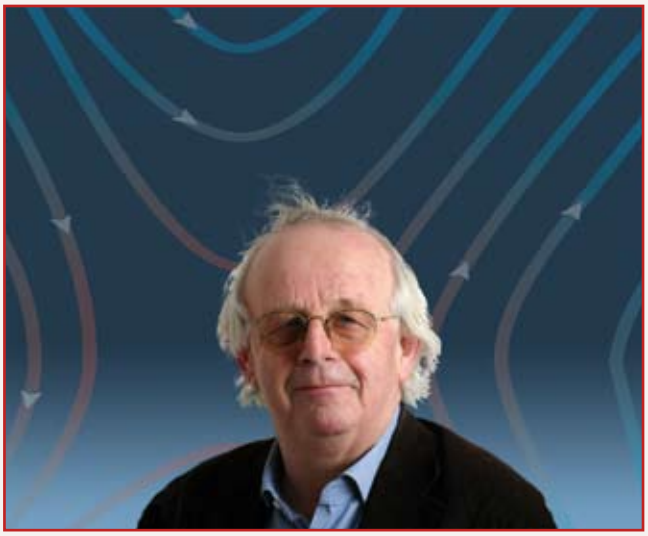
60th Anniversary for CWI

CWI celebrated its 60th anniversary last year. Founded in 1946 as the Mathematisch Centrum (Mathematical Centre), the initial purpose of the institute was to catch up on developments in applied mathematics abroad and to support post-war reconstruction of the Netherlands. It also had a mission to explore new frontiers in research, while ensuring that the results were put to good use. Over the years, CWI has made major contributions to mathematics and information technology. It gave rise to the programming language Python, crypto-systems, the database system MonetDB, and much, much more.
Jan Karel Lenstra, general director of CWI, has championed the cause of innovation in the Netherlands and pleaded for a greater emphasis on fundamental research. "True innovation comes from curiosity, serendipity and good conditions." He has also called for a greater degree of coordination in science policy.
CWI marked its 60th anniversary with the inception of the Van Wijngaarden Award, which is named after Aad van Wijngaarden (1916-1987), one of the founding fathers of computer science in the Netherlands and a former director of the Mathematical Centre. The award was presented to computer scientist Nancy Lynch (MIT), who is renowned for her pioneering work in distributed computing (particularly the impossibility of consensus), and to mathematician-magician Persi Diaconis (Stanford), who has been praised for combining deep mathematical insight with down-to-earth pragmatism. In his acceptance speech, he captivated the audience with facts on the physics of tossing coins. Both scientists received the bronze sculpture that will from now on be awarded once every five years.
The festivities were further enlivened by the Mondriaan Quartet, which played the unique String Quartet No. 1 in C Major, a piece composed by a computer program, which was written in ALGOL 60 by Lambert Meertens on the Mathematical Centre's Electrologica X8 computer as early as 1968.
The festivities took place in the Old Lutheran Church in Amsterdam on 9 February. But the celebrations did not end there. The current CWI community took a day trip to the beach on 12 September, and a reunion was organized on 12 December.

process algebra and algebraic geometry all play a role in cryptography. Speakers included Michael Backes (Saarland), Martin Abadi (Santa Cruz), and Simon Kramer (Lausanne).

Statistical inference

A symposium was held for Roelof Helmers to mark the combined occasions of his 40th anniversary at CWI and his 65th birthday. The symposium was dedicated to statistical inference, a subject Helmers studied intensively during his career. Prominent speakers demonstrated how their work had been inspired by Roelof Helmers. Speakers included Marie Hušková (Charles University, Prague), Edward van der Meulen (Catholic University of Leuven) and Ricardas Zitikis (University of Western Ontario, London, Ontario). The symposium *Statistical Inference: Searching for Facts* was held on 31 March.



Roelof Helmers

cwi.nl domain – first of the first

The Netherlands was the first country in the world to register a top-level national domain. This domain – .nl – celebrated its 20th anniversary on 25 April. CWI was in charge of registering the top-level domain, as part of its national and international networking activities. Shortly thereafter, cwi.nl became the first domain registered under .nl. The domain was registered by Piet Beertema, who played a central role in EUnet, the predecessor of the European internet. He managed the .nl top-level domain for ten years, but the explosive increase in new domains made the task too big for one person to handle. Responsibility was therefore transferred to the Internet Domain Registration Foundation Netherlands (SIDN) in 1997. Beertema received a Royal Decoration in 1999, in recognition of his pioneering work in the development of the Internet in the Netherlands and Europe.

Mathematics of swimming bacteria

How do bacteria find their way to a source of sugar? That was the topic of Jens Timmer's lecture *Design Principals of a Bacterial Signalling Network*. Based at the University of Freiburg, Timmer is a pioneer in the field of systems biology. He spoke at CWI on 8 May during the first of a series of Systems Biology Seminars organized by the Bio Centrum Amsterdam, which is a research school of the two Amsterdam universities. AMOLF and CWI are affiliated to the Bio Centrum Amsterdam.

Computational Management Science

The International Conference on Computational Management Science, held from 17–19 May, brought together people from academia and industry to discuss the theory and practice of computational methods, models and empirical analysis for decision-making in economics, finance, management, and related aspects of engineering. It focused on theoretical and empirical studies of computational models, computational statistics and data analysis, and many other topics in management science, the emphasis being on computational paradigms.

This annual conference was jointly organized by CWI and the Eindhoven University of Technology, in association with the journal *Computational Management Science*, published by Springer.

Software process improvement

The 7th International Conference on Product Focused Software Process Improvement (PROFES) was held at CWI from 12–14 June. Industrial practitioners and researchers discussed new research in the area of software product and process improvement. The conference addressed such topics as quality engineering and process management, with a focus on understanding the relationship between changes in processes and their impact on product quality in specific development environments. There is a fast-growing need for professional software development and business models in the fields of ambient intelligence, mobile applications and services, and embedded systems security and safety.

Combinatorics and Optimization

The seminar *Algebra and Symmetries in Combinatorics and Optimization Topics*, held on 30 June, addressed topics such as the Fourier spectrum of symmetric Boolean functions, lattices and spherical designs, and group theoretic algorithms for fast matrix multiplication. The seminar was organized in collaboration with DIAMANT and the NWO-Spinoza project. DIAMANT is one of the three mathematics clusters in the Netherlands.

Matrices and matroids

Bert Gerards was invited to give a keynote lecture at the International Congress of Mathematicians in Madrid on 28 August. This is the world's premier conference for mathematicians, attracting thousands of delegates. Gerards' lecture *Towards a Structure Theory for Matrices and Matroids* explored issues surrounding the use of graphs and matrices as modelling tools for real-world problems, such as road networks, telephone communications, and train schedules. The aim of Gerards' work is to gain a better understanding of the structure of graphs and matrices, as abstracted by matroids, with the ultimate goal of establishing more efficient algorithms.

Hopf Algebras

On 7 September, Michiel Hazewinkel marked his retirement from CWI with a special symposium on his favourite area of research: Hopf Algebras. The symposium *Hopf Algebras and What They Are Good For* featured presentations by leading experts in the field. Hans Jürgen Schneider (University of Munich) explained the relation to tensor categories, while Anders Lindquist (Royal Institute of Technology, Stockholm) presented a universal solution to the generalized moment problem. Other speakers were Tom Koornwinder (University of Amsterdam) and Alain Lascoux (University of Marne-la-Vallée).

Michiel Hazewinkel

The 7th International Conference on Product Focused Software Process Improvement (PROFES).

Meteorological flow models

Atmospheric and oceanic flows exhibit complex multi-scale dynamics that present a challenge for both analytical and numerical methods. CWI co-organized the workshop *Geometric and Multiscale Methods for Geophysical Fluid Dynamics* to seek a practical synthesis of different modelling techniques by way of active dialogue with scientists from meteorological centres. The workshop took place at the Lorentz Centre in Leiden from 2–6 October.

Dynamics of patterns

An audience of physicists, mathematicians and theoretical biologists attended three one-day seminars on the Dynamics of Patterns. At the first seminar, on 19 October, Ute Ebert revieved experiments exploring electrical streamer patterns in air and nitrogen. The other two seminars took place on 8 February and 23 May.

Software pioneers

Software has only been around for half a century. Since the coding of the early machines in the 1950s, the writing of software gradually evolved into an autonomous practice. Early software pioneers gathered at CWI on a conference to discuss the rapid developments in this field. They reflected on the growing pains of software development, from late deliveries and poor conformity with specifications, to simple accidents. They discussed the perceived crisis in the field in the late 1960s, as well as the role of European academics, who tended to prefer the niche that is theoretical research, as symbolized by abstract reflection on the design of languages.

The conference also reviewed the development of more advanced programming languages, compilers, operating systems and application software. Willem van der Poel of the Delft University of Technology, a pioneer in hardware and software development, discussed the users group for his 1957 ZEBRA computer, one of the very first computer communities. Maurice Verhelst (founder of SAI - Studiecentrum voor Automatische Informatieverwerking in Belgium), Gerhard Goos (compiler Construction) and Wilfried Brauer (theoretical computer science) were other speakers.

The IFIP symposium *Pioneering Software in the 1960s in Germany, Belgium and The Netherlands* was held from 2–4 November to mark the 90th anniversary of the birth of Aad van Wijngaarden (1916-1987), the founding father of computer science in the Netherlands and former director of CWI. The symposium was sponsored by CWI and NWO Physical Sciences.

Formal methods for software

The 5th Symposium on Formal Methods for Components and Objects (FMCO) was held at CWI from 7–10 November. Researchers and engineers from the fields of software engineering and formal methods gathered to discuss concepts relating to component-based and object-oriented software systems. The purpose of the FMCO symposia is to foster collaborative work, discussions and interaction.

Network performance

Without careful network planning and management, the expected dramatic increase in demand for internet applications may lead to substantial degradation of connection quality. There is a growing need for traffic management technology in complex

Participants of the Pioneering Software Symposium, among others: Willem van der Poel (first from left), Gerhard Goos (fifth from left, behind Ms Ute Brauer), organizer Gerard Alberts of the University of Amsterdam (ninth from left), and Wilfried Brauer (on the right).

environments. These issues were addressed at the workshop *Stochastic Performance Models for Resource Allocation in Communication Systems*, which was held at CWI from 8–10 November. Organized within the framework of the EuroNGI Network of Excellence, the StoPeRA workshop emphasized the use of advanced queueing models and other innovative probabilistic modelling approaches.

Space mapping

On 13 November, the Dutch Ministry of Economic Affairs sponsored a one-day workshop on Space-Mapping and Efficient Optimization. The workshop introduced several efficient optimization techniques for computing-intensive design problems, from both theoretical and practical perspectives. Topics included surrogate-based optimization, filters and response surfaces.

Other meetings

• On 12 May Bert Bos (W3C) gave a Master Class in Cascading Style Sheets (CSS) in the W3C Benelux Office, managed by CWI.

W3C CSS meeting with Bert Bos (fourth from left).

In January, the W3C Offices meeting was hosted at CWI.

• The ECCOMAS CFD conference took place from 5–8 September. The BRICKS project Scientific Computing, coordinated by CWI, was closely involved.

• The Conference of the Dutch-Flemish Numerical Analysis Communities took place from 11–13 October at Woudschoten near Zeist, the Netherlands, with support from CWI.

• From 13–15 November, CWI organized the 35th annual Meeting of Dutch Statisticians and Probabilists in Lunteren. The meeting was sponsored by the Research Council for Physical Sciences of NWO, the Netherlands Society for Statistics and Operations Research (VVS), the Mathematical Research Institute (MRI), and the Thomas Stieltjes Institute for Mathematics.

• Software as service has been identified as one of the four key focal points of activity in the new CWI strategy plan. The first in the CWI Service-oriented Computing Platform's ongoing series of bimonthly seminars took place on 20 November. These seminars are intended as a platform for presenting SoC related work from both inside and outside CWI. They are open to the public.

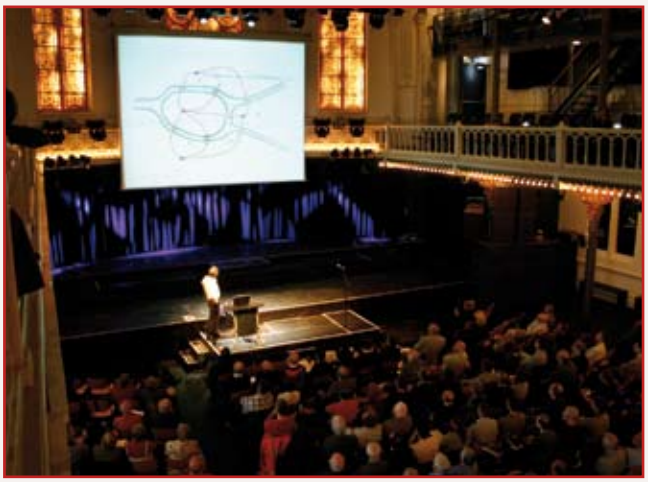
• CWI sponsored the Holland Open Source Software Conference 2006, where representatives of industry, education and science discussed open source software.

6 To increase public interest in mathematics and computer science

CWI organizes activities to show the fun side of science, inspiring people to gain a better understanding of mathematics and computer science.

Breakthroughs in mathematics

On 21 May, Lex Schrijver gave a lecture in Amsterdam's pop temple, Paradiso, on the future of mathematics. This was one of a series of public lectures in which eight scientists look to the future and explore the big questions and fundamental elements upon which our existence is built. The series reflects on the imminent breakthroughs we might expect. In his lecture *How Far Can We Calculate?* Lex Schrijver discussed a wide range of topics, including the problem of the travelling salesman, the Chinese postman, and the making of a rail timetable. The popular scientific lectures, which have been held at Paradiso for the past ten years, are a joint project of the K.L. Poll Foundation, NWO, Paradiso, and the broadcasting organization VPRO.



Alexander Schrijver in Paradiso

Biographies of mathematicians

The Biographical Dictionary of Dutch Mathematicians (BWNW) went online on 21 September. The brief biographies of Dutch mathematicians will be useful for teachers who want to brighten up or enrich their lessons, students and scholars looking for reference material, and science journalists. The dictionary can be consulted online at www.bwnw.nl. The project is sponsored and hosted by CWI.

Alex van der Brandhof (second from left), BWNW coordinator.

Mad about mathematics, crazy about computer science

On 21 October, CWI held an open day, where young visitors could play around in the fun lab or make electronic games. There was a science cafe with mini-classes on various topics, including computers, football, and the mathematics of sand ridges on the beach. Elsewhere, brains were teased with puzzles, riddles and problems, geometrical theorems danced on screens, and shapes and colours were juggled. Researchers showed children how to search in digital art collections and explained the mathematics underlying lightning bolts. And then there was the popular bridge-building contest – using paper and glue only. The bridges were weighed down until they collapsed. The last bridge standing won. The open day also paid special attention to girls, with a historical film showing how many women used to work on large calculations. There was also a special fun lab for girls.

The most exact science of all

Why can a computer calculate much more quickly than a person, while a person can recognize a face much more competently than a computer? How reliable is the evidence in a murder case? Is there such a thing as a perfect voting system? How does an internet search engine find what you're looking for? Is there a mathematics of love? These and many other applications of mathematics and computer science are described in *Opgelost* (Solved!), a book for the general public, published by CWI on 16 November 2006 to mark the institute's 60th anniversary. The book takes a light-hearted look at the role that mathematics and computer science play in our daily lives, but also under more unusual circumstances, discussing applications in sports, games, politics, economics, industry, tracing techniques, music and visual arts.

The book explains that no other science is as exact and universal as mathematics. Two plus two is always four. And Pythagoras' theorem applies equally in Tokyo and Timbuktu. That makes mathematics a multi-faceted and unequalled logical apparatus. Each chapter in *Opgelost* consists of set features, including a do-it-yourself section (e.g., a puzzle or a murder mystery), an unsolved problem from mathematics, and an interview with an expert, who discusses his or her favourite mathematical formulae.

This richly-illustrated book is a pleasant read for anyone who is curious about mathematics and computer science and their applications. *Opgelost* was written by physicist and freelance science journalist, Bennie Mols, long-time editor of the magazine *Natuurwetenschap & Techniek* (Natural Science and Technology).

The publication of *Opgelost* was jointly financed by CWI and the NWO Spinoza premium, which was bestowed on Lex Schrijver in 2005 for his work in combinatorics and algorithms. The NWO Spinoza premium is the Netherlands' most prestigious scientific award.

Impressions of CWI's open day.

Navigation for children

What is the shortest way home from school? Alexander Schrijver discussed this at the Wakker Worden (Wake Up) children's lecture in Amsterdam's Nemo science museum on 9 November.

All of the children were given a map with which they could plot the best route. They then had to add up the lengths of all the streets they would walk on the way. Not everyone chose the same route. Using the children's drawings, Schrijver explained the mathematical concepts used in navigation systems. Several of these widely-used concepts were developed by Edsger Dijkstra, who worked at CWI. Lex Schrijver also presented an impossible

(pictures: Hanne Nijhuis)

planning problem, which the children obviously couldn't solve, and then showed how Euler had devised the problem in 1736.

Schrijver went on to explain the importance of the insight the kids had gained. It would be useful for planning their rounds on Martinmas, the feast of St. Martin on 11 November. On that day, many Dutch children go from door to door singing for sweets. By planning their trips carefully, the kids wouldn't miss any streets and disappoint people waiting at home to hand out sweets.

At the end of the reading, Schrijver held a competition to see who could help the postman find the shortest route, passing each house at least once? There were seven winning entries.

Free cards for mathematics

How can you raise teenagers' interest in scientific research? This was the topic of a competition for all Bsik projects, which are financed by a substantial government fund that is earmarked to strengthen Dutch knowledge infrastructure. Researchers were asked to demonstrate that they could make their knowledge attractive to a young audience.

The competition was won by BRICKS, the Bsik-consortium for mathematics and computer science, which is coordinated by CWI. BRICKS' winning idea was to design 'postcard puzzles' that challenge youngsters to think about mathematics and computer science in a fun way. They can get a head start by visiting the youth section of the BRICKS website (www.bsik-bricks.nl), where they will discover why science is so important and gain insight into the many applications of mathematics and computer science. The site also offers a number of hints between the lines, enabling the kids to find sound solutions to the postcard puzzles.

BRICKS will use the prize of EUR 10,000 to widely distribute the puzzle cards at Dutch secondary schools in 2007.

Martine Roeleveld, BRICKS Public Relations Officer, receiving the BRICKS Award 2006 after the 'Best of Bsik: the Battle' contest. (picture: Robert Goddyn)

More public events

• Contribution to the exhibition *The ICM through History*, organized for the International Congress of Mathematicians 2006 (ICM) in Madrid.

Guillermo P. Curbera (University of Sevilla), curator of the exhibition The ICM through History.

• Sponsoring of the *Doeboekjes* (Do-it-yourself booklets) published as part of *Vierkant voor Wiskunde* (Mad about Mathematics) aimed at 10–18 year olds.

• Jeroen Wackers joined the Klokhuis Question Days for children in science center Nemo on 2 April as a maths expert.

• CWI sponsored the article *Mathematics in the Netherlands* for students on *www.science-engineering.net*, http://www.science-engineering.net/europe/maths-netherlands.htm

• On 28 November, Stefano Bocconi gave a public demonstration of his PhD project on Noorderlicht Radio, a public radio station. He discussed the Vox Populi system, which automatically generates video documentaries from semantically annotated media repositories. See page 18.

Research Highlights

Efficient health care

Chronically ill patients in hospitals are wheeled from one medical device to the next. Schedules for diagnostic tests are notoriously difficult to make, especially if several tests have to be completed in a short time. Nursing staff spend many hours a week consulting with various departments, trying to plan their patient schedules. Hospital logistics are highly complex, but the research project Medical Information Agents offers solutions for planning.

Decentralized planning

Planning procedures that work in industry cannot easily be applied in hospitals. Planning of all medical equipment and facilities is too complex for classical planning software. Last-minute changes and emergencies result in constantly changing schedules. A chosen treatment can change at any given moment, based on a new diagnosis. The activities in hospital wards are simply too closely intertwined. An operating theatre goes unused if bed space is unavailable in the adjoining IC unit. That is undesirable. In order to keep health care affordable, scarce hospital resources should be used with the highest possible efficiency.

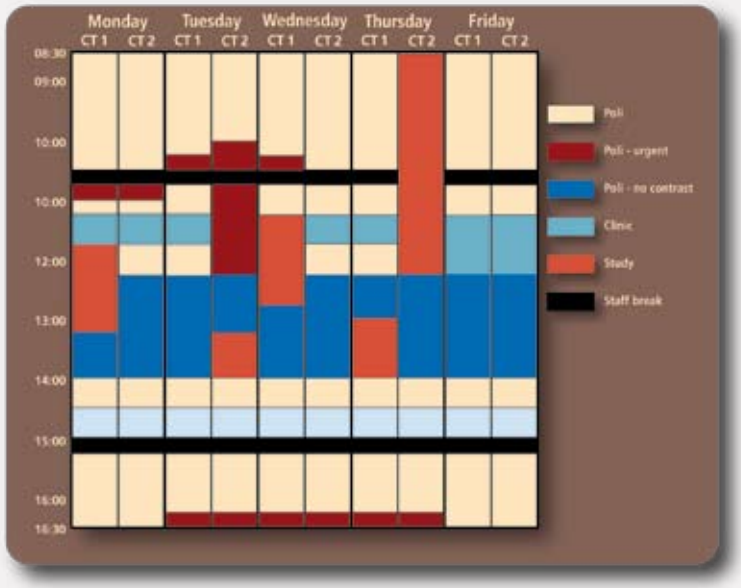
Centralised planning appears to be infeasible for hospitals. This is mostly due to its complexity and to the different operating procedures for different medical disciplines. A strong professional culture also makes it difficult to implement central efficient scheduling between many departments. In practice, decentralised planning already takes place at the separate departments. This is the most convenient way to arrive at some sort of schedule. The departments confer with one another if a patient is, for example, moved from the intensive care unit, or if appointments have to be reshuffled. However, because departments are not in constant consultation, many opportunities go unexploited.

Software agents can assume tasks from departmental planners. Agents are independent pieces of software that can perform tasks for their owners and that can communicate with each other. Until now, such agents have mostly been designed for market or manufactoring purposes, such as trading in electronic market places. Such software agents trading with the outside world should have learning capabilities and should be able to deal with competition. Collectively, these standalone agents could drive market optimization. They ensure that the right goods are delivered to the proper agents at the best price.

These agents can also be used in circumstances where profit maximization is not necessarily the prime objective. They could be programmed to give the chief priority to high occupancy rates and short waiting times. This means they are also suitable for hospitals.

Researchers Anke Hutzenreuter (TU/e and CWI) and Han La Poutré (CWI) are building health care planning agents for the Catharina Hospital in Eindhoven, the Netherlands. The agents are designed for scheduling surgery and the subsequent care, which means that various agents have to plan the schedule of the various care units: the intensive care unit, which is in turn linked with the medium care unit and the nursery. In the case of standard surgery, the subsequent process is relatively easy to predict, but complications may arise. In various instances, the schedule may shift because patients can be moved out of the intensive care unit ahead of schedule or, worse, later than scheduled.

In automated planning, each department is represented by a different software agent. These agents communicate and negotiate with one another, increasing the capacity of the entire chain. The agents use advanced models and algorithms to do so. The project is currently in the simulation phase with actual patient data. This new planning method promises to free up capacity in operating theatres and improve availability guarantees.



Parts of a resource calendar are typically allocated to different patient groups. This allocation must be flexible to make efficient use of the resource.

Patient-to-patient negotiation

Ivan Vermeulen, Sander Bohte, and Han La Poutré of CWI are also running a project at the Academic Medical Centre (AMC)

in Amsterdam. This project involves the schedule of various medical tests, like on a CT scanner for the lung function.

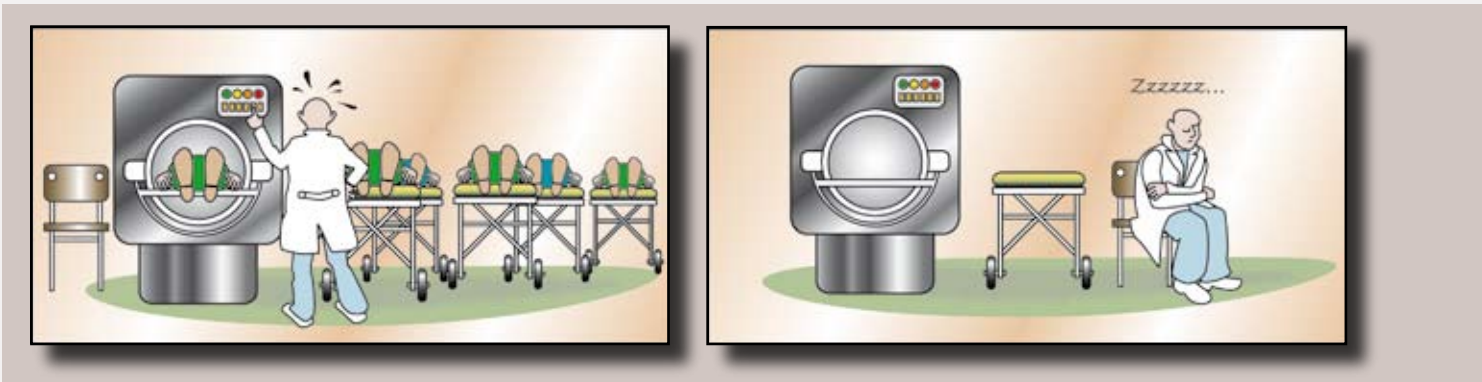
For a patient, multiple tests must be performed. As planning progresses, more and more appointments are fixed and it becomes increasingly difficult to efficiently schedule new appointments. Appointments made well in advance hamper optimal scheduling. In the first phase of the research for this instance, the software agents primarily focus on advance appointments. All patients are represented by separate agents, which exchange separate appointments in consultation with one another. The agents aim to arrange exchanges in such a way that the total set of tests for each patient is rounded off as quickly as possible, ensuring that the results are available sooner. The prime objective is to ensure that no exchange is detrimental to a patient; i.e., they should not have to wait longer for the completion of all their appointments than before and it should fit in their agendas. This gives rise to an exchange system that produces a more favourable schedule than is currently the case. In fact, the new schedule is almost optimal, because advance appointments are rescheduled. Patients could be presented with an incidentally proposed change via SMS, email, or in the future, personal agenda agents.

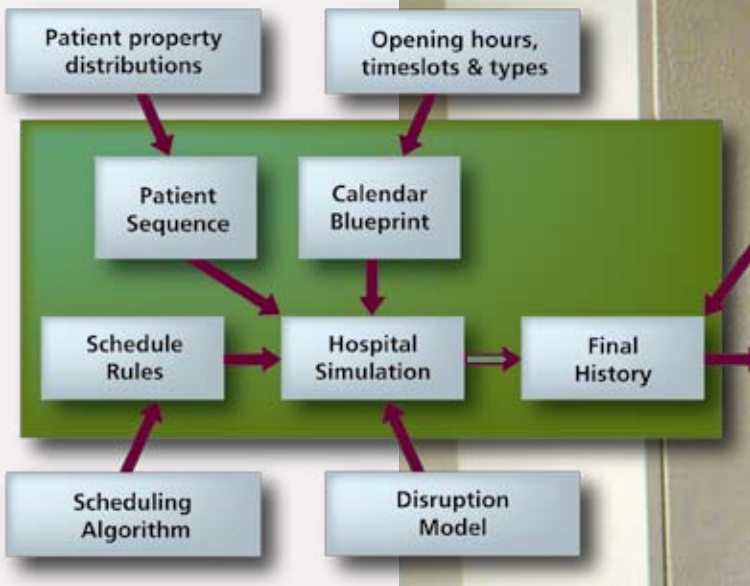
At the AMC, medical information agents have subsequently been designed to allocate time for different types of medical tests involving CT scanners. For instance, a doctor must be present when scans are conducted using contrast fluid. These scans usually take place at set times, which are labelled for this in advance, before appointments are made with patients. Advance labelling and reservation of time slots is also done for various types of emergencies. The question is: How much time must be reserved and labelled for these special scans and when can labels be changed? The software agents make use of dedicated models as well as algorithms that learn from past experience and that can therefore help to resolve this kind of planning problem. The solutions that have now been developed are currently considered to be deployed and marketed together with a software supplier. At the same time, the research is also continued towards scheduling multiple appointments for a patient on the same day. This requires extended and further advanced agents, models, and algorithms.

Divide by division

Decentralised planning offers hospitals the degree of flexibility they need to adjust to ever-changing demands. In principle, the decentralised approach to planning also allows them to factor in activities that take place outside the hospital. Data collected via mobile heart monitors and home diagnosis could also be used to reserve time slots for patients, that probably would need urgent action. Decentralised planning closely reflects the concept that medical care operates as an organic whole, in which the central hospital and medical facilities in the surrounding area are all interlinked.

Doctors and patients at the CT-scanner.
Left and middle: nowadays it is often all or nothing.
Right: with better and adaptive planning the workflow is equally divided.





Patient scheduling simulation model (green box) for a single resource, and its in- and outputs.

Research Highlights

Models for better ships

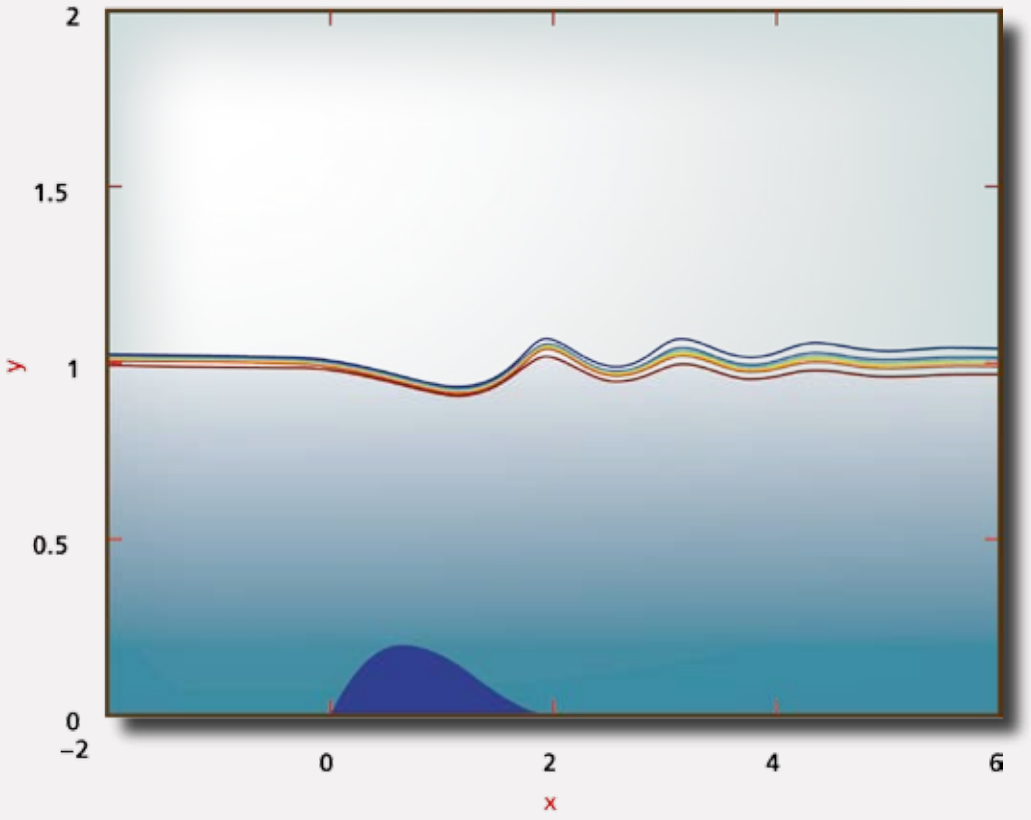
The flow of water around a ship is a key factor in fuel consumption. The simulation of flow patterns around the hull is therefore an important aspect of ship design. Lengthy computations are required for such simulations. But the research of Jeroen Wackers and Barry Koren shows that these computations can be conducted with much greater speed and precision.

Water turbulence reduces the efficiency of a ship's propeller. The propulsion system works best when the water is undisturbed, but that certainly isn't the case in a ship's wake. The stern of most ships is therefore designed to ensure a relatively regular flow pattern. The bow wave is also a key factor in energy consumption. Energy is expended in creating waves. That means a smaller bow wave results in less energy loss.

Ship designers study these phenomena to be able to design better ships. The ultimate goal is to calculate what ship shape best meets the different demands, not only in terms of fuel efficiency, but also with respect to stability, safety and logistical efficiency. To study the properties of ships, designers need software to simulate wave and wake patterns around the hull. However, the computation of such flow patterns is a time-consuming process, because waves take a long time to dissipate. During simulation, the waves wash around in the computer for a long time before a stable wave pattern emerges. Such computer simulations therefore require numerous computational steps before a usable result emerges. Moreover, repeated simulations have to be conducted for all sorts of sailing conditions and ship speeds. In practice, such simulations are insufficiently precise. That means there is a need for computation methods that produce a stable wave pattern more quickly.

The ever-changing surface

The surface of the water presents a computational problem, because it changes constantly. Computations could be carried out much more quickly if the water surface was not a factor. In the case of a submerged body, it is possible to directly calculate the stable flow pattern, without having to progress through each



Water flows from left to right in a long tank with a bump in the bottom. Numerical simulation predicts the waves on the water surface. (source: CWI)

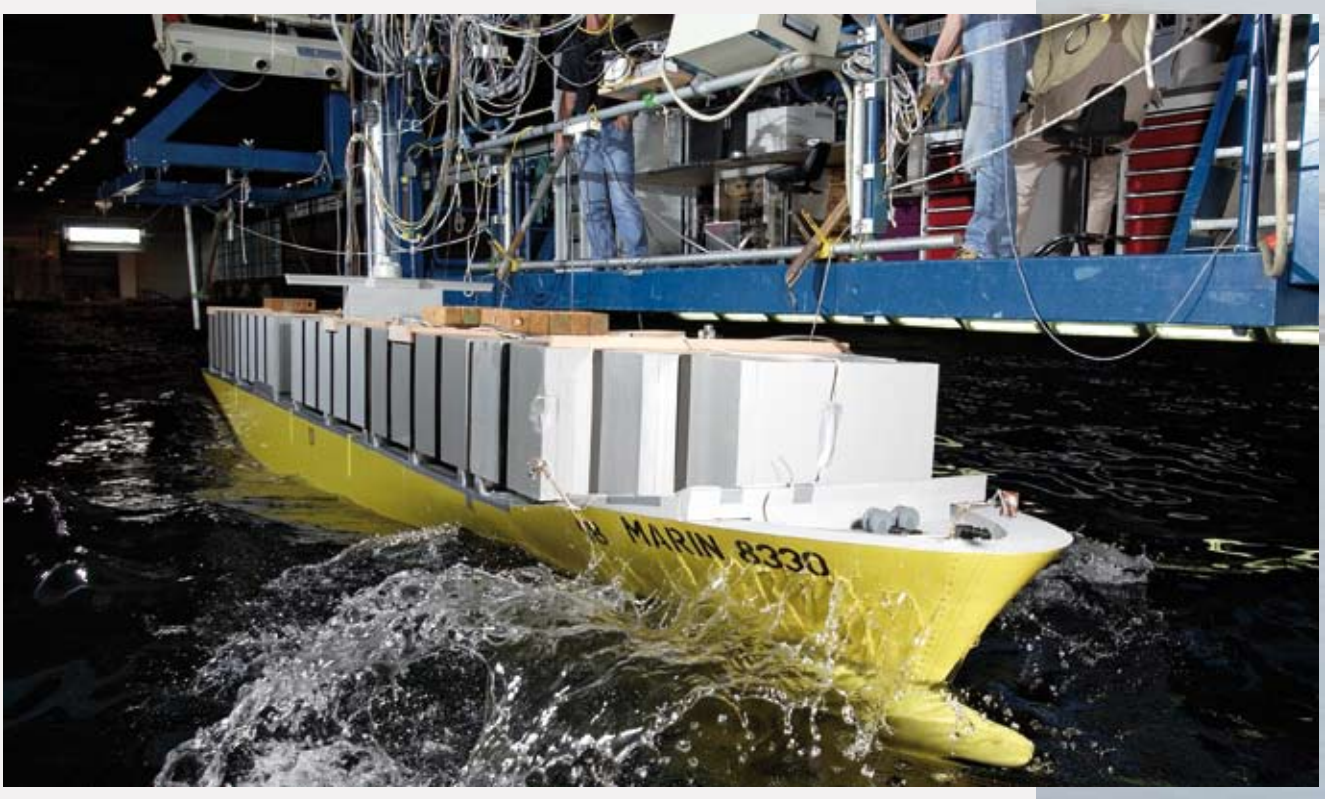
successive time phase. The water surface is no longer a boundary of the flow domain, it now lies in the interior of the domain.

Jeroen Wackers and Barry Koren found a solution for this problem by explicitly factoring in the air above the water surface. Air can be considered a fluid with a very low density, and there are several good algorithms describing the interplay of two fluids, allowing rapid computation of a stable pattern in which all forces are in equilibrium. That means the water surface no longer constitutes the boundary condition of the problem, and no longer has to be specified. The entire simulation area – water and air – is treated in one and the same manner.

Much greater speed

Using this two-fluid approach, a flow in a canal was simulated. Irregularities on the canal bed caused waves on the surface, as is the case in reality. The results were calculated dozens of times more quickly than the classical simulation method, in which all successive time phases must be computed.

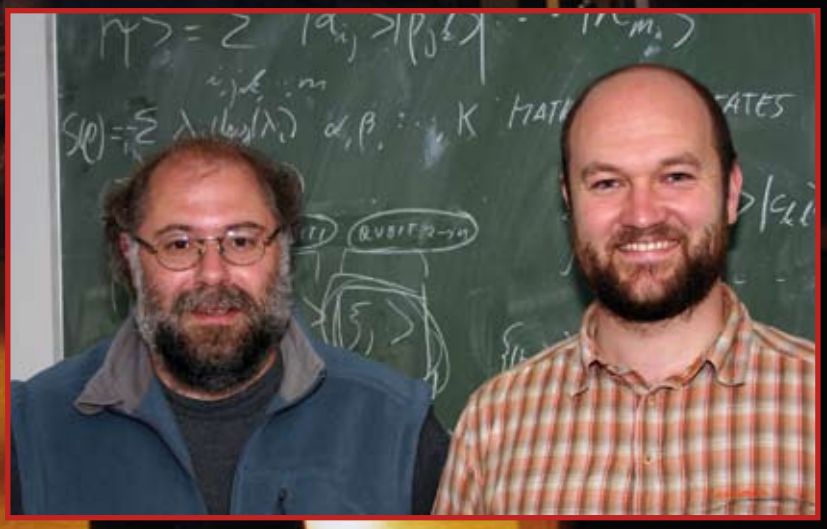
The study of Wackers and Koren will enable a reliable and efficient method of calculating flow around ships, allowing the prediction of performance, stability and control under various sailing conditions. This will give rise to better design tools, and, ultimately, better ship designs. Wackers conducted his research at CWI as part of the BRICKS programme.



Model testing of container vessel in Seakeeping and Manoeuvring Basin, at MARIN (Maritime Research Institute Netherlands) in Wageningen.
(© MARIN)

Picture kind permission of www.transportcafe.co.uk

Research Highlights



Quantum information processing

Work on quantum entanglement at CWI gives new insight in the non-locality of nature. There is also a suprising connection to fault tolerant computing and the feasibility of quantum computers.

In 1935 Einstein, Podolsky, and Rosen devised a famous thought experiment that was later called the EPR-paradox. It was their attempt to show that quantum mechanics was incomplete. Following the axioms of quantum mechanics, they showed that it is possible to construct two particles that are strongly coupled. Suppose that Alice in Amsterdam has one particle and Bob in New York has the other. When Alice measures her particle she will observe a random outcome 0 or 1 each with equal probability. The same is true for Bob when he measures his particle. However, the outcomes of Alice and Bob are correlated: They always obtain the same value. Such particles are called entangled. It seems that the outcome of the measurement of Alice instantaneously influences Bob's outcome. Einstein, Podolsky and Rosen argued that this should not be possible since nothing goes faster than the speed of light.

In order to explain this apparent non-local phenomenon one tried to come up with local classical theories, so-called local hidden variable models. One could argue that the outcome of Alice's and Bob's measurement was already known at the time the two entangled particles were created, and that their correlation thus would not require instantaneous communication.

It was John Bell who in 1964 came up with the description of a clever experiment that would shed more light on the situation. He created a game and showed that if quantum mechanics is non-local then Alice and Bob can win this game with higher probability than what is possible classically. In the early 1980's Alain Aspect and his group at Orsay in France demonstrated with this experiment that with the use of entanglement this game can be won with higher probability than what is possible classically! Nature is indeed non-local and there is no local hidden variable model that can explain it.

Quantum computing and entanglement

The quantum computing group at CWI in cooperation with North-American groups in the late 1990's addressed the EPR non-locality issue in more operational terms. In the framework of quantum mechanics entangled particles can not be used for communication between Alice and Bob. This non-signalling property is important since it would otherwise be in direct conflict with Einstein's theory of relativity. But the research groups showed that certain distributed computation tasks can be solved with less communication when one makes use of entanglement.

Take for example the agenda problem: Alice and Bob want to make an appointment and need to know what free slots the other still has available in his or her agenda. If Alice and Bob share entangled particles and have a quantum computer, they can make an appointment with significantly less communication than what is possible classically. For certain problems, there even is an exponential saving in communication. This computer science point of view illuminates the bearing, hinted at by Einstein, Podolsky, and Rosen, that non-locality has on communication: In certain cases entanglement can be used to communicate more efficiently, but it can not be used to replace communication altogether.

Savings in communication are not always possible. For example, if Alice and Bob want to count the number of appointments that they could make, they can not figure this out more efficiently with entanglement even if they just want to know whether this number is even or odd.

Beyond Quantum Mechanics

In an attempt to better understand the non-local aspect of nature, Popescu and Rohrlich in the 1990s investigated in more detail a non-locality game introduced by Clauser, Horner, Shimony, and Holt based upon Bell's original idea. This CHSH game can be won with probability roughly 85 percent when making use of entanglement whereas without, it can only be won 75 percent of the time. Popescu and Rohrlich showed that this game in principle can be won 100 percent of the time by Alice and Bob without violating the crucial non-signalling primitive. They raised the question: "Why is nature not more non-local?"

A partial answer was given by Wim van Dam, at the time PhD student in the CWI group. He showed that if nature allowed the CHSH game to be won with 100 percent, then every distributed communication task would become trivial, and would only require a single bit of communication. In this hypothetical setting Alice and Bob could, with just one bit of communication, find out whether the appointments they could make are even or odd.

Buhrman and Unger, together with groups in Montreal and Bristol, investigated this matter further and examined the case when nature would allow this game to be won with probability in between 85 percent – the quantum mechanical bound – and 100 percent – the ideal Popescu-Rohrlich bound. Their findings – reported in Phys. Rev.Letters and reviewed by Popescu in Nature Physics – show something remarkable. There is a sharp

threshold with respect to the probability to win the CHSH game and communication required for every distributed task. They show that when one can win the CHSH game with probability around 90 percent still every distributed computation problem can be solved with a single bit of communication. On the other hand at 85 percent many problems require a lot of communication. These results indicate a different reason why nature is not more non-local than at least 90 percent, since this would render communication tasks trivial. It is a fascinating open problem whether the true threshold of where communication tasks become trivial lies at the quantum mechanical bound of 85 percent or is in fact higher.

The feasibility of a quantum computer

These results were not only valuable in terms of physics theory, but also have intriguing consequences for the efficiency of computers. The high-speed computers that are set to make their entry in the coming years will inevitably be prone to errors, owing to the practical limitations of manufacturing procedures for microprocessors. Computer science has a solution for this problem in the form of fault-tolerant algorithms, where supplementary processing allows results to be verified and possibly adjusted. The computer components that carry out these adjustments are of course also susceptible to error. This implies that there are limits to the degree of error that can be rectified in this manner. This threshold is important when it comes to quantum computers since they will inevitably be prone to error. They should therefore be designed with fault-tolerance in mind. But this raises the question: at what level of error is quantum computing impossible?

Buhrman and fellow researchers have discovered a surprising connection between fault-tolerant computation and the results on non-locality. By exploiting this connection they have constructed a new upper bound for the error threshold, above which quantum computers would be unable to function. The exact bound of this error threshold is important to establish since it shows exactly how reliable the components of a quantum computer must be in order to function properly. Currently the best known bound for the error threshold is still far away from the errors observed during experiments in the laboratories around the world.

Keep communication simple. How much information does Bob have to send to Alice in order to fix a date?

Research Highlights

Larger diamonds thanks to discrete mathematics

CT scans are set to become far more efficient. That is the outcome of a study conducted by Joost Batenburg, who obtained his PhD in 2006 with a thesis on algorithms for computer tomography. The results of Batenburg's research offer new prospects for medical diagnosis, but are also of interest to diamond cutters. It also allowed him to capture images of individual atoms in small crystals.

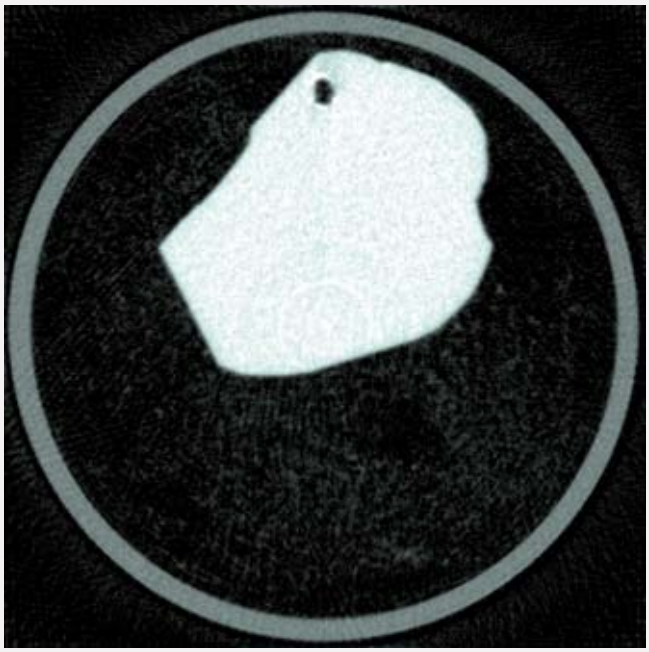
A CT scan consists of hundreds of X-ray images, each of which is made at a slightly different angle. Individually, these are little more than two-dimensional images, but together they provide enough data to reconstruct a three-dimensional image. Over the years, various algorithms have been developed for the computation of such three-dimensional images. The more X-ray images used to reconstruct the three-dimensional image, the more detailed it will be. The opposite also applies. If too few images are available, a vague image is produced.

Existing reconstruction algorithms for tomography produce unsatisfactory results if fewer than ten X-ray images are available. However, this problem can be solved if the reconstruction process incorporates additional knowledge. In industry, for example, many products are scanned to check whether they contain hidden cracks or cavities. In such instances, not all greyscale values have to be computed to produce a 3-D image. Black and white are sufficient. The material is either present or absent. This type of reconstruction, using only a limited range of greys, is known as 'discrete tomography'.

Sharper reconstruction with fewer images

Algorithms for discrete tomography produce much sharper 3-D reconstruction using fewer X-ray images, because a priori information is incorporated into the computation. However, this does not necessarily imply that such images can be computed more quickly. Reconstructions of images based on a continuum of greyscale values are easier to compute than when only a limited number of such values are available. When Joost Batenburg started his research, reconstruction algorithms in discrete tomography were limited to images no bigger than 50 by 50 pixels. That is rather small, in this age of megapixels. In practice, it was impossible to make use of a priori information to produce sharper images. It is therefore customary to simply produce extra images during CT scans to ensure sharper images, even though this results in higher radiation levels and higher costs.

In collaboration with Robert Tijdeman (Universiteit Leiden) and Herman te Riele, Joost Batenburg devised a new computation procedure. The trick is to ensure that the X-ray images are not all evaluated simultaneously. Instead, the computer evaluates the images in pairs. Based on just two X-ray images, it produces a rough three-dimensional reconstruction. This rough image is subsequently used as prior information for the evaluation of the next pair of images. In this way, the computer repeatedly reconstructs a three-dimensional image using two X-ray images. As computation progresses, the reconstruction becomes more precise. Even very tiny, single-pixel details are eventually reconstructed with great accuracy.



2D Section of a rough diamond, reconstructed from 125 projections with conventional tomography. Discrete tomography needs much less scans.

Because only two images are used in each instance, the required computation is much less complex. In fact, the computation has much in common with the so-called minimum cost flow problem, a notorious computational challenge in the field of operations research. The problem in question is all about calculating the most efficient way of pumping a fluid through a flow network. This problem has been studied extensively, resulting in a wide range of efficient algorithms.

Megapixel scan

Batenburg's computer program required the integration of knowledge from three highly diverse fields – mathematics, computer science and physics. Fortunately, Batenburg graduated cum laude in two of these fields. Insight into coding theory was required to adjust for noisy data; insight into number theory and non-numerical mathematics was required for the systems of linear equations with natural numbers; and he also applied knowledge from the fields of evolutionary algorithms and operations research.

The program Batenburg developed produces images of about one megapixel. That is large enough to ensure the feasibility of this approach, which was subsequently used to study osteoporosis in mice, in collaboration with the University of Antwerp. In bone scans of this kind, only a limited range of greyscale values are required, because osteoporosis causes cavities in the bones. So bone material is either present or absent.

Joost Batenburg also teamed up with the Materials Sciences Division of the Lawrence Berkeley National Laboratory, which is studying nanocrystals. These miniscule crystals, consisting of no more than several hundred atoms, are used in LEDs and catalysts. The materials experts in Berkeley routinely conduct electron microscopy studies of these crystals to measure the number of atoms in each crystal plane. Joost Batenburg calculated the exact position of these atoms. In short, his new computation method allowed him to capture images of individual atoms in nanocrystals. This is an important development for materials experts. If they can see exactly what they have created, they can improve their production methods.

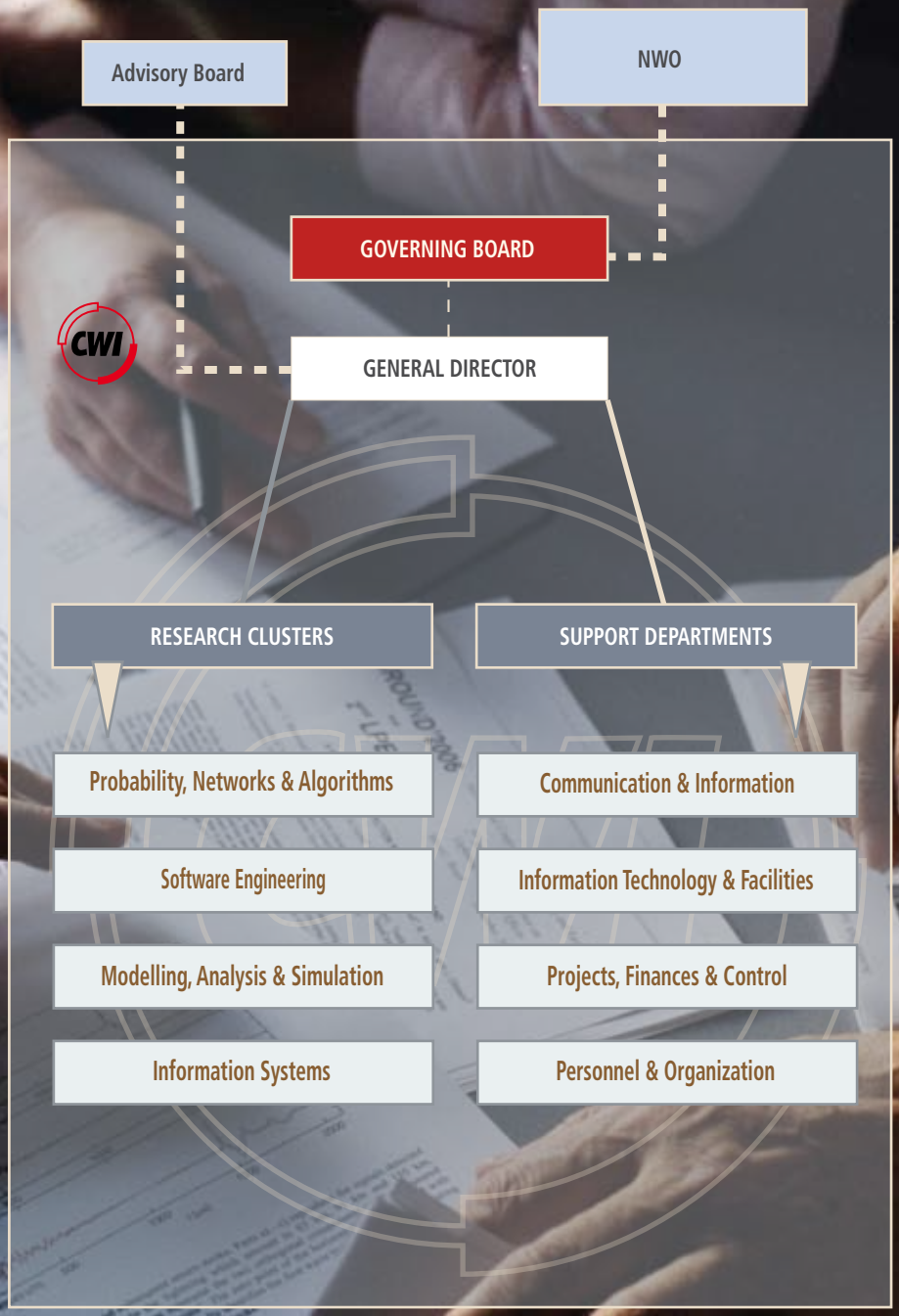
Cutting larger diamonds

The diamond industry in Antwerp also expressed an interest in discrete tomography, which would allow large diamonds to be cut with greater precision. If a diamond has flaws, it is sometimes better to split the stone. It is also very useful to locate the most attractive facets of a diamond before cutting begins, as this enables a diamond cutter to retain 5 to 10 percent more of each stone. However, an ordinary CT scan of a diamond can take many hours to complete, because X-ray images of diamonds always require lengthy exposure times. Consequently, the additional yield produced by CT scans often does not offset the extra costs. In the case of discrete tomography, however, a clear three-dimensional image can be reconstructed using fewer X-ray images.

These are but a few of the many new possibilities. Batenburg's research team now aims to develop a stronger theoretical foundation for the newly developed algorithms. They are currently considering generalizations of the algorithm to other areas of interest, such as the reconstruction of images using more than two greyscale values, or the reconstruction of three-dimensional images. Other potential areas of application include medical imaging and tomography of industrial objects, such as nanosize electronics and critical parts for aircraft.

Joost Batenburg's research was awarded the Philips Mathematics Prize for PhD students in March 2006, and the C.J. Kok Prize of the Universiteit Leiden in January 2007.

Appendices


Advisory Board
NWO
GOVERNING BOARD
CWI
GENERAL DIRECTOR
RESEARCH CLUSTERS
SUPPORT DEPARTMENTS
Probability, Networks & Algorithms
Communication & Information
Software Engineering
Information Technology & Facilities
Modelling, Analysis & Simulation
Projects, Finances & Control
Information Systems
Personnel & Organization

Organization

Research

Cluster	Cluster leader
Theme	Theme leader
Probability, Networks and Algorithms	**A.M.H. Gerards**
Algorithms, Combinatorics and Optimization	M. Laurent
Performance Analysis of Communication Networks	M.R.H. Mandjes <1 October > R.D. van der Mei
Stochastic Dynamics and Discrete Probability	J. van den Berg
Signals and Images	E.J.E.M. Pauwels
Cryptology and Information Security	R.J.F. Cramer
Software Engineering	**P. Klint**
Interactive Software Development and Renovation	P. Klint
Specification and Analysis of Embedded Systems	J.C. van de Pol
Coordination Languages	J.J.M.M. Rutten
Computational Intelligence and Multi-agent Games	J.A. La Poutré
Distributed Multimedia Languages and Infrastructures	D.C.A. Bulterman
Modelling, Analysis and Simulation	**J.G. Verwer**
Nonlinear PDEs: Analysis and Scientific Computing	A. Doelman
Computing and Control	B. Koren
Nonlinear Dynamics and Complex Systems	U. Ebert
Information Systems	**M.L. Kersten**
Standardization and Knowledge Transfer	M.L. Kersten
Database Architectures and Information Access	M.L. Kersten
Semantic Media Interfaces	L. Hardman
Visualization and 3D Interfaces	R. van Liere
Quantum Computing and Advanced Systems Research	H.M. Buhrman

Management

Management Team

J.K. Lenstra (general director)
D.G.C. Broekhuis
A.M.H. Gerards
M.L. Kersten
P. Klint
J.G.Verwer

Governing Board

P.W. Adriaans (University of Amsterdam), chairman
C.J. van Duijn (Eindhoven University of Technology)
F.A. van der Duyn Schouten (Tilburg University)
J.N. Kok (Leiden University)
S.J.M. Roelofs (ICT~Office)

Support

Communication and Information

G.M.T. Nieuwendijk <1 May > J.W. Besteman

Information Technology and Facilities

I.L. Dijkstra

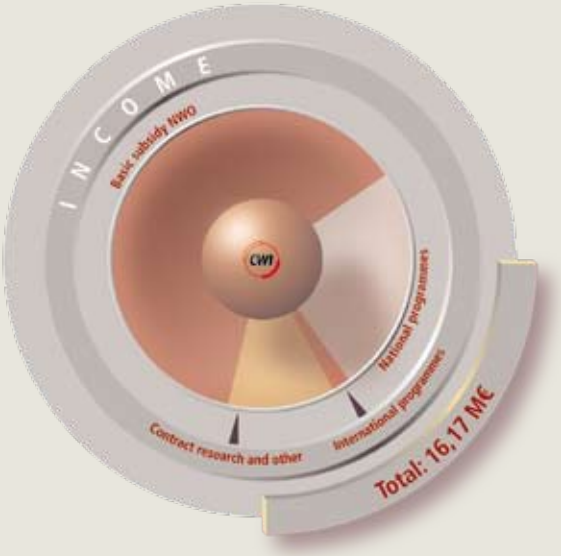
Projects, Finances and Control

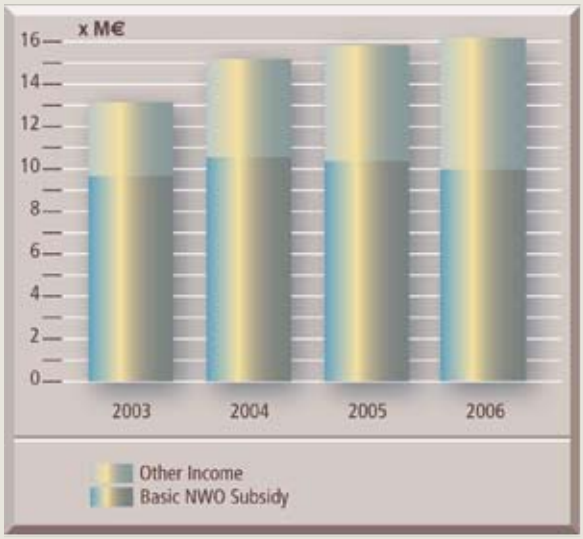
D.G.C. Broekhuis

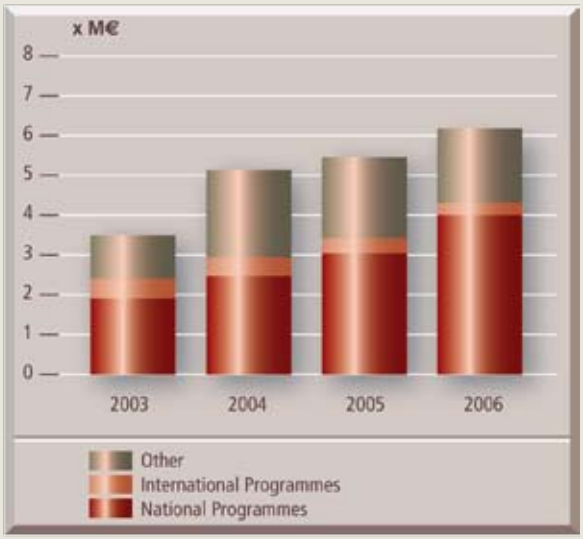
Personnel and Organization

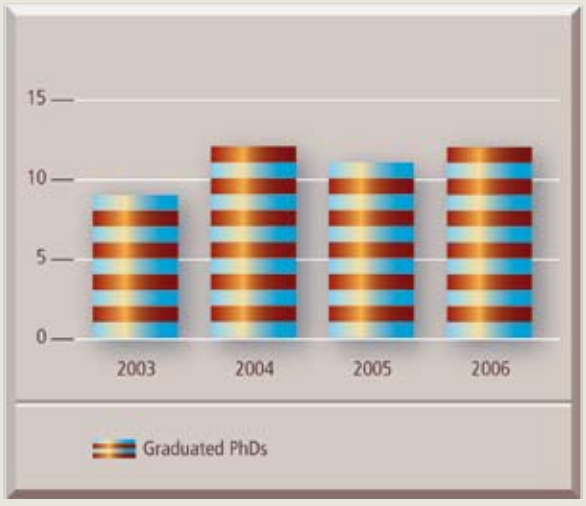
J. Koster

Facts and figures









CWI staff 2001-2006

Statistics of CWI output 2003-2006

	CWI				PNA				SEN				MAS				INS			
	2003	2004	2005	2006	2003	2004	2005	2006	2003	2004	2005	2006	2003	2004	2005	2006	2003	2004	2005	2006
Awards and grants	29	20	27	26	14	9	13	11	5	1	2	1	10	7	9	7	0	3	3	7
Refereed journals or proceedings	316	308	391	406	105	62	99	128	89	131	173	138	54	74	49	57	68	41	70	83
Other journals or proceedings	27	22	37	16	7	8	4	10	14	5	10	5	1	2	6	1	5	7	17	0
Monographs	6	5	5	1	2	2	3	1	0	3	2	0	1	0	0	0	3	1	0	0
Book chapters	10	14	10	16	3	9	5	2	3	2	3	8	0	1	0	1	4	2	2	5
PhD Theses	9	12	11	12	2	1	4	3	3	6	4	3	3	3	3	3	1	2	0	3
Professional products and other output	109	74	104	74	37	22	37	23	34	37	36	19	1	5	6	7	39	10	25	25
Total	506	455	585	551	170	113	165	178	148	185	230	174	70	92	73	76	120	66	117	123

CWI 2006 staff numbers

Male/female staff in FTE at the end of 2006 (CWI payroll)

	Research	Support
Male	130.15	31.8
Female	25.5	19.8

Master students in numbers

2003	2004	2005	2006
16	21	16	15

International staff in 2006 in FTE/year

Australia	2.0	Indonesia	1.0
Austria	1.0	Iran	2.0
Belgium	3.75	Israel	2.0
Bosnia-Herzegovina	1.0	Italy	3.0
Bulgaria	3.0	Moldavia	1.0
Cuba	1.0	Poland	4.0
China	6.0	Portugal	1.0
Czech Republic	2.0	Romania	2.0
Denmark	1.0	Russia	4.0
Finland	1.0	Serbia	1.0
France	5.8	Spain	5.5
Germany	13.8	Switzerland	1.0
Great Britain	5.8	Turkmenistan	1.0
Greece	4.0	Ukraine	0.7
Hungary	1.0	USA	4.5
India	3.0	Vietnam	1.0

Total non-Dutch in FTE 90 (58%)
Total CWI research staff in FTE 156

International staff at CWI in numbers 2003-2006

Year	# Persons	# Nationalities	# European nationalities
2003	76	25	16
2004	75	26	18
2005	69	26	18
2006	93	33	23

Research clusters and themes

Probability, Networks and Algorithms

Cluster leader: A.M.H. Gerards

Constraint and Integer Programming: Foundations and the applications of integer and constraint programming, including their cross-fertilization and links to game theory.
Algorithmic and Combinatorial Methods for Molecular Biology: The mathematical analysis of molecular structures in biology and the design, analysis and implementation of algorithms for computational molecular biology.

Algorithms, Combinatorics and Optimization

Theme leader:
M. Laurent

The design, analysis and implementation of optimization and approximation algorithms for combinatorial problems arising, in particular, from combinatorial optimization, game theory, molecular biology, mobile networks, production and transportation planning, scheduling, time-tabling. The methods come from mathematics (graph theory, discrete mathematics, topology, algebra, geometry), operations research (integer, linear, semidefinite and constraint programming), and computer science (complexity theory).
Combinatorics and Optimization: Investigation of combinatorial, geometric and algebraic methods in combinatorics and optimization.

Performance Analysis of Communication Networks

Theme leader: M.R.H. Mandjes (till 1 October)
R.D. van der Mei (as of 1 October)

Traffic Modelling, Analysis, and Performanec: Development of queueing-theoretic models and methods to study congestion phenomena in communication networks under new traffic paradigms. Focus is on the impact of heavy-tailed file size distributions and self-similar traffic patterns.
Wireless Networks: Development of analysis techniques for dimensioning, engineering, and operating wireless networks. Special attention is devoted to capacity gains from user mobility and opportunistic scheduling algorithms in wireless data transmission.
Service Differentiation: Investigation of fundamental research issues raised by quality of service differentiation in wired and wireless communications. A central role is played by the integration of streaming (voice, video) and elastic (file transfer, web browsing) services.
Performance of Distributed ICT Systems: Development and analysis of quantitative models for predicting and controlling the end-to-end quality of service in next-generation large-scale distributed ICT infrastructures, explicitly taking into account the combined impact of information systems and communication networks.

Stochastic Dynamics and Discrete Probability

Theme leader:
J. van den Berg

The mission of this theme is theoretical and applied research at the frontiers of modern probability, in particular on problems motivated by biology, (geo-) physics, finance and technology. The theme consists of two subthemes, Probability and Stochastic Analysis.

Probability: Research on stochastic systems with a large number of interacting components; these are motivated by a variety of biological and physical processes and by problems concerning wireless communication networks.

Stochastic Analysis: Fundamental and applied research, in particular spectral analysis of Gaussian processes and fields based on the theory of vibrating strings, with special interest to stochastic models in mathematical finance and queueing systems driven by scalar or spatial fractional Brownian motions.

Signals and Images

Theme leader:
E.J.E.M. Pauwels

Image Understanding, Retrieval and Indexing: Investigates mathematical methodologies to generate content-specific descriptions of images and video, for the purpose of robust indexing, understanding and retrieval from large databases.

Image Representation and Analysis: Deals with multi-resolution signal and image representations in general and methods in wavelet analysis and mathematical morphology in particular. Furthermore, it seeks to use such representations for problems in image analysis and coding. This group has recently branched out into biometrics.

Stochastic Geometry: Is concerned with the modelling and analysis of random geometric structures using techniques from spatial statistics and stochastic geometry.

Cryptology and Information Security

Theme leader:
R.J.F. Cramer

Mathematical cryptology: Problems reducible to standard (computational) mathematics, algebraic geometric/number theoretical secure computation and secret sharing, cryptanalysis (Number Field Sieve (NFS) for factoring RSA-moduli, algebraic cryptanalysis), algebraic complexity.

Highly composed security systems: Models, universal composability, simulatability, interaction with formal methods, theoretical cryptography.

Public-key cryptography: Chosen ciphertext security, signatures, identity-based encryption, dedicated secure multi-party protocols.

Quantum cryptography and information theory: Quantum oblivious transfer, privacy amplification, alternative (non-complexity-theoretic) security enablers (quantum bounded storage).

Computational Number Theory and Discrete tomography: Algorithmic number theory (NFS, computational issues concerning Riemann hypothesis), algorithmic reconstruction of objects from projections.

Software Engineering

Cluster leader: P. Klint

Interactive Software Development and Renovation

Theme leader:
P. Klint

Software Evolution: Development of methods, tools, and techniques that help to make and keep software systems sufficiently flexible.
Software Transformatio: Improvement of run-time efficiency (optimization), improvement of static structure (refactoring), and systematic modification (computer-aided maintenance) of software systems.
Generic Language Technology: Increased applicability and usability of our generic language technology as embodied in the ASF+SDF Meta-Environment is achieved by the steady introduction of new technologies like lexical matching and rewriting, generic pretty printing, information visualization and user-interface extensibility. The introduction of a relation calculator has created new perspectives on fact extraction from source code and on source code analysis.
Concept-Based Reasoning and Knowledge Engineering: Applied logic research covering a broad spectrum of aspects, like dynamic logic, tableau reasoning, construction of electronic textbooks for logic, and interactive information engineering.

Specification and Analysis of Embedded Systems

Theme leader:
J.C. van de Pol

This group studies modelling and validation techniques for computer controlled systems, which allow more efficient designs and constructions with fewer embedded faults. This is achieved by developing and implementing algorithms for the analysis and verification of distributed systems. The current focus is on symbolic model transformations, and on parallel algorithms for model checking.
The group applies new techniques for theorem proving, testing and (distributed) model checking with industrial partners to various case studies, for instance, communication protocols, embedded controllers, software architectures, safety-critical railway interlockings, and security protocols for e-commerce. The purpose is to establish the correctness of programmed systems 'beyond reasonable doubt'.

Coordination Languages

Theme leader:
J.J.M.M. Rutten

The activity in SEN3 ranges from mathematical models of behaviour and computation to experimental systems and demonstrator applications. SEN3 aims to provide the technology for coordination and dynamic composition of concurrent systems, based on solid mathematical foundations. Systems of special interest include long-lasting distributed applications, component-based systems, and service-oriented computing. Building such concurrent systems by composition of independent components and services involves coordination of their mutual interactions. Coordination, for instance, through connector circuits, is therefore one of the central subjects of the research in this group.

Computational Intelligence and Multi-agent Games

Theme leader:
J.A. La Poutré

The theme group works on the combination of two areas: computational intelligence techniques (like genetic and adaptive algorithms, neural networks, and graphical models) and games in multi-agent systems. Games represent the interactions between agents, like negotiations, auctions, social dilemmas, and market mechanisms. Computational intelligence techniques are investigated to build the adaptive strategies for agents participating in such games, as well as to simulate (economic) multi-agent systems governed by market mechanisms. The latter includes the design of these market mechanisms, in order to get the desired overall behaviour.
Furthermore, the group performs fundamental research on computational intelligence for optimization problems. Applications include e-business, transportation logistics, health care planning, distributed recommendation, and computational economics.

Distributed Multimedia Languages and Infrastructures

Theme leader:
D.C.A. Bulterman

The goal of this research group is to study methods for the specification, scheduling, and verification of complex distributed multimedia presentations. Our approach is to define composite presentations as distributed heterogeneous collections of objects that are bound to underlying devices and networks based on an abstracted homogeneous environment. The research studies desktop, consumer electronics and mobile delivery platforms and includes the development of system architectures, languages and user models. Experimental implementations of our work are distributed world-wide via our Ambulant Player software and via our extensive participation in the W3C.

Modelling, Analysis and Simulation

Cluster leader: J.G. Verwer

Nonlinear PDEs: Analysis and Scientific Computing

Theme leader:
A. Doelman

Scientific Computing in the Life Sciences: Mathematical modelling, mathematical and numerical analysis, and numerical simulation for life sciences, in particular biology and medicine. Cooperation has been established with researchers working in cell, neuro, and microbiology.
Nonlinear Dynamics of Natural Systems: Mathematical analysis of finite and infinite dynamical systems in interaction with the earth and life sciences. This research is embedded in the national mathematics cluster Nonlinear Dynamics of Natural Systems (NDNS).
Geometric Integration of Wave Phenomena: Numerical analysis and simulation of partial differential equations, in particular structure-preserving numerical methods with applications to conservative continua like geophysical fluids.
Asymptotics and Special Functions: Research on uniform asymptotic expansions and numerical and algebraic algorithms for special functions.

Computing and Control

Theme leader:
B. Koren

Computational Fluid Dynamics and Computational Electromagnetics: Current research focuses on efficient solution methods for turbulent, steady two-fluid Navier-Stokes flows, immersed boundary methods for Navier-Stokes flows around complex geometries, shape-optimization methods for electromechanical devices, stochastic methods for electromagnetic field computations, and parallelization of software for fluid-structure interaction.
Control and System Theory: Research on problems of control and system theory for various dynamic systems motivated by control problems of engineering and by cell biology. Current research is directed at control of hybrid systems, realization theory for subclasses of hybrid systems, supervisory control of decentralized and modular discrete-event systems, and computational properties of nonlinear systems.

Nonlinear Dynamics and Complex Systems

Theme leader:
U. Ebert

This theme focuses on nonlinear dynamics and model reduction, presently mainly applied to spark formation in technology and geophysics - a challenging problem on multiple scales. On the level of partial differential equations, the group concentrates on numerical questions of operator splitting, monotonicity preservation and adaptive grid refinement. The group further focuses on analytical front dynamics, reduction to free boundary problems and solutions with conformal mapping methods.
Model reduction on a different level takes place when partial dif-

ferential equations are coupled to stochastic models in so-called hybrid models. The theme leader holds a part-time professorship in physics in Eindhoven where she plans and interprets spark experiments in the range of her theoretical research.

Information Systems

Cluster leader: M.L. Kersten

Standardization and Knowledge Transfer

Theme leader: M.L. Kersten

Knowledge transfer on evolving standards, primarily within the context of the World Wide Web Consortium (W3C). This includes general management of all W3C offices worldwide, leadership of the W3C HTML Working Group, co-leadership on the W3C XForms activities, and participation in the work of the Document Format domain of W3C.

Database Architectures and Information Access

Theme leader: M.L. Kersten

Multimedia Databases: Development of an efficient storage and retrieval system of multimedia data. The research line on multimedia information retrieval aims at developing a multimedia database system, which can offer a high level of abstraction to both developers of end-user applications and researchers working on content analysis techniques.
Database Architectures: Development of the next generation database technology to support Ambient Intelligence applications. Ambient Intelligence refers to digital environments in which multimedia services are sensitive to people's needs, personalized to their requirements, anticipatory of their behaviour and responsive to their presence.
Query Languages & Optimization: Development of a multi-layer query optimizer infrastructure to support multimedia information access. At the core of such a system we envision a sound and flexible probabilistic model to steer the retrieval process, integrated with query optimizers and kernel functionality.
MonetDB Dissemination: Promoting the development and use of the database experimentation platform MonetDB. MonetDB is an open source high-performance database system developed at

CWI, designed to provide high performance on complex queries against large databases, e.g., combining tables with hundreds of columns and multi-million rows.

Semantic Media Interfaces

Theme leader:
L. Hardman

Investigation of the boundaries between multimedia and the Semantic Web and development of models and tools for automatic generation of high-quality hypermedia presentations. This includes the modelling of argument structures for the generation of meaningful video sequences, domain-independent structuring of a semantically annotated media repository for presentation to end-users, dependencies of the user and domain models in the generation process, characteristics of media types for presenting information to the user, and to what extent presentation knowledge can be included in the generation process.

Visualization and 3D Interfaces

Theme leader:
R. van Liere

Data Visualization: Projects in the application area of the Dutch Living Cell initiative. Key research focus is the interactive visualization of time dependent data sets and the exploration of multidimensional information spaces. Furthermore, the problems of classification and visualization of multidimensional parameter spaces are addressed.
3D User Interfaces: Projects concerned with applying virtual reality technology to cost effective and ergonomic desktop virtual environments. Two-handed interaction with tangible devices is the main research focus. This research is combined with the engineering of prototype desktop solutions together with several affiliated research groups.

Quantum Computing and Advanced Systems Research

Theme leader:
H.M. Buhrman

Quantum Computing: Research on quantum information and communication technology and processing, quantum algorithms, quantum communication complexity, quantum complexity classes, quantum cryptography, quantum information theory, and applications of quantum information theory to classical computing and physics.
MDL Learning and Algorithmic Statistics: Information theoretic methods for learning from data, Minimum Description Length (MDL), maximum entropy, pattern recognition, learning when all models are wrong, practical individual rate distortion theory, and applications and refinement of parameter free clustering and classification
Advanced Algorithms, Systems and Genomics: Kolmogorov complexity, computational complexity, distributed computing, and bio-informatics. In particular: new non relativizing separations in line with P vs NP problem, time limited Kolmogorov complexity, universal distributions, characterization of random strings, and symmetry of information. General lower bound techniques. Design and analysis of algorithms for distributed and parallel systems.

Research programmes

International and national research programmes

CWI participates in many national and international research projects.
This overview lists all major projects with their duration, partners, and CWI project leader(s).

European programmes

European Union

RESQ: Resources for Quantum Computing
2003-2006
Univ. Libre de Bruxelles, Univ. Paris-Sud, Univ. of Bristol, Max-Planck Gesellschaft zur Forderung der Wissenschaften, UU, SZTAKI, Univ. de Genève, Univ. of Cambridge, Univ. of Gdansk
H.M. Buhrman

QAP: Qubit Applications
2005-2009
36 Partners from different countries
H.M. Buhrman

SPICE – Service Platform for Innovative Communication Environment
2006-2008
Telematica Instituut, France Télécom
D.C.A. Bulterman

CREDO – Modelling and Analysis of Evolutionary Structures for Distributed Services
2006-2009
Univ. Oslo, Christian-Albrechts-Univ. Kiel, Rheinische Friedrich-Wilhelmus Univ. Bonn, Uppsala Univ., United Nations Univ. (International Inst. for Software Technology), Almende, Rikshospitalet - Radiumhospitalet HF, Norsk Regnesentral
F.S. de Boer

EU networks

ADONET: Algorithmic Optimization Discretization
2004-2007
Various partners: CWI is coordinator of the Dutch Consortium
M. Laurent

EuroNGI: Design and Engineering of the Next Generation Internet - Towards Convergent Multi-service Networks
2003-2006
58 partners from different countries
M.R.H. Mandjes

BIOSECURE: Biometric for Secure Authentication
2004-2007
48 partners from different countries
B.A.M. Schouten

MUSCLE: Multimedia Understanding through Semantics, Computation and Learning
2004-2008
38 partners from different countries
E.J.E.M. Pauwels (scientific coordinator)

DELOS: Digital Libraries
2004-2008
60 partners from different countries
M.L. Kersten

PASCAL: Pattern Analysis, Statistical Modelling and Computational Learning
2003-2007
Univ. London, and 50 more sites
P.D. Grünwald

EuroFGI – Design and Engineering of the Future Generation Internet – Towards Convergent Multi-service Networks
2006-2008
Many
R. Núñez Queija

K-Space – Knowledge Space of Semantic Inference for Automatic Annotation and Retrieval of Multimedia Content
2006-2008
14 partners
L. Hardman

National programmes

NWO

SPCO: Semidefinite Programming and Combinatorial Optimization
2002-2007
LAAS-CNRS, Univ. Klagenfurt, Univ. Rennes, TUD
M. Laurent

DIAMANT – Discrete, Interactive & Algorithmic Mathematics, Algebra and Number Theory
2006-2010
TUE, UL, RU
A.M.H. Gerards

CIP: Constraint and Integer Programming Techniques
2002-2007
ERCIM, Univ. Victoria (Canada), Univ. Singapore, Brooklyn College
K.R. Apt

FDP: Foundations of Declarative Programming
2002-2007
UvA, VU
K.R. Apt

DIACoDeM – Distributed Implementations of Adaptive Collective Decision Making
2006-2008
SEN3, SEN4
K.R. Apt

RAPS: Rare-event Analysis of Processor-sharing Systems
2004-2007
Lucent Technologies, TUE
S.C. Borst

Efficient Flow-scheduling in Resource-sharing Networks with Variable Service Rates
2005-2009
-
R. Núñez Queija

Coordination With Perfomance Guarantees
2005-2009
-
R.D. van der Mei

CooPer – Coordination with Performance Guarantees
2006-2010
SEN3, PNA2 project
F. Arbab, R.D. van der Mei

QNOISE – Queueing Networks
2006-2007
TUE, UT
R.D. van der Mei

Critical Percolation and Excitable Media
2005-2007
-
J. van den Berg

AGP: Spectral Analysis of Processes with Stationary Increments
2003-2007
VU
K.O. Dzhaparidze

Quantum Cryptography: Achieving Provable Security by Bounding the Attacker's Quantum Memory
2006-2009
-
S. Fehr

Mathematical Aspects of Discrete Tomography
2002-2006
UL, FEI Eindhoven, Lawrence Berkeley National Laboratory
H.J.J. te Riele

Algorithmic Validation of Widely Used Cryptosystems
2004-2007
Microsoft, TUE, UL
H.J.J. te Riele

Deliver: Intelligent Software Management and Delivery
2003-2006
Exact BV, Planon BV, ChipSoft BV, VU
P. Klint

LPPR: Language-Parametric Program Restructuring
2004-2006
VU
J. Heering

Hefboom-project
2005-2009
Hogeschool Amsterdam, VU, UvA
J.J. Vinju

TIPSY: Tools and Techniques for Integrating Performance Analysis and System Verification
2004-2007
TUE
W.J. Fokkink

Account: Accountability in Electronic Commerce Protocols
2004-2007
VU, UT
W.J. Fokkink

MoveBP – Modelling and Verification of Business Processes
2005-2007
TUE
W.J. Fokkink

VeriGEM – Verification Grid for Enchanced Model Checking
2005-2008
TUE, UT
J.C. van de Pol

VEMPS – Verification and Epistemics of Multi-party Protocol Security
2006-2010
TUE, VU, UL, UU
D.J.N. van Eijck

MOBI-J: Assertional Methods for Mobile Asynchronous Channels in Java
2001-2007
UL, Christian-Albrechts-Univ. Kiel
F.S. de Boer

CoCoMAS – Coordination and Composition in Multi-agent Systems
2006-2010
UU
F.S. de Boer

C-Quattro: Compositional Construction of Component Connectors
2004-2008
VU
F. Arbab, J.J.M.M. Rutten

Infinity – Infinite Objects, Computation, Modelling and Reasoning
2006-2009
VU
J.J.M.M. Rutten

SYANCO – Synthesis and Analysis of Component Connectors
2006-2008
Rheinische Friedrich Univ. Bonn, UL
F. Arbab

MIA: Medical Information Agent
2004-2008
AMC, UM, TUE
J.A. La Poutré

NA – Task Coordination for Non-cooperative Agents
2006-2010
TUD
J.A. la Poutré

ScaNN: Scalable Reinforcement Learning in Asychronous Spiking Neural Networks
2003-2007
Veni project
S.M. Bohte

Three-dimensional Simulation of Phytoplankton Dynamics
2001-2006
UvA
B.P. Sommeijer

DEBpump – Understanding the 'Organic Carbon Pump' in Meso-scale Ocean Flows
2005-2008
IMA, UU, VU
B.P. Sommeijer

Mesoscale Simulation Paradigms in the Silicon Cell
2004-2008
UvA
J.G. Blom

3D-RegNet: Simulation of Developmental Regulatory Networks
2004-2008
UvA
J.G. Blom

Mathematics and Computation for the System Biology of Cells
2004-2008
UvA, TUE, VU, MAS2 (Van Schuppen)
J.G. Blom

Modelling of Developmental Regulatory Networks
2004-2008
UvA
J.G. Blom

CellMath: Mathematics and Computation for the System Biology of Cells
2004-2008
VU, UvA, TUE, MAS2 (van Schuppen)
J.G. Blom

Symplectic Integration of Atmospheric Dynamics: Long-term Statistical Accuracy for Ensemble Climate Simulations
2005-2009
-
J.E. Frank

Interactions of Pulses and Fronts
2005-2009
-
A. Doelman

NDNS: Nonlinear Dynamics of Natural Systems
2005-2009
-
A. Doelman

Robust: Numerical Methods and Computational Technologies for Singularly Perturbed Multiscale Problems
2004-2006
TUE, MSU Moscow, RAS UB
P.W. Hemker

RPOS: Realization and Control of National Positive Systems
2005-2009
-
J.H. van Schuppen

Computational Topology for Systems and Control
2005-2010
Vidi project
P.J. Collins

NUMLED: Numerical Methods for Leading Edge Dominated Dynamics
2002-2006
-
W. Hundsdorfer

MRPDE: Multirate Time Stepping for PDEs
2004-2007
-
W. Hundsdorfer

MBA – Moving Ionization Boundaries and Charge Transport
2005-2008
NWO/FOM (Dynamics of Patterns)
U. Ebert

Pinwheel – Cracking a Scientific Database
2006-2008
UU, OMEGACEN/RUG
M.L. Kersten

CIRQUID: Complex Information Retrieval Queries in a DBMS
2003-2007
UT
A.P. de Vries

Quantitative Design of Spatial Interaction Techniques for Desktop Mixed-Reality Environments
2005-2009
TUE
R. van Liere

Quantum Computing
2004-2006
-
P.M.B. Vitányi

ACAA: Average-Case Analysis of Algorithms
2002-2006
Univ. Waterloo, BSI
P.M.B. Vitányi

Quantum Information Processing
2004-2009
Vici project
H.M. Buhrman

Learning When All Models Are Wrong
2005-2010
Vidi project
P.D. Grunwald

N/A – The Skeptical Minimum Description Length Principle
2006-2009
EURANDOM
P.D. Grunwald

Quantum Computing: Algorithms, Proofs and Tradeoffs
2005-2008
Veni project
R.M. de Wolf

STW

PHOTO-ID: Photo-ID for Cetaceans Using Shape Matching Methods
2004-2007
CML Leiden, Netherlands National Herbarium, UU
E.J.E.M. Pauwels, E.B. Ranguelova

SEQ: Sequential Point Processes
2004-2006
Centrum voor Milieukunde Leiden, FOM-AMOLF, ITC, Kapteyn Instituut, Philips Research
M.N.M. van Lieshout

Practical Approaches to Secure Computation
2005-2008
TUE, Philips Research Lab.
R.J.F. Cramer

Electric 'Fracture': Growth and Branching of Ionised Channels
2005-2007
TUE
U. Ebert

SenterNovem (including IOP)

BASIS: Biometric Authentication Supporting Invisible Security
2004-2009
UT, TUE
B.A.M. Schouten

IDEALS: Idiom Design for Embedded Applications on a Large Scale
2003-2006
ASML, TUE, UT, ESI
A. van Deursen

TT-Medal: Testing Methodologies with Advanced Languages
2004-2006.
LogicaCMG, ProRail, Improve QS, Fokus, DaimlerChrysler, Nokia, VTT, Conformiq, Nethawk
J.C. van de Pol

CIM III: Cybernetic Incident Management
2003-2006
SEN4, TUD, VU, Almende, CMotions, Falck
F. Arbab, J.A. La Poutré

DEAL: Distributed Engine for Advanced Logistics
2002-2007
Almende, ERBS, VU, Groeneveld Groep, Post-Kogeko Transport Groep, Vos Logistics
J.A. La Poutré

Calce: Computer-aided Life Cycle Enabling
2003-2006
PinkRoccade Public BV, Software Improvement Group, VU
J. Heering

IOP-EMVT: Space-mapping and Related Techniques for Inverse Problems in Magnetic Shape Design, with Application to an Electromagnetic Actuator
2003-2007
TUE
P.W. Hemker

IOP-EMVT: Stochastic Methods for Field Computations in EMC Problems
2004-2007
TUE
P.W. Hemker

Passepartout
2005-2007
Stoneroos, V2, INS2 en SEN5
D.C.A. Bulterman, L. Hardman

Trust4 ALL
2005-2007
Oce, RUL
F. Arbab

Near Field Virtual Reality Technologies
2005-2006
Gallium Europe, VOF
R. van Liere

Bsik projects

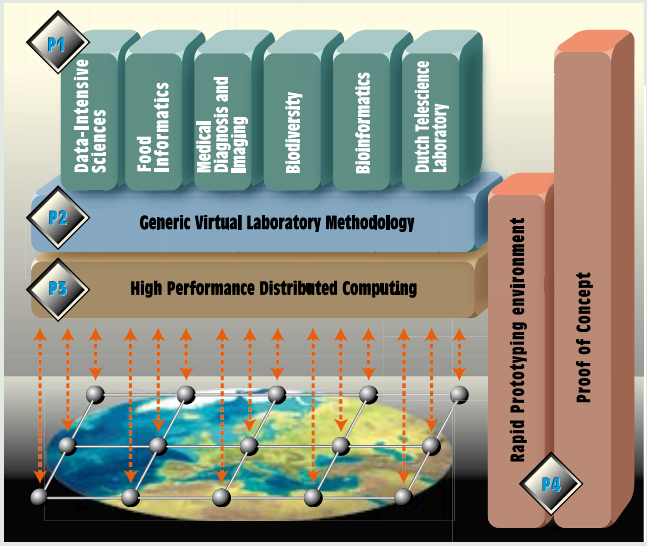
BRICKS: Basic Research in Informatics for Creating the Knowledge Society
2004-2009
TUD, TUE, UT, UU, NWO
J.K. Lenstra, J.G. Verwer, J.R. van Ossenbruggen

MultimediaN: Multimedia Next Generation
2004-2008
CTIT, LogicaCMG, Philips Research, TI, TNO, TUD, UU, UvA, VU, V2_, Waag Society
M.L. Kersten

VL-e: Virtual Laboratory for e-Science
2004-2009
see www.vl-e.nl about VL-e consortium partners
R. van Liere

GeoInfoNed – A Multimedia Geo-database Infrastructure
2006-2008
OTB/TUD/Section GIS Technology
M.L. Kersten

BioRange – Biomathematics in Mass Spectrometry Based Proteomics and Modelling of Protein Networks
2006-2009
EUR/Dept. of Cell Biology
J.H. van Schuppen



VL-e

Contract research

Stagesporen
1995-indefinite
VU, UM, UL
A.M.H. Gerards

Railway Optimization
1994-indefinite
NS Reizigers
A.M.H. Gerards

FLORIN: Flow-level Performance of Integrated 3G CDMA Networks
2003-2006
France Télécom
M.R.H. Mandjes

Telematica Instituut projects

CHIP: Cultural Heritage Information Personalization
2005-2008
TUE, Rijksmuseum
L. Rutledge

Miscellaneous

Spinoza Award project
2005-2010
A. Schrijver

Parallel Implementation of a Coupling Interface for Fluidstructure Interaction
2005-2006
NCF Grant
B. Koren

Molecular Systems Biology at Science Park Amsterdam
2005-2009
MAS2, AMOLF, SILS
J.H. van Schuppen

STREAMERS-Moscow: Streamer Discharges: Experiments, Theory, Applications
2004-2007
NWO-RFBR Programme (Russisch Nederlandse Samenwerking)
TUE, MIPT (Moscow), IVTAN (Moscow)
U. Ebert

Modelling and Inferring Developmental Regulatory Networks
2005-2008
NWO-RFBR Programme (Russisch-Nederlandse Samenwerking)
UvA-section Computational Science, The Ioffe Institute of the Russian Academy of Sciences
J.G. Blom

Appendices

Colophon

Published by: Stichting Centrum voor Wiskunde en Informatica, 2007
Production: Communication & Information Department (C&I), CWI
Text and editing: Bram Vermeer, Annette Kik and Lieke Schultze
Design, artwork & illustrations: Tobias Baanders
Photographs CWI: Wim Klerkx, Tobias Baanders and Jan Schipper
Picture in cover illustration: Wim Klerkx
Printing: Grafisch Bedrijf Ponsen & Looijen bv, Wageningen