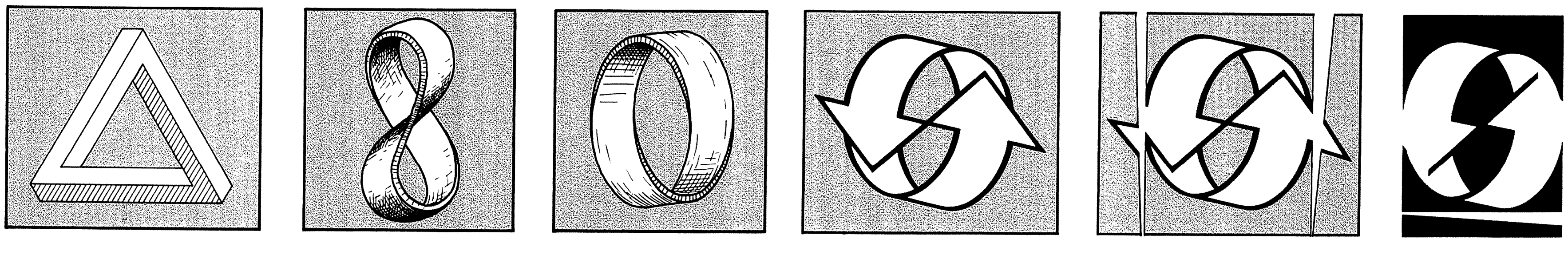
ANNUAL REPORT

19 88

Centrum voor Wiskunde en Informatica

Centre for Mathematics and Computer Science



ANNUAL REPORT 1988

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

Kruislaan 413 1098 SJ Amsterdam
P.O.Box 4079 1009 AB Amsterdam the Netherlands

The Stichting Mathematisch Centrum was founded on February 11 1946, as a non-profit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands organization for scientific research (NWO).

Board of Directors

P.C. Baayen (scientific director)
J. Nuis (management director)

Centrum voor Wiskunde en Informatica
(Centre for Mathematics and Computer Science) CWI

Kruislaan 413 1098 SJ Amsterdam The Netherlands	P.O. Box 4079 1009 AB Amsterdam The Netherlands
Telephone (from abroad)	020-592 9333 31 - 20 592 9333
Telefax (from abroad)	020-5924199 31 - 20 5924199

Contents

Introduction

Funding and continuity

For CWI, 1988 was dominated by the same major factors as the previous year: the closing of the Information Technology Promotion Plan (INSP) at end 1988, and the continuation of research started under its auspices; the balance between mathematical and computer science research, and between strategic and fundamental research. In April, matters were tested against international opinion: in that month NWO (The Netherlands Organization for Scientific Research) asked a committee chaired by R.P. van de Riet (Free University, Amsterdam) to evaluate CWI for possible action required in the post-INSP period; membership comprised A. Bensoussan (INRIA, Paris), N.G. de Bruijn (Technical University, Eindhoven), J.M. Goethals (Philips MBLE, Brussels), A.N. Habermann (Carnegie-Mellon, Pittsburgh), and R. Milner (University of Edinburgh).

Despite the committee's highly positive findings NWO has only converted a small proportion of INSP funding (Dfl. 2 million per annum) into a permanent grant, the remainder coming in the form of a temporary grant - and that not for the full amount.

In September, CWI itself aired matters nationally at the *Workshop on Strategic Research in Computer Science and Mathematics,* whose sixty participants came from industry, government, major technical institutes and universities.

CWI has now put its case to both national and international opinion. The conclusions have reinforced our conviction that CWI is on the right road, and that it must continue along that road.

Internationalization

Internationalization is a frequently heard theme in discussions on the future of CWI. In 1988 this took the form of closer cooperation with the West German Gesellschaft für Mathematik und Datenverarbeitung (GMD) and the Institut National de Recherche en Informatique et en Automatique (INRIA), of France. In spring agreement was reached to upgrade existing research contacts in a series of workshops. A preliminary meeting at CWI in July was followed by the first workshop in November 1988; this was also held at CWI and proved a great success. Other activities planned include the preparation of a policy document on joint research projects, and the publication of a GMD-INRIA-CWI Newsletter. The ongoing increase in the number of visitors from abroad also underlined the increasingly international character of CWI activities.

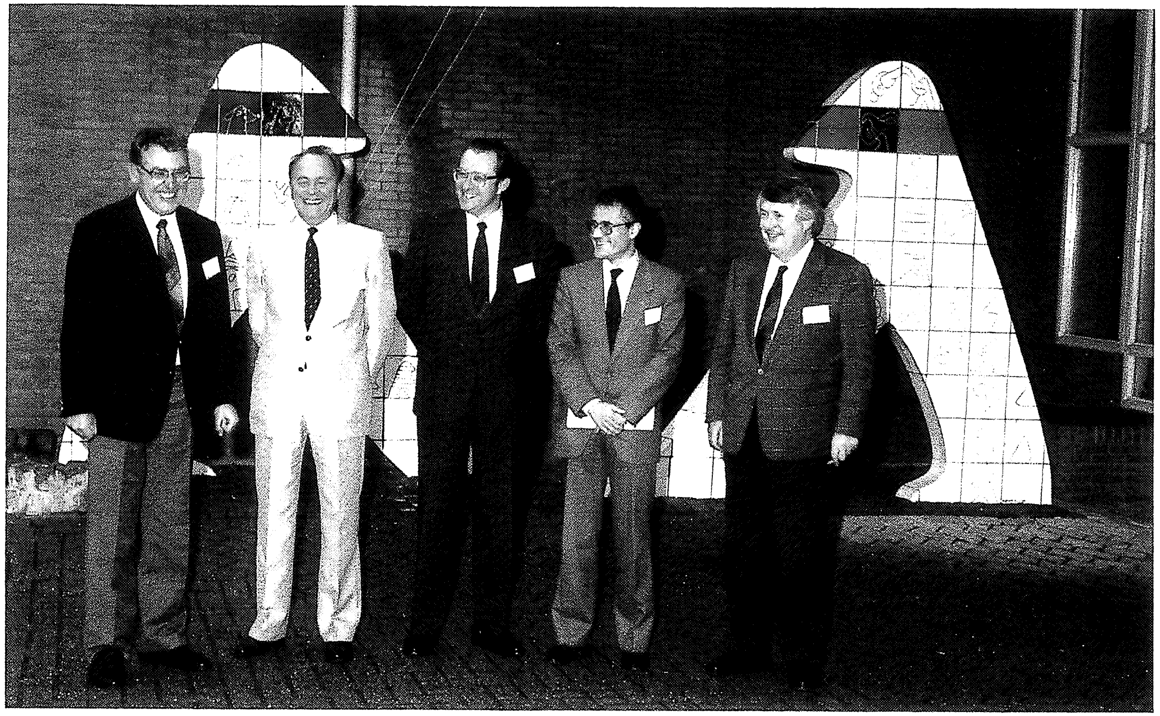
Official visits, new agreements

Government interest in CWI was demonstrated by a working visit in October by Mr. W.J. Deetman, Minister for Education and Science. During the minister's visit the computer company DEC and the Stichting Mathematisch Centrum (SMC) signed an agreement whereby DEC makes available equipment for CWI research into distributed systems (in particular the Amoeba-project). A declaration of intent was also signed by SMC and SURF foundation (a national computer service organization for higher education and research). SMC and SURF aim for integration and expansion of network services for users of EUnet (CWI is USEnet gateway) and SURFnet, the Dutch academic network.

Shortly after this, the newly formed board of NWO - our chief source of funding - visited CWI as part of an orientation programme taking in all NWO-related foundations and institutes.

Reorganization

There were also developments within CWI. Some scientific departments were restructured as of 1st September: Pure Mathematics and Applied Mathematics were amalgamated to form a single department, Analysis, Algebra & Geometry. The same happened to Mathematical Statistics and Operations Research & System Theory which combined to become Operations Research, Statistics, & System Theory. On the same date, R.D. Gill, head of Mathematical Statistics, was appointed Professor of Stochastics at Utrecht University. Some months later, H.A. Lauwerier, head of the former Applied Mathematics Department, retired. Two more senior members of staff also left CWI during 1988: Assistant Director, F.J.M. Barning, retired in February and J.C.P. Bus, head of Management & Presentation, took up a position with the European Community in Brussels.



The first explicit manifestation of closer cooperation between the national research institutions GMD (West Germany), INRIA (France) and CWI (The Netherlands) came in November, with a joint workshop at CWI. Over 100 researchers discussed specific topics of common interest. Directors of the three institutions dealt with more general matters including a common research policy. From left to right: G. Goos (GMD), G. Seegmüller (GMD), P.C. Baayen (CWI), A. Bensoussan (INRIA) and F. Winkelhage (GMD).

Computer Systems & Telematics was originally tasked with supporting operating systems and networks. The appointment of a departmental head in 1988 marked expansion to a full research-oriented component of CWI's computer science departments.
Finally, the lack of space at the institute, due to ongoing increases in personnel and extra computer equipment, became acute. With realization of new construction - planned years back - nowhere in sight, a temporary solution was required; and the Analysis, Algebra & Geometry department moved into Portakabins towards the end of the year.

Projects
No new projects as such started up in 1988. However, some ongoing activities received new impetus. The *Stichting Computer Algebra Nederland* (Dutch Computer Algebra Foundation) started up in June. Its aim is to offer centralized national facilities and services to researchers and users of computer algebra, who are found in various scientific disciplines. CWI will play an important role here. Activities in the field of cryptography were also expanded via CWI's task as prime contractor in the *RIPE* project (RACE Integrity Primitives Evaluation); RIPE is part of the European Community's RACE programme (R&D in Advanced Communications-technologies in Europe). Increasing emphasis on research into *term rewriting systems* (TRS) will promote this to the status of a separate project in 1989.
Once again CWI produced results in the field of factorizing very large numbers. After regaining the world record in April (using the National Aerospace Laboratory's NEC SX/2 supercomputer), CWI was one of the partners in factorizing a 100-digit number using the combined capacities of 400 minicomputers scattered worldwide. Major support from the EC's ESPRIT I programme for the Software

Technology department will end in 1989. With this in mind the department made preparation of proposals for the two new programmes, *ESPRIT II* and *ESPRIT Basic Research Actions* a priority.

Publications

As usual a complete list of publications is given at the end of this annual report. Several deserve special mention. The CWI Monograph Series produced No.7: *Queueing Theory and its Applications,* a tribute for the 65th birthday of J.W. Cohen - an advisor to CWI. No.7 was edited by O.J. Boxma (CWI) and R. Syski (Maryland). The second part of Reidel's English translation of the *Russian Encyclopaedia of Mathematics* also appeared during 1988. Academic Services published P.J.F. Lucas and L.C. van der Gaag's *Introduction to Expert Systems*; Addison-Wesley is due to produce an English translation of this Dutch original. Lastly, A.M. Cohen edited, together with M. Aschbacher and W.M. Kantor, *Geometries and Groups* (Reidel).

The start of 1988 also brought a change of name for the CWI Newsletter. As the new title makes clear, the *CWI Quarterly* appears four times a year; its core consists of high quality scientific articles aimed at a broad range of mathematicians and computer scientists; readership is worldwide. The new title does the publication better justice.

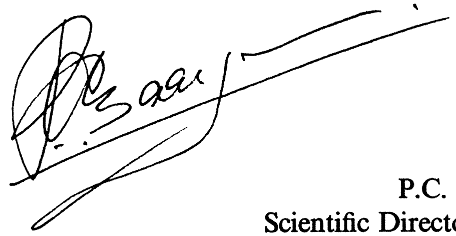
Conferences, courses

During 1988 CWI organized several conferences, workshops and courses, some as joint efforts. S.J. Mullender accepted an invitation to contribute to *Arctic '88: an advanced course on distributed systems,* in Tromsø, Norway. As in the past, CWI arranged a number of post-graduate courses; subjects in 1988 were *Artificial Intelligence* and *Networks.* In February there was also a course on *ABC* (a simple, structured, user-friendly programming language developed by CWI). In March this was followed by a course on the programming language C^{++}. The *IIICAD* workshop held in Veldhoven in April 1988, attracted 40 participants - 25 from abroad. This turn-out was left far behind by the 180 participants in the extraordinarily successful workshop devoted to *REX* (Research and Education in Concurrent Systems), organized by CWI in Noordwijkerhout in May-June. In autumn, an average of 25 participants from across the country were involved in a series of six colloquia on *Image Reconstruction,* with speakers from home and abroad. The CWI vacation course for school teachers, an unbroken annual tradition going back to foundation of the Mathematical Centre - as CWI was originally known - in 1946, took place as usual. This year's subject was *Difference and differential equations.*

In October, CWI organized a symposium as part of its knowledge transfer activities: *Planning and Control in Traffic* attracted sixty participants from industry, government and universities. Lastly, in November, CWI was joint organizer of the annual SION congress which took as its theme *Computer Science in The Netherlands.*

This Annual Report has the same format as its predecessor. There are six scientific department reports, following the reorganization carried out during 1988; but detailed project reports are given according to the old departmental subdivision. Computer Systems & Telematics now reports as a scientific department. The other support departments are covered separately. In the Foreign Visitors and List of Publications chapters the old departmental subdivision is maintained.

Presenting the CWI Annual Report requires a judicious balance of the practical and purely scientific. As with all our activities, this is a team effort. We aim to present our wide-ranging readership with an informative and readable account of our activities; hopefully we have succeeded in doing so, once again, in 1988.



P.C. Baayen
Scientific Director CWI

Organization

The Centre for Mathematics and Computer Science (CWI) is the research institute of the Stichting Mathematisch Centrum (SMC), which was founded on 11th February 1946. SMC falls under The Netherlands organization for scientific research (NWO), the main source of funding.
In line with its statutory purpose 'to foster the systematic pursuit of pure and applied mathematics in The Netherlands', SMC immediately set up an institute for fundamental research, the Mathematical Centre. From the outset this institute played an important role in the development of computer science in The Netherlands. A change to the present name, CWI, in September 1983, reflected the major expansion of research in this field. On the national level this growth led to the setting-up in 1982 of the Stichting Informatica Onderzoek in Nederland (SION), an independent NWO research organization for computer science. Its formal connection with SMC is embodied in a Permanent Consultation Commission.

SMC also finances research projects at Dutch universities. These projects are organized in eight national working parties in the following fields:

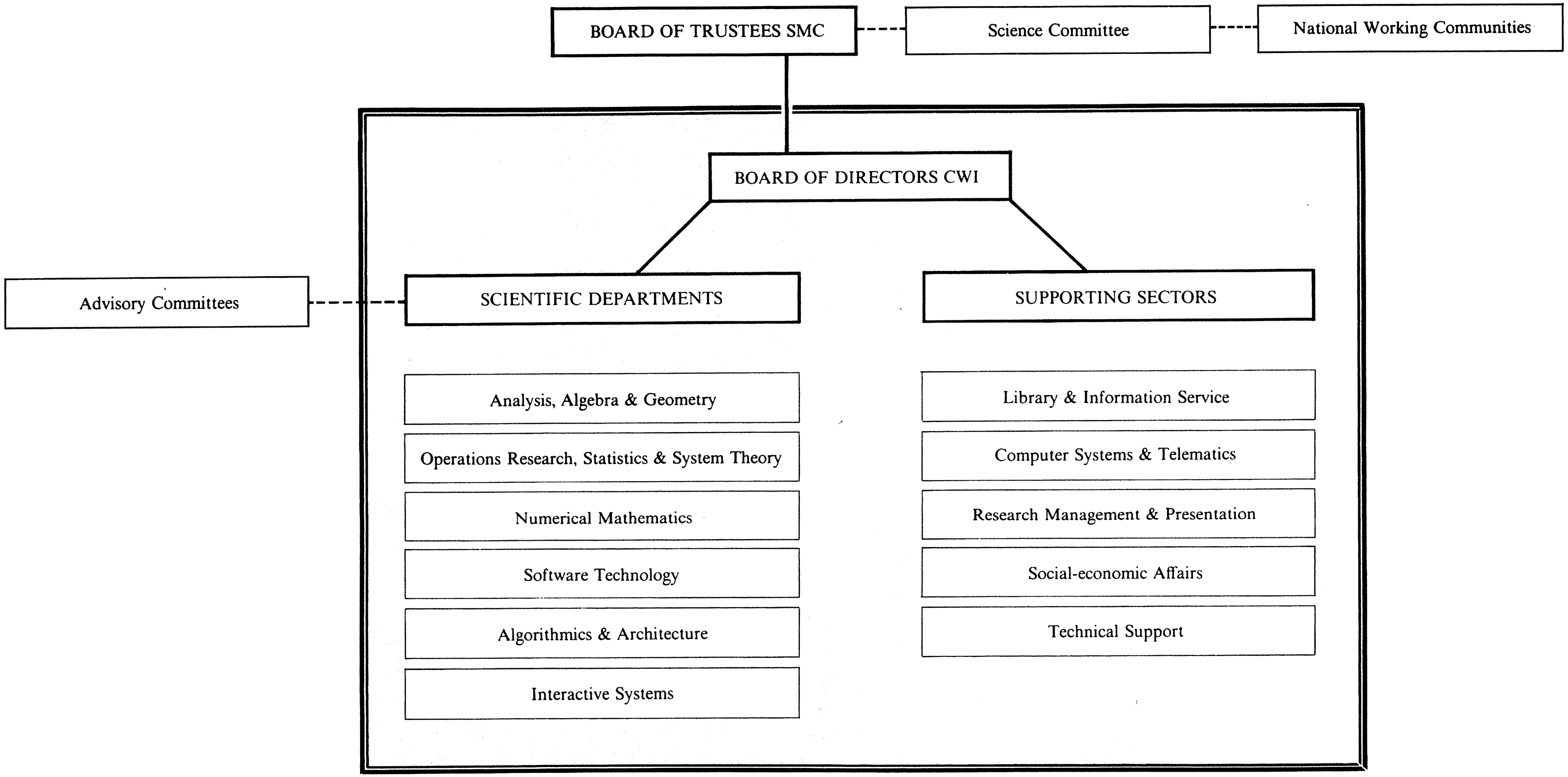
- Numerical mathematics;
- Stochastics;
- Discrete mathematics;
- Operations research and system theory;
- Analysis;
- Algebra and geometry;
- Logic and foundations of mathematics;
- Mathematical physics.

SMC is administered by a Board of Trustees. Actual administration is delegated to the Board of Directors of SMC, which is also responsible for CWI. A Science Committee advises the Board of Trustees on matters of research policy and organization involving both the National Working Parties and CWI. The Science Committee is made up of researchers from universities and CWI. A number of Advisory Committees make recommendations to CWI scientific departments on implementing research plans.
Research at CWI is also evaluated by international visiting committees. The first evaluation, in 1987, covered statistics, stochastics and system theory. The next, due in 1989, will deal with algebra, analysis, geometry, optimization and numerical mathematics.

CWI's goal is fundamental and advanced research into mathematics and computer science, with special emphasis on areas to which the research may have relevant applications. Research is fundamental in that it mainly concerns those problems lacking standard methods of solution. It is advanced, in that CWI aims at a high level, both nationally and internationally. Preference is given to subjects with internationally relevant development potential.

During 1988, CWI reorganized some of its scientific departments, reducing their number from eight to six. The departmental structure is less rigid than it appears, given considerable inter-departmental collaboration. This is a matter of deliberate policy, not only in the selection of research topics, but also in the selection of the permanent scientific staff. There are also a number of supporting service departments. The organization structure of SMC and CWI is shown on the opposite page. In this scheme, the department of Computer Systems & Telematics comes under supporting sectors. However, because of the increasing emphasis on research, its activities are represented as those of a scientific department.

By international standards CWI might appear relatively small and incapable of involvement in the full range of major developments in mathematics and computer science. However, size can be deceptive. By its very nature CWI, with its close knit research units supported by state-of-the-art computer facilities and a well stocked library, is ideally equipped to handle the dynamic and interdisciplinary demands of present day research.



Organizational chart: the Stichting Mathematisch Centrum SMC and its research institute, the Centrum voor Wiskunde en Informatica (Centre for Mathematics and Computer Science) CWI.

Department of Analysis, Algebra & Geometry

M. Hazewinkel (head of department)

G. Alberts	P. Hofstee	J.B.T.M. Roerdink
J.T.M. van Bon	H. Inaba	H.N.M. Roozen
A.E. Brouwer	Jin Cheng-fu	S.N.M. Ruijsenaars
A.M. Cohen	T.H. Koornwinder	G.C.M. Ruitenburg
O. Diekmann	M. Kretzschmar	J.K. Scholma
B. Dijkhuis	H.A. Lauwerier	B. de Smit
I.M. Duursma	J. van de Lune	R. Sommeling
P.P.B. Eggermont	J.A.J. Metz	N.M. Temme
A. Grabosch	S. Mjølsness	J. de Vries
J.A.P. Heesterbeek	J. van Neerven	M. Zwaan
H.J.A.M. Heijmans		

INTEGRABLE SYSTEMS

Introduction
The area of integrable systems has mushroomed over the past two decades. It is becoming increasingly clear that these systems are situated at the crossroads of various subdisciplines in both mathematics and theoretical physics. On the mathematical side these include: representation theory of Lie algebras, Lie groups and quantum groups, harmonic analysis on symmetric spaces and special function theory, algebraic and symplectic geometry, combinatorics and knot theory. Included on the physical side are: statistical mechanics, quantum field theory and string theory. Research in this area at CWI is aimed at a deeper understanding of the interconnections between the manifold incarnations of integrable systems (classical/quantum, finite/infinite, discrete/continuous, ...), and at developing the theory of special functions related to quantum integrable systems, symmetric spaces and quantum groups.

The soliton rèvolution
The concept of 'integrable system' is by no means new. Even so, the intense and still increasing international research activity dealing with integrable systems only started with the discovery of the soliton in the mid-sixties. The existence of the solitary wave had been known much longer. Its first documented observation, as a heap of water moving with constant speed and shape along a canal, was made in 1834 by the Scottish scientist and engineer, John Scott Russell. Theoretically it was known as a solution to the Korteweg-de Vries equation (KdV), which models the behaviour of one-dimensional water waves (1895). However, the extraordinary stability properties of these solitary waves were first discovered numerically by Zabusky and Kruskal (1965). They studied collisions of solitary waves, and found that the waves emerge unscathed - with the same velocities and shapes as before the collision. Thus the waves behaved as if they were linearly superposed. This is highly surprising, since the KdV equation is nonlinear (it has the form $u_t = u \cdot u_x - u_{xxx}$, where t and x denote partial differentiation in time and space, respectively).

After their numerical discovery the N-soliton solutions to the KdV equation were soon found in closed form, and it became clear that there are many more partial differential equations (PDE's) admitting such particle-like solutions. Today, the range of applications of soliton PDE's is so vast, that it is often said that solitons have revolutionized nonlinear applied science. Apart from modelling a host of wave phenomena in physical contexts like hydrodynamics, acoustics, nonlinear optics, plasma physics and solid-state physics, they have found applications in areas as diverse as molecular biology, ecology, chemistry and electronics.

Classical integrable systems

In the 19th century, Hamilton and others recast the laws of mechanics as formulated by Newton in a most elegant and - as it transpired - fertile form. Thus, quantum mechanics emerges quite naturally from the Hamiltonian formulation of classical mechanics. Hamilton used *canonical* coordinates q and momenta p to describe a mechanical system. Without losing generality, but with simplicity in mind, we take a system with only one pair q,p (one degree of freedom). The temporal evolution of the state q,p of the system is then given by Hamilton's equations of motion $\dot{q}=\partial H/\partial p$, $\dot{p}=-\partial H/\partial q$ (the dot denotes differentiation with respect to time). The 'Hamiltonian' H usually represents the total energy of the system. Using *Poisson brackets* $[A,B]=\partial A/\partial q \cdot \partial B/\partial p - \partial A/\partial p \cdot \partial B/\partial q$, Hamilton's equations are brought in their most lucid form: $\dot{q}=[q,H], \dot{p}=[p,H]$. Two functions A and B are said to be Poisson-commuting if $[A,B]=0$.

In this simple situation one can make a 'canonical' coordinate transformation $p,q \rightarrow I, \phi$ to *action-angle* coordinates. 'Canonical' means that the transformation preserves the form of Hamilton's equations. These coordinates are characterized by H being a function of the action coordinate I alone. Hence one gets $\dot{\phi}=\partial H/\partial I$, $\dot{I}=0$, so that I is constant and ϕ evolves linearly in time. Thus, Hamilton's equations are easily solved ('integrated') in the new coordinate system.

Next, suppose a $2N$-dimensional system with coordinates $q_1,...,q_N$ and momenta $p_1,...,p_N$ is described by a Hamiltonian H_1. Then the above approach can also be applied, assuming the existence of further, independent Hamiltonian functions $H_2,...,H_N$ such that $[H_i,H_j]=0$ for all i,j. Specifically, a theorem by Liouville ensures that there is a canonical transformation to action-angle coordinates such that the transformed Hamiltonians only depend on the action coordinates and Hamilton's equations can be explicitly solved, provided one succeeds in locating explicitly the action-angle map. Such being the case, we speak of a *completely integrable system*. An early example is the so-called Euler top, the integrability of which was discovered in the 19th century.

Solitons vs. integrable systems

In the late sixties Kruskal and co-workers showed that the soliton phenomenon is intimately related to the presence of an infinite number of conservation laws. They also constructed a linearizing transformation which maps the initial value for the nonlinear evolution equation (e.g. $u(0,x)$ in the KdV case) to scattering data of an associated one-dimensional differential operator. This *inverse scattering transformation* (IST), as it is known, may be viewed as a nonlinear generalization of the familiar Fourier Transform. It maps evolution according to the original nonlinear equation into a very simple (in essence algebraic) evolution of scattering data.

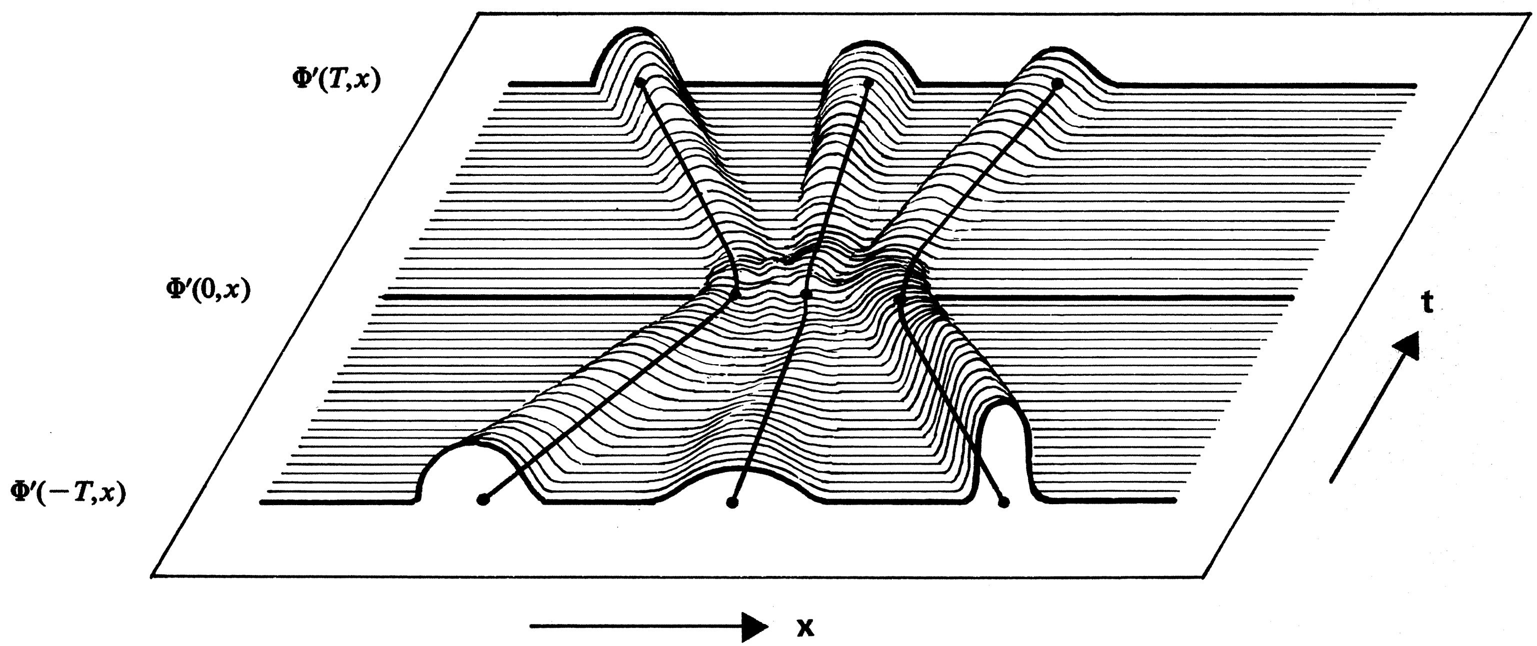
Inspired by these findings, Zakharov and Faddeev (1971) then made the connection to the classical Liouville concept of integrable system, by showing that the IST may be viewed as an infinite-dimensional action-angle map, the spectral and scattering data being the action-angle variables and the infinity of conserved quantities the Poisson-commuting Hamiltonians.

This insight led to a revival of interest in finite-dimensional integrable systems. As a result, several new systems of this type were discovered, most notably the Calogero-Moser and Toda N-particle systems in the 1970's. The particles described by these systems behave like solitons - in the sense that the set of velocities is conserved under scattering, and the position shifts are sums of pair shifts. At the quantum level these stability properties persist, just as for the quantum versions of various soliton PDE's the unitary scattering operator describing an N-particle collision preserves particle number and velocities, and factorizes into a product of 2-particle scattering operators.

Yang-Baxter equations and quantum groups

If more than one type of particle takes part in the scattering process, then a consistent factorization entails tight constraints on the 2-particle scattering operators: they must satisfy equations first written down by Yang. These braid-like equations arose independently in the context of soluble models in statistical mechanics (Baxter). The Yang-Baxter equations are now playing a crucial role in a quantum version of the classical IST and in a recent breakthrough in knot theory, which is relevant for recombinant DNA research. Moreover, they led Drinfeld and Jimbo to the invention of quantum groups. These are generalizations of Lie groups, which were introduced independently by Woronowicz from a quite different viewpoint (for more on quantum groups, see below).

More generally, it has turned out that the seemingly totally different subjects of Virasoro and Kac-Moody algebras, hierarchies of soliton PDE's and soluble lattice systems, conformally invariant quantum field theories, string theory, knot theory and quantum groups are intimately connected. A vast number of researchers is presentely exploring these subjects and their interrelationships.



Solitons are particle-like solutions to nonlinear partial differential equations. The picture shows a 3-soliton collision for the sine-Gordon equation $\phi_{xx} - \phi_{tt} = \sin \phi$. *This equation has been used to model the propagation of dislocations in crystals, phase differences across Josephson junctions, torsion waves in strings and pendulas, and waves along lipid membranes. It arose already in the last century in the context of pseudo-spherical surfaces and is also used (in quantized form) as a model for elementary particles. The presence of the nonlinear interaction only shows up in shifts of the soliton positions, as compared to the positions that would arise for a linear superposition. Furthermore, the shifts can be written as sums of pair shifts, leading to a physical picture of individual entities scattering independently in pairs. The 'weighted' sum of all position shifts adds up to zero, entailing that the centre of mass of the N solitons moves at uniform speed. The 'particle' trajectories underneath the soliton profiles arise in a relativistic generalization of the Calogero-Moser systems. They make it possible to follow the individual solitons during the course of the collision. There is mounting evidence that this correspondence between soliton field theory and sequences of generalized N-particle Calogero-Moser systems also holds in quantized form.*

Integrable systems vs. harmonic analysis

There is a relation between integrable systems of Calogero-Moser and Toda type and the theory of symmetric spaces (a special kind of space intimately related to Lie algebras). In the early eighties Olshanetsky and Perelomov showed that there is not only a relation at the classical level, but even more so at the quantum level: for special values of the coupling constants the series of commuting Hamiltonians may be viewed as the radial parts of the invariant differential operators associated with symmetric spaces. For these values (and for the case of Riemannian symmetric spaces) the two key problems of constructing the joint eigenfunction transform and proving its unitarity have been solved in essence by Harish-Chandra, whereas the first problem was recently solved for the general case by Heckman and Opdam. For a certain parameter regime where the eigenfunctions are polynomials in several variables, McDonald introduced a further generalization in terms of a parameter q. When $q \to 1$ his polynomials reduce to those of Heckman and Opdam. For the rank -1 ($\approx$2-particle) case his polynomials are given by basic hypergeometric functions.

Relativistic Calogero-Moser systems and solitons

Several years ago a generalization of the Calogero-Moser systems was discovered (Ruijsenaars/Schneider, 1985), characterized by an extra parameter. This parameter can be physically interpreted as the speed of light c: in the nonrelativistic limit ($c \to \infty$) the Calogero-Moser systems are recovered. Both the N-particle Toda systems and the infinite Toda lattice admit a similar integrable relativistic generalization (Ruijsenaars, 1985). This theory is now being developed by several workers. The new systems are intimately related to various soliton PDE's; in fact, one can obtain a unified picture of soliton scattering via their action-angle maps and associated scattering theory.

The N Poisson-commuting Hamiltonians can be quantized in such a fashion that N commuting analytic difference operators arise (Ruijsenaars, 1986). The resulting N-dimensional integrable quantum systems are again intimately related to various infinite-dimensional integrable systems. The main roadblock in a full clarification of these relations is formed by the construction of a unitary eigenfunction transformation, the quantum analogue of the action-angle map. This involves the functional analysis of analytic difference operators, an area which has not been studied before. Recently, Ruijsenaars has made considerable progress on these problems; even so, many questions remain open.

In a special parameter regime the N-particle eigenfunctions are now known from the work of McDonald mentioned above; the limit $q \to 1$ corresponding to the limit $c \to \infty$. This was pointed out by Koornwinder, who also proved the quantum analogue of the duality properties discovered by Ruijsenaars in his construction of action-angle maps. However, it turns out that the regime in which both sets of dual variables are continuous cannot be reached from McDonald's work - in which one set is discrete. In particular, the $N=2$ unitary eigenfunctions in this 'master' parameter regime so far constructed by Ruijsenaars reduce to q-ultraspherical polynomials upon analytic continuation and restriction, but this cannot be reversed by invoking the extensive lore on basic hypergeometric functions. This is intimately connected to the fact that analytic difference equations admit a plethora of solutions as compared to discrete difference and differential equations.

Quantum groups and special functions

Consider the group $SU(2)$ of unitary 2×2 matrices with determinant $=1$. The matrix elements u_{ij} $(i,j=1,2)$ can be considered as complex-valued functions on the group. They generate a commutative algebra $\mathcal{A}$, consisting of all complex linear combinations of finite products of the u_{ij} and the identity function I. The quantum group analogue of $SU(2)$ is obtained by assuming that the generators u_{ij} of $\mathcal{A}$ no longer commute, but rather that they satisfy a specific set of commutation relations. Quantum groups are not only intimately connected to quantum integrable systems, as mentioned above, but as it turns out they also constitute a new, vast area, where basic hypergeometric functions live naturally. Many of the analogues of classical concepts used in the theory of these functions depend on an additional parameter q, such that the limit $q \to 1$ leads to the classical situation. For instance, the q-analogue of the integral

$\int_0^1 f(x)dx$ is:

$$\int_0^1 f(x)d_qx := (1-q)\sum_{k=0}^{\infty} f(q^k)q^k.$$

It is easy to verify that this q-integral approximates $\int_0^1 f(x)dx$ as q tends to 1 from below (in essence Fermat used this method to compute $\int_0^1 x^\alpha dx$, as long ago as 1650). There is an analogue of the Haar measure on the $SU(2)$ quantum group, which, in certain realizations, can be expressed as a q-integral.
Vaksman and Soibelman (Soviet Union) were the first to observe that little q-Jacobi polynomials occur as matrix elements of the irreducible unitary representations of the quantum $SU(2)$ group. Later, independently, and using different methods, Masuda and others (Japan) and Koornwinder (CWI) also obtained this result. Still later it turned out that many other ways of associating special functions with representations of $SU(2)$ and their tensor products, do have analogues in the quantum case - with even more possibilities. For instance, due to the non-commutativeness of the algebra $\mathcal{Q}$, infinite-dimensional irreducible representations of $\mathcal{Q}$ will occur; and the generalized Clebsch-Gordan coefficients related to their tensor products can be expressed in terms of Wall polynomials, another family of q-analogues of the classical orthogonal polynomials.
The study of quantum groups also had its impact on special function theory. Starting from quantum $SU(2)$, Koornwinder derived a q-analogue of the addition formula for Legendre polynomials. Later on Rahman (Ottawa, Canada) proved this formula analytically, without the use of quantum groups, whereas Van Assche (Leuven, Belgium) showed that for $q \to 1$ the formula approaches the classical addition formula.
In principle, it is now possible to generalize the results in Vilenkin's frequently quoted book on special functions and group representations to a quantum group setting - at least for those parts dealing with compact groups. It would be even more interesting to obtain and study quantum analogues for non-compact groups like $SL(2,\mathbb{R})$. Unfortunately, we still lack a general theory offering prerequisites for harmonic analysis on such groups, as was so conveniently provided by Woronowicz in the case of compact matrix quantum groups.

PROCESSING AND RECONSTRUCTION OF IMAGES

Introduction

Computer image processing is a rapidly expanding technology with important consequences for science and industry. With the availability of cheap imaging hardware and computers, many researchers can now collect data in the form of digital images rather than photographic or numerical records. Examples are satellite pictures, optical and electron microscope images of materials and biological structures, radio telescope maps, and especially medical scan images. Each image represents a large quantity of highly structured data presenting new mathematical and computational challenges.
The goal of image processing may be just to improve visual quality, or to reconstruct an image from other signals (as in ultrasound or X-ray tomography). A recent development is the use of images for decision-making, e.g. in the automated inspection of production lines, or computer diagnosis of medical tissue samples. For such purposes we need to extract quantitative information by making a summary or analysis of the image.
CWI research on image processing focuses on *reconstruction from projections,* where the aim is to apply and develop mathematical methods from classical and numerical analysis to dynamic imaging; and *image analysis,* where stochastic image models and deterministic techniques from mathematical mor-

phology are used to extract information from image data.

Image reconstruction

Advances in computerized tomography (CT) have been spectacular in recent years, especially in the context of medical imaging. The Nobel prize for medicine in 1979 went to A. M. Cormack and G. N. Hounsfield for their work on CT. There are many CT techniques using different imaging modalities (X-rays, gamma rays, ultrasound, magnetic resonance, positron emission) all based on the idea of making a cross-section of a patient or object without physically cutting the object. This is done by measuring radiation passing through the object in different directions, then using numerical algorithms to reconstruct the desired image on a computer screen. Although the physics of the process may vary greatly, there is a common mathematical problem - how to reconstruct a function of a two-dimensional argument, given its integrals over straight lines. The mathematical solution was given by Radon as early as 1917, although this is not immediately suitable for practical implementation. Instabilities are inherent in the problem, and in practice only a finite number of line projections can be measured. Stability issues can be studied by numerical analysis techniques.

Considerable effort is devoted to the study of *incomplete data problems,* which arise for example when the X-ray viewing angle is restricted. A recent development is the use of probabilistic models, in which the image to be reconstructed is considered to be just one sample from a whole class of images which occur with varying probability. There is a close relation between stochastic modelling and the regularization techniques of numerical analysis.

In the classical CT problem it is assumed that radiation travels along straight paths, an approximation that is excellent for X-rays but less so for sound waves. This is relevant in ultrasound imaging and in seismic tomography. The corresponding mathematical problem, of recovering a function from its integrals over curved paths, is the subject of current research.

Dynamic cardiac imaging

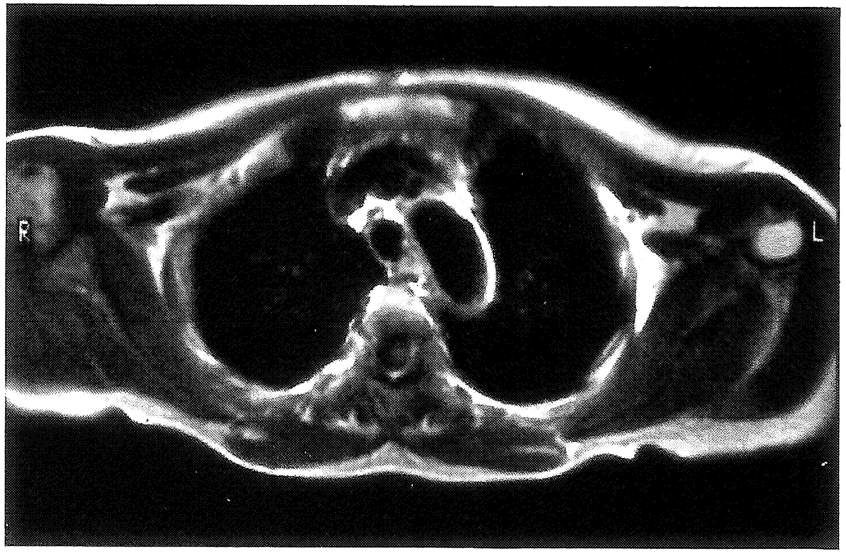
The work at CWI in the area of image reconstruction is concerned with dynamic imaging of the beating human heart by magnetic resonance imaging (MRI), in collaboration with Philips Medical Systems (Best). By a judicious choice of magnetic fields one is able to selectively excite the magnetic dipoles (spins) of hydrogen atoms which occur abundantly in water, and therefore in human tissue. The excited spins emit electromagnetic radiation which is recorded and the data are processed to construct an image of the chosen cross-section. In the case of dynamic imaging, one collects data for a number of phases during the cardiac cycle. Images of the heart during each phase are reconstructed and displayed in movie mode, enabling observation of blood-flow dynamics and dynamic heart function. A major problem is blurring and motion artifacts caused by irregular heartbeats (arythmia). A partial solution adopted in current practice is to reject data corresponding to very irregular beats. At CWI, models for the data acquisition process are being developed, which will automatically compensate for the variability of the heartbeat.

Image analysis and mathematical morphology

Image analysis is the task of extracting quantitative information about an image, which summarizes or describes the image. The extracted information is usually needed for decision-making purposes.

One very successful approach to image analysis is *mathematical morphology*. Information is extracted from an image by subjecting it to various 'transformations'. In general the required transformations do not improve visual quality, and actually reduce the information content. Instead they reflect one particular aspect of the image.

The case of *binary* (black or white) images is easiest to describe. Binary images can be modelled as sets in the plane by identifying 'black' with the object and 'white' with background. Image transformations are then simply transformations of subsets of the plane. As a simple example, to analyze the sizes of roughly circular features in an image, we may translate (shift) circular discs of varying sizes over the image and see where they 'fit' inside the black area. In effect one probes a compli-



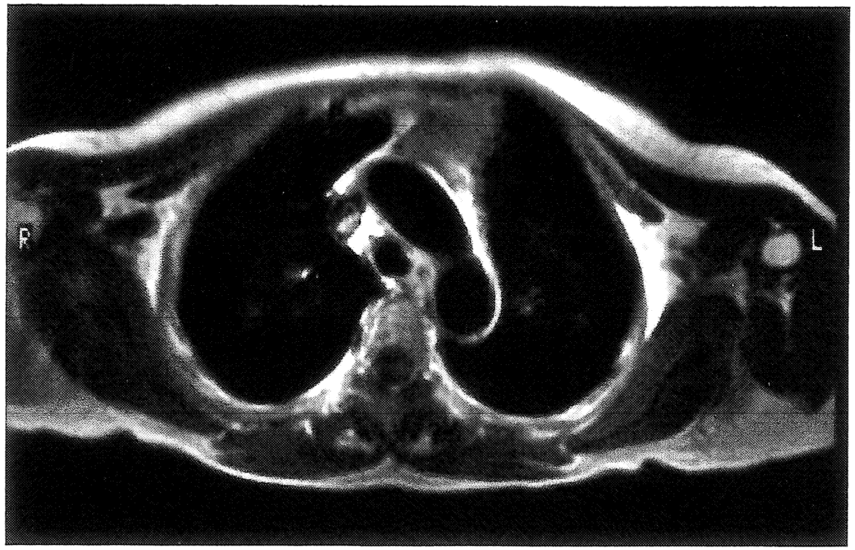


Image processing has numerous medical science applications and is an important source of information in the study of specific diseases. Hence, image processing can be used to make a movie of the human heart by combining multiple images taken at various stages, into one full cardiac cycle. CWI and Philips Medical Systems collaborate in a study of heartbeat variability. Here, images produced with the Philips Gyroscan show in cross-section given phases of the cardiac cycle of a patient with suspected paracardiac lymphoma (thymoma). (Courtesy Philips Medical Systems, Best)

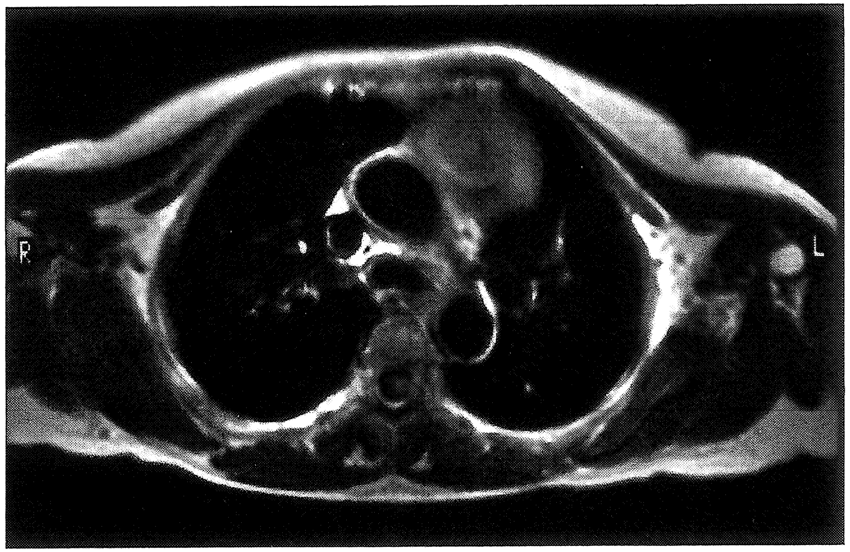
cated image by a simpler one (called the 'structuring element'). A large class of transformations can be generated from such basic operations (translation, set union and intersection). The simple structure of the operations enables one to build in a large degree of parallelism in the computer algorithms, to give high speed and efficiency.

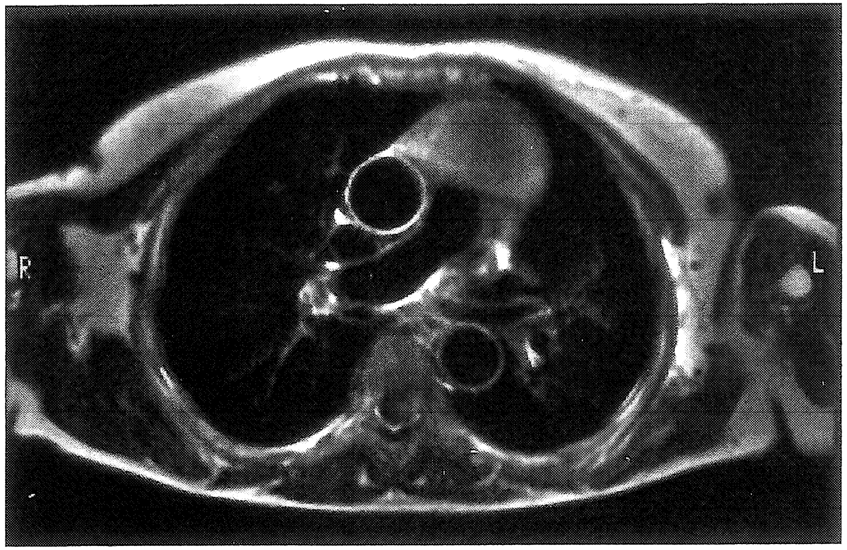
In practical applications such as industrial product inspection, the sequence of transformations required for decision-making is quite long and needs careful design. The theory of mathematical morphology is used to increase our insight into the mathematical structure of such sequences, as well as to develop and test new algorithms.

More abstractly one may describe binary image transformations as mappings from the Boolean lattice of all subsets of the plane into itself. The strongly algebraic approach suggested by this formulation has been the main object of study at CWI so far. A generalization has been developed towards more general lattices which are applicable to specific classes of subsets of the plane such as closed sets or convex sets, as well as to greytone images. There is also growing interest in the morphological approach to analysis of image data, and in relations between morphology and stochastic models.

Stochastic image analysis

It is increasingly recognized that every image processing algorithm is based on some under-





lying *model* describing the class of images likely to be encountered. Models incorporate our prior information, and may be deterministic (imposing a fixed constraint) or stochastic (specifying a probability for each possible image).

Stochastic image models are currently an area of feverish activity. Even in simple image enhancement problems, it is beneficial to model the corruption of the image by a random 'noise' process, and formulate the noise removal as a statistical estimation problem. This has led to very effective new algorithms.
In image reconstruction problems, the statistical community has developed new methods based on *Markov random field* models (generalizations of the classical Ising model in theoretical physics) which specify a stochastic dependence between neighbouring pixels. Bayesian methods for the statistical estimation problem have introduced a new class of efficient image restoration algorithms.
The stochastic viewpoint also provides a way of generating hypothetical images at random, by *computer simulation*. This can be used to perform computer experiments to measure the performance of image reconstruction algorithms. Simulation methods can also supply a series of alternative reconstructions from one set of data, indicating the strength of evidence for (say) the presence of a tumour. It turns out that the dependence structure between pixels in a Markov random field is very well suited to simulation, and is also 'natural' from a computing viewpoint.
Since image analysis is essentially a data reduction process, an alternative way to extract information from an image is to use statistical methods of data reduction. We formulate a stochastic model for the image, and estimate the parameters of the model, which then serve as a quantitative summary of the image. This approach provides extra benefits, such as measures of significance for the data extracted.
CWI research is developing stochastic models and estimation techniques where the image consists of a pattern of individual objects or features. The models allow random positions, sizes and shapes for these objects, with inter-

dependence between objects. The resulting parameter estimation techniques could be used in image analysis applications such as materials science and pathology. The same models can also be used in *feature extraction* problems.

Outlook

Image processing technology has traditionally been developed by the engineering community. The time is ripe for active involvement of mathematicians, with contributions from numerical and classical analysis, statistics and probability, geometry, topology and systems theory. CWI has an increasing interest in finding connections between different mathematical aspects. Various approaches to image reconstruction were the subject of a CWI colloquium in 1988.

The involvement of computer science is natural and obvious, both in the provision of new software for image processing research, and in elucidating the structure of processes such as simulation. By encouraging exchanges between the mathematical and computer science approaches, CWI hopes to make a substantial contribution to the exploration of this multidisciplinary research area.

PROJECTS

The following information is given for each project: a short description, the start-up year, research staff (project leader in italic) and cooperating institutions.

Algebra, discrete mathematics and computer algebra

The research is concerned with Chevalley groups and the associated geometries and, more generally, with geometries of Buekenhout-Tits type.

It is also concerned with some algebraic/discrete mathematical aspects of Lie groups, e.g. the classification of finite subgroups of exceptional Lie groups. In addition, there is research in coding theory, the theory of designs and the theory of graphs (especially distance-regular graphs).

There are also recent activities concerning the systematic use of computer algebra (symbolic manipulation) in these and other investigations. (1972)

A.M. Cohen, J.T.M. van Bon, A.E. Brouwer, I.M. Duursma, G.C.M. Ruitenburg, B. de Smit, R. Sommeling.

Univ. Rotterdam, Free Univ. Brussels, Univ. Michigan, Univ. Eindhoven, Univ. Freiburg, Cal. Tech. Pasadena, UC Santa Cruz.

Analysis

The purpose is harmonic analysis on (pseudo-)Riemann symmetric spaces, the study of special functions and their group theoretic interpretation, the study of (zero patterns of) special analytic functions and various problems of a number theoretic nature.

- Analysis on semisimple Lie groups and symmetric spaces and the connection with special functions. (1972)
  T.H. Koornwinder.
- Classical analysis and number theory. (1972)
  J. van de Lune, H.J.J. te Riele (CWI Dept. of Num. Math.).

Univ. Leiden.

Algebraic mathematical physics

The investigation of algebraic (and algebraic-geometrical), combinatorial and representation theoretical aspects of completely integrable Hamiltonian systems (both quantum and classical), the exactly solvable models from lattice statistical mechanics and parts of gauge theory and representation theory which are related to this.

- Relations between finite degree of freedom, infinite degree of freedom lattice, and classical integrable models. (1985)
  M. Hazewinkel, S.N.M. Ruijsenaars (Huygens), J.K. Scholma.

- Relativistic and quantum integrable systems. (1985)
  S.N.M. Ruijsenaars (Huygens).

Univ. Twente, Philips Telecomm. Hilversum, Univ. Utrecht, Univ. Amsterdam.

Dynamical systems
Research on dynamical systems, with emphasis on topological and measure-theoretic aspects. Later on possibly also chaotic and stochastic aspects (e.g. stochastic (partial) differential equations and their applications) will be studied. (1976)

J. de Vries.

History of mathematization
History of mathematical activity in the Netherlands over the period 1945-1960, in particular the history of founding the Mathematical Centre and of setting up the study course of Mathematical Engineer. Both events are being considered on the one hand in the general history context of their time, on the other hand against the background of the preceding development in the relation between mathematics and application. (1988)

P.C. Baayen (dir. CWI), G. Alberts, M. Hazewinkel.

Univ. Twente, Univ. Amsterdam.

Dynamical systems with stochastic perturbations
The investigations concern:
- Stochastic population dynamics;
- Random walks on random networks.

Characteristic of the first topic is the study of the expected sojourn time of the system in the neighbourhood of a stable equilibrium. In the second topic it is analyzed how the diffusion approximation is derived from the transition randomness of the network on large time properties. (1982)

J.B.T.M. Roerdink, H.N.M. Roozen.
Univ. Amsterdam, Univ. Utrecht, UC La Jolla.

Asymptotics and applied analysis
This project includes research on asymptotic expansions of integrals, and solving problems on analysis and asymptotics (with numerical aspects) from physics, biology, and statistics. (1975)

N.M. Temme, B. Dijkhuis.

Univ. Groningen, Univ. Winnipeg, Univ. Knoxville.

Nonlinear analysis and biomathematics
Analysis of differential equations (both ordinary, partial and functional) and integral equations which correspond to a mathematical description of biological processes. Whenever appropriate due attention is paid to the modeling aspects. (1975)

O. Diekmann, A. Grabosch, J.A.P. Heesterbeek, H.J.A.M. Heijmans, H. Inaba, Jin Cheng-Fu, M. Kretzschmar, H.A. Lauwerier, J.A.J. Metz, J. van Neerven.

Univ. Leiden, Univ. Delft, Univ. of Tech. Helsinki, Free Univ. Amsterdam, Univ. of Strathclyde Glasgow, Univ. Heidelberg, Virginia Polytech. Inst. and State Univ., Philips Telecomm. Hilversum.

Processing and reconstruction of images
- Research by means of mathematical and numerical analysis, mathematical statistics and computer science in support of methods for the processing and reconstruction of images;
- Development of algorithms and software;
- Contact with medical investigators, biologists and physicists, as well as with laboratories.

(1985)

J.B.T.M. Roerdink, P.P.B. Eggermont, H.J.A.M. Heijmans, P. Hofstee, M. Zwaan.

Acad. Hospital Utrecht, Philips Medical Systems Best, Shell KSEPL Rijswijk.

Department of Operations Research, Statistics & System Theory

J.K. Lenstra (head of department)
J.M. Anthonisse
A.J. Baddeley
D. Bakker
H.C.P. Berbee
J. van den Berg
J.L. van den Berg
O.J. Boxma
R.J. Chitashvili
J.W. Cohen (advisor)
A.L.M. Dekkers
F.A. van der Duyn Schouten
K.O. Dzhaparidze
S.A. van de Geer
R.D. Gill
P. Groeneboom
W.P. Groenendijk
L.F.M. de Haan
R. Helmers
A.W. Hoogendoorn
J.A. Hoogeveen
S. Kalikow
M. Kuijper
B.J. Lageweg
R.A. Moyeed
H. Oosterhout
M.W.P. Savelsbergh
A. Schrijver
J.M. Schumacher
J.H. van Schuppen
S.A. Smulders
S. Tardif
S.L. van de Velde
B. Veltman
P.R. de Waal
P. Wartenhorst
E.A.G. Weits
J.W. van der Woude

trainees:
C. Bibo
J. Borst
L. Jans
J.N.T. Schuit
A. Siekerman
C. Zwaneveld

STOCHASTIC PROCESSES

Introduction

Uncertainty plays an important role in many decisions. If the uncertainty is of a regular type, underlying the notion of probability, one can make sound and comprehensible decisions: hence the importance of probability in decision making and its development into a major tool in mathematical modelling. At CWI it is used as such in many projects, and a small research group specializes in stochastic processes. The CWI group's ongoing research explores new areas of this important way of investigating reality, e.g. higher-dimensional models and dependence structure in processes.

Main models and their use

We begin by briefly mentioning some basic probability models. As is clear from the introduction, probabilistic aspects had to be introduced into many deterministic models; a degree of insight into the role of probability, when dealing with uncertainty, is reasonably widespread. The repeated toss of a coin leads to an independent, identically distributed (i.e. all tosses are performed with the same coin) sequence of events - heads or tails. A sequence of random variables such as this is the simplest probability model one can imagine. Aspects like averaging and the error in averaging in these and similar models are still very important for practical purposes.
If independence becomes dependence in this sequence, the model becomes much more interesting. If dependence is such that memory of the past is lost, we get an interesting type known as Markov dependence. Such sequences, or *Markov chains*, can be used very flexibly in mathematical modelling; and, indeed, they are used extensively in topics as varied as the study of random walks, queueing networks, the spread of diseases and the voting behaviour of people at a meeting. Research on these chains confronts exciting open problems which are of basic interest. For example, in certain one-dimensional models with finite-range interaction developing in time, it is not known whether a unique equilibrium distribution exists. A solution is also relevant for certain computing problems in the theory of cellular automata.
Another simple and fundamental model in a different direction is obtained by studying the behaviour of a particle in a suspension; this gives rise to the *Brownian motion* of the particle. The basic theory was initiated by Einstein's celebrated paper in 1905. It was later elaborated on by Wiener, who studied the capriciousness of the particle's path struc-

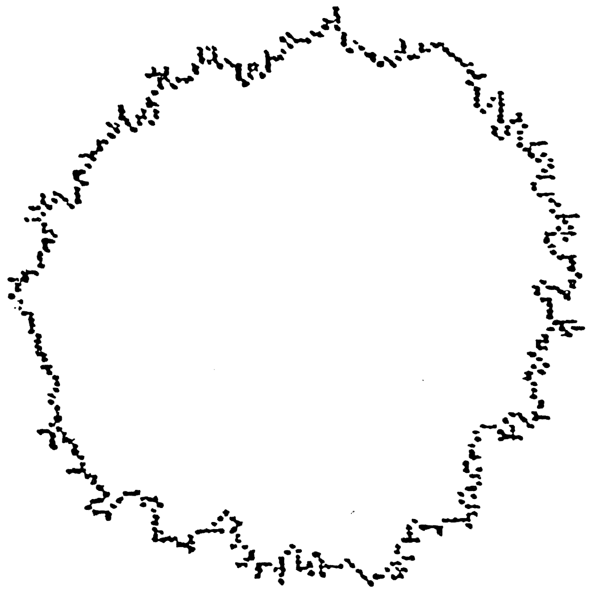
ture. This model had very early applications in quite different fields - e.g. description of stock market prices. The model is also very important in studying the basic equations of quantum mechanics (Schrödinger's equation) and related diffusion equations. Diffusion is a continuous-time Markov process which generalizes Brownian motion. Its study also gave rise to the formulation of *stochastic differential equations.* Equations of this type were the subject of various studies at CWI, e.g. in the field of traffic theory and in biomathematics. The solution of stochastic differential equations poses essentially new problems for which notions like 'martingale' (characterized e.g. in games by the future expected capital remaining the current capital) were developed.

The Dutch contribution to international development in probabilistic modelling really dates from the late fifties - with a prominent role being played by D. van Dantzig, a founding father of CWI. Currently, a large body of Dutch researchers publish regularly in prominent international journals; their articles cover many of the important and advanced models.

Current research at CWI

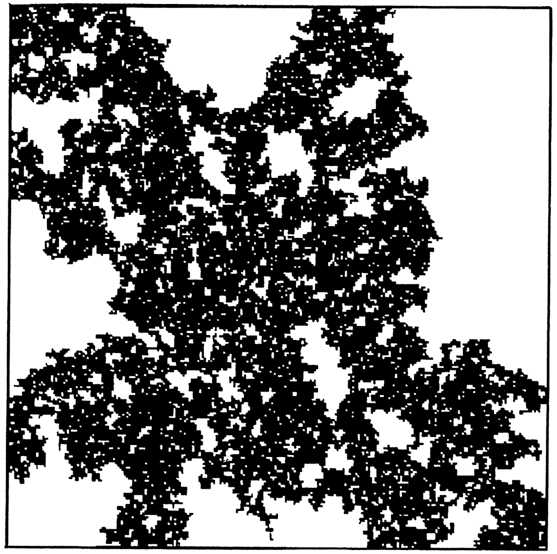
Most CWI researchers involved in probability have been applied probabilists studying special branches and statisticians who - by the nature of their work - also need good insight in probability models. The chance mechanism has its own, sometimes quite complicated, laws; these cannot always be unraveled by people working in side branches. And so, a few years back, CWI decided to form a small, separate research group to study stochastic processes. The decision was especially important for the exploration of new areas in probability theory.

Berbee studied varying topics including applications in game theory, in the simplex method in econometrics, in ergodic theory, in statistical mechanics, and also in pure probability theory. There are important connecting ties between these applications - in particular aspects of the *renewal theory* and its relation with Markov chains. To understand this theory consider a stationary stream of events, such as the operation of a machine in a factory. Now concentrate on a special event in this stream, such as the break-down of a certain unit of the machine, and consider its later occurrences in time, assuming this event has occurred at time 0. Renewal theory investigates the circumstances under which the probability of the occurrence of this event at time t converges to a constant for $t \rightarrow \infty$. This is related to the concept of 'mixing' in ergodic theory (the theory of dynamic systems, changing in time). The speed at which convergence occurs may be very important for practical reasons: for example, in queueing theory in networks a fast convergence rate expresses that the network stabilizes quickly and this is again linked to efficiency. In our approach to the simplex method (a standard method to solve a system of linear inequalities, i.e. constraints, as applied, for example, to econometric problems) it means that the ease with which essential constraints are found is proportional to their equilibrium



Growth in a plane or in space can occur without coordination between the various positions at the edge. The result is an edge with a capricious form. The global properties of such forms have been studied in probability theory. Renewal theory also requires better understanding of regularities in the growth pattern. The picture shows a given type of growth, some time after the moment of the origin.

probability of occurrence. It is important to remove the inessential constraints, since they cause a lot of additional, unnecessary work.
Van den Berg, who recently joined the stochastic processes group, did important work in *percolation theory.* In this branch of probability theory we investigate a very simple model related to phase transitions, which are studied in statistical physics to understand processes like magnetization and the formation of ice from water. In this theory the dimension of the percolation medium determines the character of the method used; consequently these methods can differ vastly from each other. In magnetization problems one may, for example, study the probability that a particle reaches infinity (occurrence of open paths) in a two-dimensional regular lattice. However, in the ice-water problem one works in a three-dimensional continuous Euclidean space.



Two-dimensional cluster of interconnected cells. A porous medium can be taken as comprising many small cells. Structure is dictated by the configuration of connected and unconnected cells. In percolation theory one studies the cluster of all cells connected with a given cell. An important application area is oil exploration. If pressure is used to expel oil from a given point of a porous medium, it can only be extracted from the cluster connected to that point.

Recent developments

One of the most appealing of Berbee's recent contributions concerns description of a stationary sequence of random variables as a functional of a Markov chain. Stationary sequences appear very frequently, in fact in all situations where there is a large stream of similar data. However, they may have a high complexity. The aim is to find a Markov chain of which the stationary sequence is a function: the complexity of the stationary sequence at a given time then being determined by the position of the Markov chain at this time in its state space. Generally, as there is no unique Markov chain, one aims at finding a simple chain. System theorists at CWI also work on this problem. There are clear relations with artificial intelligence. As a concrete example of discovering structures in a stationary sequence one may consider a language text as a stationary sequence of characters. Parsing the text induces a deterministic structure in the Markov chain to be developed. This chain describes the probabilistic frequencies of occurrence of text parts and their mutual relations.
Two other recent results should be mentioned here. A study on entropy and random walks in collaboration with researchers from the Technical University of Delft, sheds an interesting light on the asymptotic behaviour of the random walk with dependent steps (in contrast to the usual independence assumption). Other work in statistical mechanics attracted international attention. This concerned a model where at the critical temperature - at which a phase transition takes place - a jump occurs in the magnetization. A method was given to investigate uniqueness of the equilibrium state.

AIRCRAFT-STAND ALLOCATION

The complex logistics of a modern airport have a major influence on economic viability, with aircraft location during sojourn at an airport playing a crucial role. Between 1986 and 1988, CWI helped develop a planning system for aircraft-stand allocation at Schiphol Airport. The result was an interactive system: the planner makes his decisions in dialogue with the computer. Mathematically the problem can be formulated as an interval scheduling problem or a resource constrained scheduling problem.

Problem

Some 500 aircraft land at Schiphol every day, they stay for given periods and depart again. During such a *visit*, the aircraft needs a *stand*, i.e. a place for various handling operations such as loading and unloading of passengers and freight. These operations utilize a great number of resources: handling personnel, waiting-rooms, avio-bridges, fuel tankers, tractors, buses, luggage-belts etc. The location of the aircraft determines the flow of passengers outside and inside the terminal building and the flows of personnel and goods on the platforms. Hence, aircraft-stand allocation planning has a central role in the overall planning; it influences, directly and indirectly, other planning activities. Moreover, airport space being a scarce commodity, efficient use of the available stands is an important goal of aircraft-stand allocation.

Planning levels

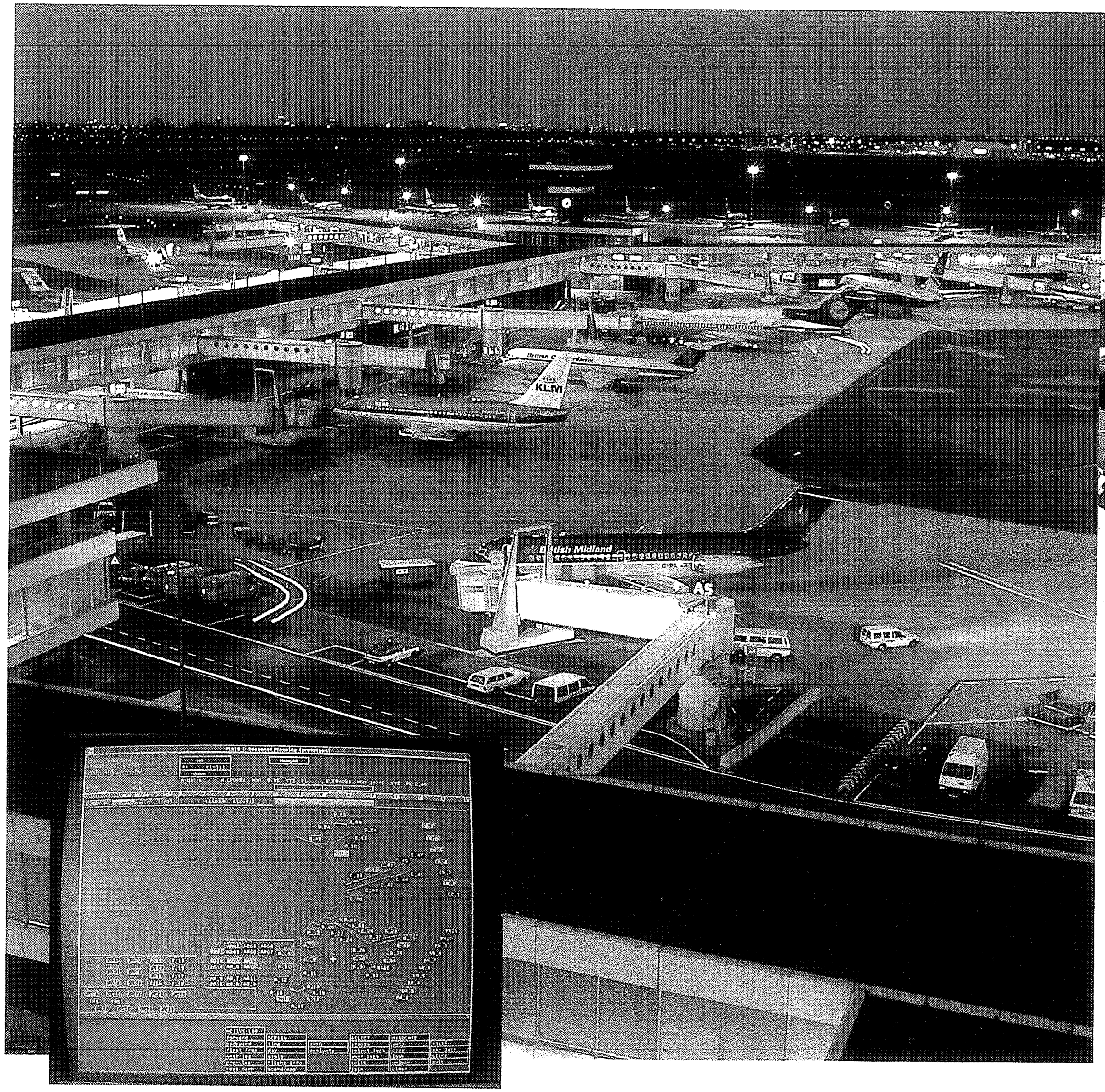
Planning of aircraft-stand allocation operates on three levels. As a first step there is twice yearly *seasonal planning*. This is based on airline schedules and available airport resources for the following season. A 'typical' week is selected from the season. Each visiting aircraft has to be assigned to a stand or a series of stands for this week. In this way, seasonal planning fixes the location of arrival and departure operations. It can be used for a short-term capacity analysis and as a starting point for other planning activities.

The second step in the aircraft-stand allocation, is a *basic day-plan*, made for the next day; more information is available now than at the seasonal planning stage; furthermore, each day will deviate from the corresponding day in the seasonal planning. The basic day-plan should take these things into account, while trying to stick to the seasonal planning as closely as possible.

Finally, on the operative level, a permanently updated *current day-plan* gives the actual stands to which aircraft are assigned. Deviations of time-table data will occur during the day. As a consequence, the basic day-plan has to be modified; this in turn can cause further changes in the remaining part of the day. The current day-plan should, however, stick to the basic day-plan as closely as possible.

Approach

Allocating aircraft to stands is a complex planning problem. Constraints and objectives are numerous and difficult to quantify. Moreover, it is not always clear whether a desired property, for example the assignment of passenger flights to gates with an avio-bridge, should be treated as a constraint or as an objective. The consequences for the planning are different: if it is a constraint, other assignments are forbidden, whereas they may occur in the case of an objective, but as infrequently as possible. The objectives cannot be combined into a single overall criterion. For example, gates with avio-bridges should be utilized as much as possible; however, this sometimes conflicts with the capacity of the corresponding waiting-room. It is then unclear whether the inconvenience caused by adding five more passengers to a waiting-room is equal to one more minute idle time for an aircraft at the gate. Neither can the objectives be strictly ordered according to priorities: an efficient use of platform capacity may impair the utilization of waiting-room capacity, but neither objective will always take priority over the other. As a consequence



Handling aircraft during sojourn is an increasingly complex operation. Until the recent introduction of computerized systems, Schiphol Airport allocated aircraft to stands manually. The first step came in 1988, when seasonal planning was transferred to the PLATO system; this interactive decision support system acts as advisor and assistant to the planner, who remains in constant control and is able to insert ad hoc modifications to the plan. PLATO was developed in cooperation with CWI. (Photos NV Luchthaven Schiphol)

of these facts, it is impossible to construct a model which fully captures the real-life planning situation. A variety of models, each emphasizing or ignoring aspects of the actual situation, is more appropriate for the planning process.
Planning itself is a continuous activity. An old plan is chosen as a starting point, then revised for changed constraints or objectives, or extended in time. The new plan is evaluated and on this basis modified again. Finally, the planner is satisfied and adopts as his own a certain plan from the set generated.
The traditional approach to a real-life problem in Operations Research (OR) involves formulation of a mathematical model which is solved, thus yielding a decision or a plan. However, the planning situation for aircraft-stand allocation demands a tool which supports the planning process rather than the generation of a single plan. Hence, our approach is oriented towards decision support rather than decision making.

Between assistant and advisor

This planning tool should enable the planner to generate and modify a plan. To do so, it must provide facilities for storage, retrieval and display of data on problem situations and plans; these are the typical functions of a Management Information System.
Now the planner can use the planning tool as an automatic scratch pad using modern computerized means to support the traditional manual planning techniques on a planning board. In such a way it becomes possible to use different representations of the problem data and to manipulate these data. The tool can also evaluate the quality of a given plan, in which traditional OR-models and -techniques may be applied. The system acts as an *assistant* to the planner.
On the other hand there is a need for the generation of a complete plan. The tool should have means, i.e. algorithms, to construct a complete plan or to modify an existing plan, by itself. It has now the role of an automatic pilot and acts as an *advisor* to the planner.
Many intermediate forms can occur between these two extremes; and the system can be used in several ways. For example, the planner may break down the problem into a series of subproblems, each based on the evaluation of an existing provisional plan, and then have the system generate solutions for those subproblems. Typical subproblems are assignment of all KLM London-bound flights to gates close to the terminal building, or reassignment of visits with the same departure time, to neighbouring gates. The system could also be used to extend a partial plan to a complete plan. Yet a third possibility is that the system suggests improvements for a plan, which the planner may subsequently implement manually - or ask the system so to do.
Whatever the case, the system should be able to perform the more routine-like parts of the planning job, enabling the planner to concentrate on main points and exceptional cases.
Characteristic for such a tool is the interaction between man and machine, using strong points of both. The machine is unbeatable when it comes to solving well-defined detailed problems. All the same, the planner, however, has to tell the system which problems to solve, and the planner can deal with ad hoc constraints which cannot be modelled adequately. So interaction can result in a better, more effective plan. Secondly, the system can display data and plans in an informative way to the planner, thus allowing him to select alternative plans, and increasing the efficiency of the solution process. The interaction may eventually increase the acceptance of the planning system. The human planner is not replaced, but remains in control over the powerful and flexible tool with which he has been supplied.

Implementation

The period 1986-1988 saw development and implementation of an interactive system for the seasonal planning problem by a joint project team from Schiphol Airport N.V. (NVLS) and CWI. The system is known by its Dutch acronym, PLATO1, standing for PLAtform Toewijzing Opstelplaatsen; this translates as 'platform allocation of stands'. From the start, two modules were distinguished within the system: a data module and a planning module.
The data module provides functions for storing and updating input data. The user then selects a planning problem and the data module sets ready all input data needed for

the proper planning, including a set of already existing plans. In the planning module the planning itself takes place on the basis of the input from the data module, resulting in one or more new plans. The data module finally stores these new plans and produces reports for various purposes.
We specified a simple interface between data and planning module, enabling us to develop the planning module without needing to know the detailed structure of the data module, and vice versa. NVLS developed the data module including communication with other systems at the airport. CWI concentrated on the planning module.
Following the approach outlined above, we first developed functions supporting the manual planning process. Two representations were chosen: the traditional planning board, already in use by the planners, and a geographical representation, i.e. the layout of the airport at a given moment. Functions to manipulate a single visit were specified for both representations. After adding functions for selecting and ordering sets of stands and visits, the planner could define subproblems and thus decompose the planning problem into smaller problems according to his insight. Next, evaluation functions gave the planner feedback on the plan produced so far.

Algorithms

In order to test these evaluation functions in an early stage, without being forced to complete a plan by hand, we implemented a simple and fast heuristic - i.e. a method which does not necessarily produce an optimal solution - for allocating all visits in a subproblem. In fact, this heuristic is a priority rule, based on the combination of a small subset of objectives by priorities and weights. A score is computed for all stands which are allowed for a given visit. Subsequently all visits are ranked - first by security classification - next by size of aircraft. Finally, the visits are assigned, one by one and as ranked, to the free stand having the highest score for the visit concerned.
We also formulated a mathematical model for the allocation problem. This problem can be formulated as an interval scheduling problem or as a resource constrained scheduling problem. Both problems are NP-hard, indicating that computation of an optimal solution may require an inordinate amount of computation time. Therefore, we restricted ourselves to approximation algorithms which deliver an acceptable solution within an acceptable amount of time.
Taking a given visit, the set of feasible stands can be ranked according to decreasing preference. All criteria must be taken into account in the ranking. From the moment ranking is known, we disregard priorities and weights, and use only the ranking itself. When we look at a short enough time interval, a set of visits contends for the same set of stands; this defines a linear assignment problem or, more precisely, a bipartite cardinality matching problem. We now determine whether this problem has a feasible solution minimizing the number of assignments of the lowest preference. Say we establish that, in any solution, we have to use this sort of 'least desirable visit-stand combination' five times. Next, fixing this number, i.e. adding the constraint to our problem that we use the least desirable combination at most five times, we minimize the number of assignments of the next lowest preference, and so on. We solve a series of linear assignment problems with side constraints, minimizing and then fixing preferences from below. Then, while respecting these side constraints, we maximize and fix preferences from above. It should be noted that in so doing, no lower preference is used in the assignment than is strictly necessary; so nobody comes off worse than necessary, i.e. to improve the assignment of a certain visit, the assignment of an other visit has to be made worse. Moreover, respecting this condition, as many as possible high preferences are assigned. By repeatedly applying these algorithms to a set of neighbouring time intervals we can generate a complete plan.
So far only the simple heuristic has been implemented in the PLATO1 system; however, it is easy to plug in more elaborate algorithms as described above.

PROJECTS

The following information is given for each project: a short description, the start-up year, research staff (project leader in italic) and cooperating institutions.

Combinatorial optimization

Combinatorial optimization is the mathematical study of problems involving the optimal arrangement, grouping, ordering or selection of a finite number of discrete objects. The subjects are:

- Design and analysis of algorithms (1973);
- Geometric methods (1983);
- Parallel algorithms (1982);
- Interactive distribution planning (1983);
- Interactive production planning (1985).

J.K. Lenstra, J.M. Anthonisse, J.A. Hoogeveen (NFI), B.J.B.M. Lageweg, H. Oosterhout, M.W.P. Savelsbergh (Shell fellow), A. Schrijver, S.L. van de Velde (NFI), B. Veltman.

Erasmus Univ. Rotterdam, Tilburg Univ., Bellcore, Eötvös Lorand Univ. Budapest, MIT Cambridge, Univ. Augsburg, Univ. California Berkeley, Univ. Pennsylvania.

Analysis and control of information flows in networks

The project concerns the mathematical modeling, analysis and control of information flows in computer systems and telecommunication networks. The subjects are:

- Analysis of mathematical queueing models (1981);
- Performance analysis of communication systems (1983);
- Performance analysis of computer systems (1985);
- Performance analysis of traffic control procedures (1987);
- Reliability and availability of networks (1987).

O.J. Boxma, J. van den Berg, J.L. van den Berg, J.W. Cohen (advisor), F.A. van der Duyn Schouten, W.P. Groenendijk, P. Wartenhorst.

Erasmus Univ. Rotterdam, Free Univ. Amsterdam, Tilburg Univ., Univ. Utrecht, AT&T Bell Laboratories, IBM Forschungslaboratorium Zürich, INRIA, Univ. Maryland.

System and control theory

System and control theory aims at formulating and analyzing mathematical models for dynamic phenomena, and solving control and prediction problems. The subjects are:

- Deterministic system theory (1984);
- Stochastic system theory (1978);
- Systems with a generalized state space (1988);
- Control of discrete event systems (1988);
- Prediction and control of motorway traffic (1984);
- Inverse scattering and image processing of seismic data (1988);
- Overload control for communication systems (1985).

J.H. van Schuppen, M. Hazewinkel (CWI, AM), M. Kuijper, J.M. Schumacher, S.A. Smulders (STW), P.R. de Waal (STW), J.W. van der Woude (Shell fellow).

Univ. Twente, Univ. Groningen, Philips Telecomm. Hilversum, Univ. California Berkeley, Univ. Gent, Univ. Padua.

Stochastic processes

Fundamental research on stochastic processes with special emphasis on processes in space *and* time, and research on the statistical analysis of particular stochastic processes.

- Stationary processes and their applications in physics (1981);

H.C.P. Berbee, S. Kalikow (guest).

- Statistical analysis of stochastic processes (1984);
  K.O. Dzhaparidze, R.J. Chitashvili (guest).
- Statistic analysis of traffic streams (1984).
  R.D. Gill, P. Groeneboom (advisor), E.A.G. Weits (STW).

Ministry of Public Works, Moscow Univ., Razmadze Mathematical Institute Tbilisi.

Semiparametric statistics
The construction of statistical procedures and the derivation of their properties for semi-parametric models, i.e. models which are partly parametric and partly nonparametric in character. Furthermore, the application of techniques from parametric statistics in non-parametric models, in particular estimation theory.

- Semiparametric estimation theory (1983);
  R.D. Gill, S.A. van de Geer, K.O. Dzhaparidze.
- Bootstrap methods (1984);
  R. Helmers.
- Order statistics (1984);
  R.D. Gill, R. Helmers.
- Statistical inference using extreme order statistics (1986);
  R. Helmers, L.F.M. de Haan (advisor), A.L.M. Dekkers.
- Statistical analysis of partially specified models (1988);
  K.O. Dzhaparidze, R.J. Chitashvili (guest).
- Statistical consultation and cooperation.
  R. Helmers, A.J. Baddeley, A.L.M. Dekkers, K.O. Dzhaparidze, S.A. van de Geer, A.W. Hoogendoorn, R.A. Moyeed, R. v.d. Horst (CWI-STO), L.F.M. de Haan (advisor).

Univ. Utrecht, Univ. Amsterdam, Univ. Leiden, WAVIN BV, CBS, Univ. of Washington (Seattle), Univ. Kopenhagen, Univ. Oslo, Univ. Baltimore, Limburg University Centre (Belgium).

Analysis and (re)construction of images
The aim of this project is to carry out research in the field of the statistical analysis of images. This means the investigation of methods for the solution of statistical problems, when the data are represented in the form of images.

- Statistical aspects of image analysis and reconstruction. (1986)
  A.J. Baddeley, R.A. Moyeed, R.D. Gill (advisor).

Hubrechtlab. KNAW Utrecht, Univ. Amsterdam, CSIRO Australia.

P.J. van der Houwen (head of department)

M. Bergman	P.A. van Mourik	*programmers*:
C.T.H. Everaars	R.R.P. van Nooyen	J.G. Blom
E.D. de Goede	H.J.J. te Riele	W.M. Lioen
P.W. Hemker	J. Schlichting	M. Louter-Nool
W.H. Hundsdorfer	J.H.M. ten Thije Boonkkamp	B.P. Sommeijer
J. Kok	J.G. Verwer	D.T. Winter
B. Koren	H.A. van der Vorst	P.M. de Zeeuw
J. Molenaar	P. Wesseling	
J. Mooiman	P.A. Zegeling	*trainee*:
		H. Meckering

FACTORIZATION OF LARGE NUMBERS ON VECTOR AND PARALLEL COMPUTERS

Introduction

Number theory is an area of mathematics which has a history going back to the ancient Egyptians and Greeks. Number-theoretic problems are often easy to state, but very difficult to solve. Computers can be a great help in sampling experimental information about the problem; doing so by 'hand' can be both dull and laborious.

Finding the prime factors of a positive integer is one of the classical problems in number theory. Many factoring methods were investigated before the coming of the computer. Of course, the advent of increasingly faster computers has considerably stimulated this research, but the largest impetus came from the invention of the RSA cryptographic system in 1975. The security of this system depends on the difficulty of finding the prime factors of a given large number.

With the arrival of vector computers, like the Cyber 205 at the Amsterdam Academic Computing Centre SARA in 1984, CWI started to study the factorization problem. The aim was to establish utmost bounds on the size of the numbers which can be factorized in a reasonable amount of computing time, with the help of the best-known factoring methods and the fastest available (vector and parallel) computers. The outcome of this research helps cryptographers to decide upon a 'safe' bound on the key in the RSA system. Moreover, the ability to factorize larger numbers helps extend our knowledge about certain other problems in number theory, e.g. the (non-)existence of odd perfect numbers (see below).

Factoring large numbers implies that we are able to prove primality of found factors. Therefore, we will discuss recent developments not only in factorization, but also in primality testing.

Primality testing

In 1640, Pierre de Fermat mentioned the following result in a letter to his friend, Bernard Frenicle de Bessy: if N is a prime number and if a is a positive integer such that their greatest common divisor GCD(a,N)$=1$, then

$$a^{N-1} \equiv 1 \pmod N. \qquad (1)$$

The congruence notation $p \equiv q (\bmod\, r)$ means that r divides $p-q$, also written as $r \mid p-q$. This result is known as *Fermat's Little Theorem.* It helps us decide whether a given number is composite without knowing a single prime factor of that number. Compute $b := a^{N-1} (\bmod\, N)$; this can be efficiently done by using the binary representation of the exponent $N-1$. If $b \neq 1$, then N must be composite. Unfortunately, the converse does not hold: if $b=1$, then N may be prime, but there are exceptions! The simplest one for $a=2$ is $341=11*31$.

A proper converse of (1) is the following result: if, for given N, we can find a positive integer a such that $a^{(N-1)/q} \neq 1 (\bmod\, N)$ for all prime divisors q of $N-1$, and if $a^{N-1} \equiv 1 (\bmod\, N)$, then N is prime.

If a number N satisfies (1) for more than one a for which GCD(a,N)$=1$, then the 'chance' of having a prime N increases, but there will still be many exceptions. Many such Monte-Carlo tests have been devised in the past 15

Fascination with the factorization of numbers is no recent phenomenon. From ancient Greece through to the present day mathematicians have tried to devise methods for checking whether a number is prime. The 17th century French mathematician, Pierre de Fermat, proved his important Little Theorem (not to be confused with his still unproven famous conjecture). The dominating figure of 19th century mathematics, Carl Friedrich Gauss, introduced modular arithmetic. In our present century, Derrick Henry Lehmer and Hendrik W. Lenstra, Jr. have made outstanding contributions, such as the Lucas-Lehmer primality test for Mersenne numbers and the Lenstra Elliptic Curve Method.

Pierre de Fermat (1601-1665)

Carl Friedrich Gauss (1777-1855)

years. None of them *guarantees* primality of the number being tested, but composite numbers which *pass* them are extremely rare.
It is only very recently that efficient *deterministic* primality tests have been found. It goes beyond the scope of this exposition to explain details, but it should be emphasized that efficient implementations of these tests enable us to prove primality of 200-digit numbers on a high-speed mainframe (like the Cyber 995) in about ten minutes CPU-time.

Factorization

In the simplest, and probably oldest factorization method one checks whether N is divisible by, successively, the primes 2,3,5,... . If a prime divisor of N is found, this is 'divided out' and the check is continued with the quotient until a number is left which has no prime divisors smaller than or equal to its square root (so that it should be prime).
Many refinements of this 'trial-and-error' method have been worked out, but for all these methods the amount of computational work to find a prime divisor p of N is always close to $O(p)$.
Many much more efficient methods are known, some of them requiring $O(\sqrt{p})$ operations. Here, we shall only give a simplified description of the best known method, called the *Quadratic Sieve Method* (QS). The method was devised by Maurice Kraïtchik in the nineteen-twenties and elaborated in the early eighties by Carl Pomerance. As the factoring out of small prime factors is better done by other methods, we will assume that the number N to be factorized is the product of only a few (we take here the typical case of two) large prime numbers: $N = pq$. Now, if we have a congruence of the form $u^2 \equiv v^2 (\bmod N)$, then N divides $u^2 - v^2$, or: $pq \mid (u-v)(u+v)$. The cases $pq \mid (u \pm v)$ do not bring us any further; however, if p or $q \mid (u \pm v)$, then the computation of GCD$(u-v,N)$, which can be performed quite fast, yields either p or q. In practice one only needs to try a few of these congruences to obtain the desired result.
Congruences of this form are found from a set of suitably chosen *quadratic residues*. Q is called a quadratic residue modulo N if there

Derrick Henry Lehmer (b. 1905)

exists a number A for which $A^2 \equiv Q(\mathrm{mod}\, N)$. If the set $Q_1,...,Q_n$ is chosen such that their product $Q_1 \cdot Q_2 \cdots Q_n$ yields a square, say u^2, then $u^2 = A_1^2 \cdot A_2^2 \cdots A_n^2 \equiv v^2\,(\mathrm{mod}\, N)$. This could in principle be realized as follows. Suppose, by some procedure, we have generated many Q's. Choose a *factor base* of r primes $p_1,p_2,...,p_r$ and find by trial-and-error at least $r+1$ Q's that completely factor over the factor base. Then it is easy to show that we can always find - by a so-called Gaussian elimination process - a subset of these Q's whose product contains only even powers of primes, and hence is a square. The problem is that, for the large numbers to which the method should be applied (N is typically several tens of decimal digits), this trial-and-error approach is extremely costly in computer time due to the volume of 'error': most of the time is spent on finding out that a particular p_i does *not* divide some Q. In order to keep the computation time within manageable limits it is also necessary that the trial-Q's are much smaller than N, for example $O(\sqrt{N})$. Characteristic for the QS method is that it generates sufficiently small Q's and avoids these 'negative' computations. Choose as the factor base all primes p smaller than some number B, satisfying $x^2 \equiv N(\mathrm{mod}\, p)$ for some x. The number B is a very sensitive 'tuning' parameter in the method. The set of Q's is chosen as $Q(x) := (x+M)^2 - N$, $x = 0, \pm 1, \pm 2, \ldots$, where $M = [\sqrt{N}]$. Clearly Q is a quadratic residue modulo N, and for $x << M$ we have $Q(x) \approx 2xM << N$. Also all prime factors $<B$ of the Q's belong to the factor base. These Q's can be factored with considerably less trial-and-error, because if $p \mid Q(x)$, then also $p \mid Q(x+np)$ for all integer n. All

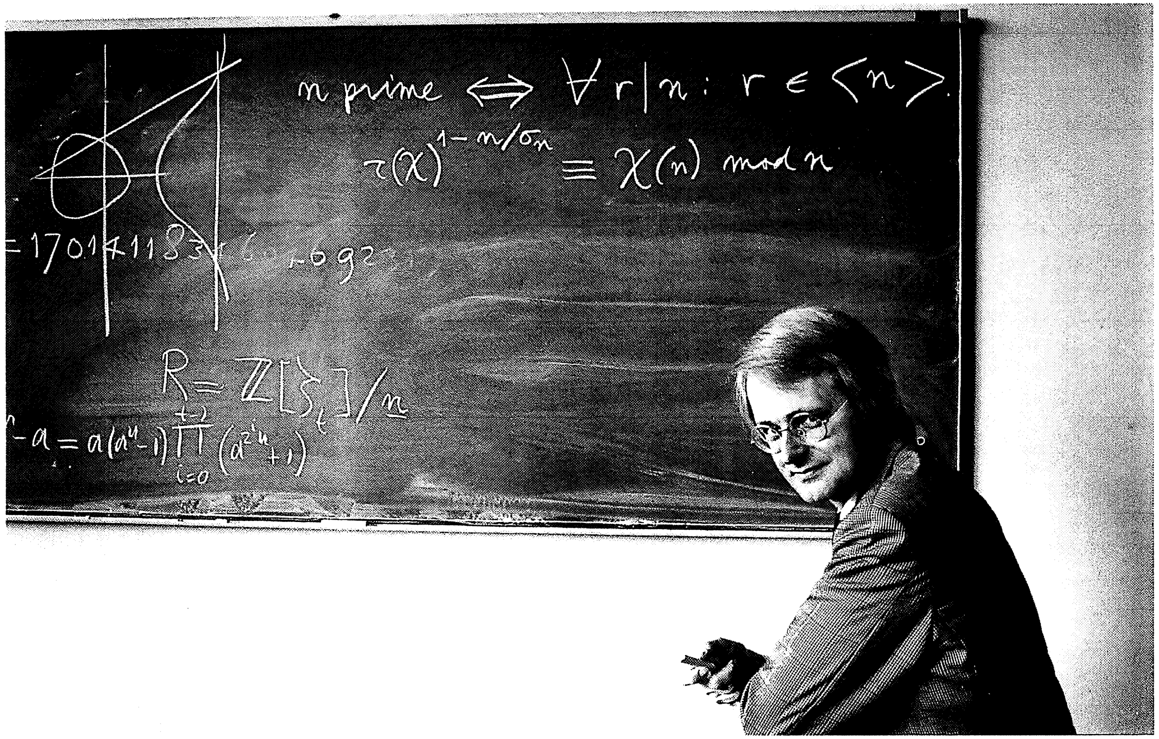


Photo by Mark Kohn

Hendrik W. Lenstra, Jr. (b. 1949)

Example of factorization with the QS Method

The number to factorize: $N = 5069$

$m=[\sqrt{N}]=71$

$Q(x)=(x+m)^2-N=x^2+142x-28$

Try as factor base $\{-1,2,5,7,11,13\}$; -1 is always included. Factorize $Q(x)$ for $x=0,\pm1,\pm2,...$, using the sieve; for example $Q(1)=5\cdot23$, therefore 5 is also a factor of $Q(6), Q(11),...,$ and of $Q(-4), Q(-9),....$ Find 7 Q's with only factors from the factor base. Construct binary vectors $r_1,...,r_7$ with coordinates 0 or 1 if a factor occurs with an even or odd exponent, respectively, as shown in the following table.

x	$Q(x)$	vector	coordinates (0's omitted)					
			-1	2	5	7	11	13
9	$1331=11^3$	r_1					1	
2	$260=2^2\cdot5\cdot13$	r_2			1			1
0	$-28=-2^2\cdot7$	r_3	1			1		
-1	$-169=-13^2$	r_4	1					
-2	$-308=-2^2\cdot7\cdot11$	r_5	1			1	1	
-8	$-1100=-2^2\cdot5^2\cdot11$	r_6	1				1	
-9	$-1225=-5^2\cdot7^2$	r_7	1					

Find linear dependences among the r_i that add up to zero (mod 2). One of these is $r_1+r_3+r_5=0$ (mod 2), corresponding to multiplication of the congruences $(80)^2\equiv11^3$(mod N), $(71)^2\equiv-2^2\cdot7$ (mod N) and $(69)^2\equiv-2^2\cdot7\cdot11$ (mod N). This leads to the quadratic congruence $(80\cdot71\cdot69)^2\equiv(2^2\cdot7\cdot11^2)^2$ (mod N), or $(1607)^2\equiv(3388)^2$ (mod N).

Computation of the two greatest common divisors GCD(1607−3388, N)=137 and GCD(1607+3388, N)=37 finally yields $N=37\cdot137$.

Remarks:

- in this case including 13 in the factor base was unnecessary, but non-inclusion means that one is not assured of finding a linear dependence;
- not every linear dependence leads to the desired result, e.g. $r_3+r_4+r_5+r_6=0$.

we then have to do is to find for each p in the factor base one x for which $p\mid Q(x)$. As soon as we have found one, we can generate a whole series of Q's which contain p as a prime factor. Skilful bookkeeping of these results makes it possible to find sufficiently many Q's, which completely factor over the factor base, in considerably less computing time than with other methods.

A complicated variant of the QS method is currently being used to factorize numbers of 100 and even more decimal digits.

A quite different class of factorization methods, called the *Elliptic Curve Method* (ECM), is based on Monte-Carlo type calculations in finite groups. This method was recently developed by H.W. Lenstra, Jr. It is complementary to the QS method in the sense that small divisors of large numbers N (of, say, 60 and more decimal digits) are usually found more easily by ECM, whereas larger prime divisors of N, in particular those which are close to $\sqrt{N}$, are usually found quicker by means of QS.

The recent developments in factorization and in primality testing are concisely described in the reference given below.

Results at CWI

The 'multiple polynomial' version of the QS algorithm was implemented and optimized on the Cyber 205 vector computer at SARA, prior to 1988. Many large numbers in the range of 40-72 decimal digits were factorized with the help of this program. These numbers fall into three categories:

- numbers of the form $b^n\pm1$;
- numbers which play a role in primality proofs of factors of Mersenne numbers 2^n-1;
- numbers which play a role in the proof of the non-existence of odd perfect numbers.

In 1988, CWI got access to the NEC SX-2 vector computer of the Dutch Aerospace Laboratory. At present, the SX-2 is the fastest known single-processor vector computer. The Cyber 205 factorization program was converted to and optimized for this machine, and several numbers in the range of 70-92 decimal digits were factorized about ten times faster than on the Cyber 205. The largest number factorized contained 92 digits: $(6^{131}-1)/(5*263*3931*6551)$. This represented a world record for numbers factorized on single-processor computers.

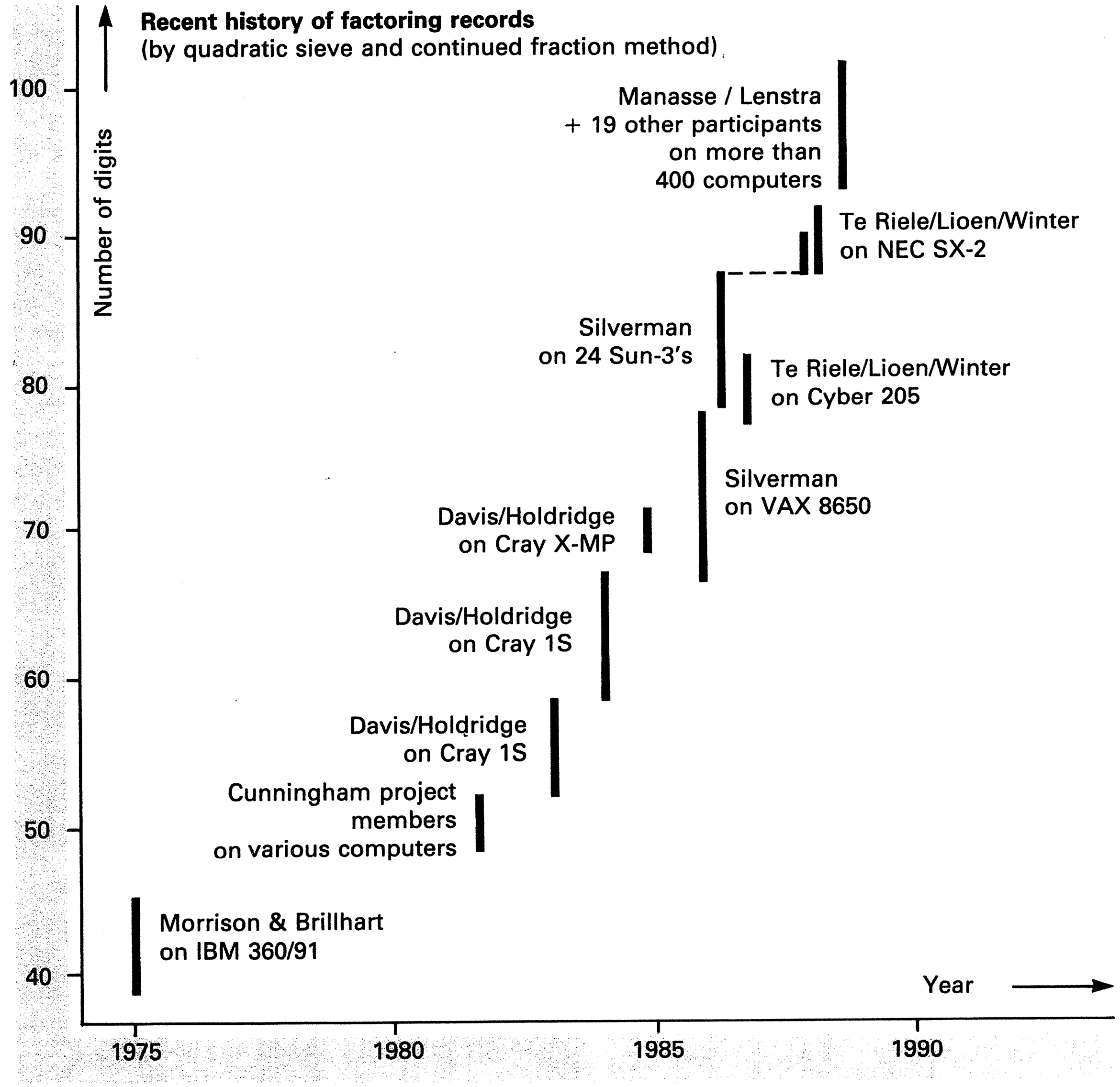
Following on from that, even larger numbers (of 93 and 96 decimal digits) have been factorized (by A.K. Lenstra and M. Manasse) using the QS method. The computer equipment employed here was a parallel system of several hundreds of micro-VAXes. Finally, a 'googol' (i.e., a 100-digit number) and a 102-digit number have been factorized by Lenstra and Manasse, using the computing power of several other computers in the USA, Australia and The Netherlands (including CWI). The googol attracted considerable attention in the popular-scientific press.

Many of the numbers factorized on the Cyber 205 and the NEC SX-2 were selected from a large list provided by R.P. Brent and G.L. Cohen. This helped them to shorten a proof of the non-existence of odd perfect numbers below 10^{300}.

Reference

J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, S.S. Wagstaff, Jr. (1988). *Factorizations of* $b^n \pm 1$, $b = 2,3,5,6,7,10,11,12$ *up to higher powers,* 2nd Edition, AMS Contemporary Mathematics Series, Vol. 22, Providence.

This excellent book gives a wealth of information both on historical and recent developments in factorization and primality testing, including extensive tables of numbers of the form $b^n \pm 1$, both factored and, as yet, unfactored.



PROJECTS

The following information is given for each project: a short description, the start-up year, research staff (project leader in italic) and cooperating institutions.

Discretization of initial value problems
Development, analysis and documentation of algorithms for determining numerical solutions of initial value problems for differential equations. The project is divided into two groups of subjects:

- Stability and convergence (1978);
- Navier-Stokes equations (1984);
- Differential-algebraic equations (1986);
- Adaptive grid techniques (1987).

J.G. Verwer, J.G. Blom, W.H. Hundsdorfer, H. Meckering, B.P. Sommeijer, J.H.M. ten Thije Boonkkamp, P.A. Zegeling.

- Shallow-water-equations (1985);
- Smoothing techniques (1987).

P.J. van der Houwen, J.G. Blom, E.D. de Goede, W.H. Hundsdorfer, B.P. Sommeijer, J.H.M. ten Thije Boonkkamp.

Univ. Bonn, Univ. Nijmegen, Univ. Manchester, Shell Research Amsterdam, Naval Postgraduate School California, Philips Eindhoven, Univ. of Valladolid, Univ. Halle, Techn. Univ. Delft.

Multigrid methods for boundary value problems
Development and analysis of modern techniques for the efficient numerical solution of boundary value problems. In particular the study of multigrid and related methods and their implementation on modern computer architectures. The subjects are:

- Defect correction and theoretical background (1978);
- Singularly perturbed boundary value problems (1978);
- Adaptive methods (1987);
- Applications in fluid dynamics (1983);
- Efficient techniques for the steady Euler and Navier-Stokes equations (1983);
- Evaluation and development of reliable and efficient numerical methods for the solution of semiconductor equations (1987).

P.W. Hemker, B. Koren, J. Molenaar, R.R.P. van Nooyen (IOP), P. Wesseling (advisor), P.M. de Zeeuw (STW).

NLR, Techn. Univ. Delft, Philips CAD-Centre Eindhoven, Univ. of Michigan Ann Arbor USA, GMD St. Augustin, INRIA Sophia-Antipolis, Techn. Univ. Hamburg Harburg, NAG Downers Grove (USA).

Computational number theory
Study of fundamental problems (which may be very old) in number theory with the help of modern (numerical) methods and fast computers. (1976)

H.J.J. te Riele, J. van de Lune (CWI, AM).

Gesamthochschule Wuppertal, Bell Laboratories/AT&T Murray Hill.

Numerical software

- Numerical software in the programming language Ada. (1981)
  J. Kok, D.T. Winter.
- Numerical software for vector- and parallel processors. (1984)
  H.J.J. te Riele, M. Bergman, E.D. de Goede, W.M. Lioen, M. Louter-Nool, P.A. van Mourik, J. Schlichting (CDC), B.P. Sommeijer, H.A. van der Vorst (advisor), D.T. Winter, P.M. de Zeeuw.

NPL Teddington, Argonne Nat. Lab., Univ. Amsterdam, NAG Oxford, Ada-Europe Numerics Working Group Brussels, ESPRIT.

Department of Software Technology

J.W. de Bakker (head of department)

K.R. Apt	R.J. van Glabbeek	E.A. van der Meulen
J.A. Bergstra	J.F. Groote	A. Ponse
M. Bezem	J. Heering	J. Rekers
F.S. de Boer	P.R.H. Hendriks	J.J.M.M. Rutten
R.N. Bol	P. Klint	J.W. Spee
M.H.H. van Dijk	J.W. Klop	M. Teunisse
A. Eliëns	J.W.C. Koorn	F.W. Vaandrager
P. van Emde Boas	L. Kossen	F.-J. de Vries
L.C. van der Gaag	P.J.F. Lucas	W.P. Weijland

LOGICAL ASPECTS OF ARTIFICIAL INTELLIGENCE

Many aspects of artificial intelligence are intimately connected with areas of mathematical logic. By using mathematical logic to model concepts originally developed in the area of artificial intelligence, we can get a better understanding of the issues at hand.
The aim of this project is to investigate the logical foundations of three areas of artificial intelligence: automated theorem proving, knowledge representation, and common sense reasoning. To this end our research is concentrated on logic programming, deductive databases, non-monotonic reasoning and the resolution method.

Logic programming
Logic programming is a simple and powerful formalism allowing us to model reasoning and knowledge representation in a single framework based on a fragment of first order logic. Logic programming was introduced in 1974 by R.A. Kowalski and has drawn considerable attention in the 1980s. There are at least two reasons for this. Firstly, it forms a theoretical basis of the widely used programming language PROLOG, and was adopted as the basis for the influential Japanese Fifth Generation Project. Secondly, the flurry of research on alternative programming styles led to a renewed interest in logic programming and its extensions. The power of logic programming stems from its extremely simple formalism and its reliance on mathematical logic. Logic programs are finite, non-empty sets of certain formulas of a first order language (see Box 1). Strictly speaking, logic programming is nothing more than a restricted form of automatic theorem proving (see Box 2).

Deductive databases
Deductive databases form an extension of relational databases in the sense that some of the relations are implicitly defined. They can be viewed as logic programs where the *explicitly* defined relations are those defined by means of unconditional clauses (i.e. clauses without premises). The *implicitly* defined relations are those which are also defined by conditional clauses. The main difference between deductive databases and logic programming lies in their emphasis on different problems. In deductive databases one studies such issues as query processing (i.e. computation of *all* answers to a given goal), integrity constraint checking, handling of updates (i.e. additions and deletions of clauses) and processing of incomplete or negative information (null values, distributed information, non-monotonic reasoning).
Deductive databases allow us to model a limited form of reasoning and certain modal aspects of knowledge, like 'necessity' and 'possibility'. They form a theoretical basis for expert systems.

Non-monotonic reasoning
SLD-resolution is an example of a *monotonic* method of reasoning. A reasoning method '$\vdash$' is called monotonic if, for any two programs P and P', $P \vdash \Phi$ (meaning: Φ can be proved from P) implies $P \cup P' \vdash \Phi$. Only positive facts can be deduced by SLD-resolution. Non-monotonic reasoning naturally arises when dealing with dynamically evolving informa-

BOX 1

Logic programs

A first order language (the notion goes back to G. Frege in the 19th century) consists of a collection of symbols (forming an alphabet) and all formulas defined over it. The symbols consist of a fixed set of *logical* symbols (connectives, quantifiers, parentheses, variables) and a varying set of *non-logical* symbols (constants, relations, functions), the latter characterizing the language. Two classes of strings of symbols are defined: *terms* (built up from variables and constants by applying the functions symbols) and *formulas*. The basic type of formula, called *atom*, is $p(t_1, \ldots, t_n)$, where p is an n-ary relation (predicate) and $t_1, \ldots, t_n$ are terms. Arbitrary formulas are constructed from atoms with the help of connectives and quantifiers.

The syntax of logic programming contains the following features:

- *atoms* A;
- *literals* L, being either atoms A (*positive* literals) or their negation $\neg A$ (*negative* literals);
- *clauses* C, written as $A \leftarrow A_1, \ldots, A_n$, and - in the declarative interpretation - to be understood as: conclusion A is true if premises $A_1, \ldots, A_n$ are true;
- *programs* P, consisting of finite sets of C;
- *goals* N, being clauses without conclusions: $\leftarrow A_1, \ldots, A_n$;
- the *empty goal* □, interpreted as a contradiction.

The execution of a logic program P with respect to a goal $G = \leftarrow A_1, \ldots, A_n$ aims at refuting G from P, i.e. showing that $\neg G$ is a consequence of P.

The refutation process produces a constructive answer to the question expressed in the goal. It generates a sequence of goals in which each consecutive goal is derived by computing a resolvent of the previous goal with one of the program clauses. To this purpose an atom is selected in each goal. This refutation process is called an *SLD-resolution*. When the first atom from the left is selected in each goal, the programming language *PROLOG* is obtained.

tion. Characteristically, statements which are true at a certain stage in the reasoning, will not always remain true. Examples of this type of reasoning are induction as used in empirical sciences and statistical reasoning. Instances of non-monotonic reasoning also occur very frequently in describing our behaviour in every-day situations - called 'common sense reasoning' in the terminology of artificial intelligence. Non-monotonic reasoning is modeled by a number of non-standard proof systems and methods including the circumscription method, default theory, auto-epistemic theory, various forms of closed-world assumptions and logic programming.

Stratified programs

Until three years ago research in logic programming, deductive databases and non-monotonic reasoning proceeded in an almost independent fashion. Recently, a number of researchers in this domain have succeeded in connecting these areas by establishing a common basis in the form of *stratified programs*. Stratified programs are logic programs which admit negative literals under the restriction that recursion through negation is disallowed. They have a natural semantics in the form of a specific Herbrand model (see Box 3). In 1988, T. Przymusinski introduced the concept of *perfect model semantics* and showed that a stratified program has a unique perfect Herbrand model. Recently, this model has been shown adequate for several forms of non-

BOX 2

As an example consider the following simple logic program, related to direct/indirect flights between cities:

1 $conn(x,y) \leftarrow direct(x,z), conn(z,y)$,
2 $conn(x,y) \leftarrow direct(x,y)$,
3 $direct(F,S) \leftarrow$,
4 $direct(S,P) \leftarrow$.

The first clause can be interpreted as: if cities x and z have a direct connection and if cities z and y are connected (directly or indirectly), then x and y are connected. The meaning of the other clauses is then clear.
The proof of the statement: 'There is a connection between cities F and P', is provided by the following SLD-refutation (numbers indicate the clauses applied):

$\leftarrow conn(F,P)$
| 1
$\leftarrow direct(F,z), conn(z,P)$
| 3
$\leftarrow conn(S,P)$
| 2
$\leftarrow direct(S,P)$
| 4
□

In general, SLD-derivations can be finite, ending in *success* (the empty clause □) or *failure* (no clause applicable to the selected atom of the goal), or infinite. SLD-derivations for a given goal can be grouped into SLD-trees, each tree corresponding to one selection rule. Each SLD-tree is finitely branching, but may contain infinite paths (consider the logic program $\{p \leftarrow p\}$ and the goal $\leftarrow p$).

monotonic reasoning, including circumscription method, default theory and auto-epistemic logic. This has established a natural connection between logic programming and non-monotonic reasoning and has shown the adequacy of perfect model semantics. Moreover, the use of stratification in theories dealing with non-monotonic reasoning has enabled us to establish various forms of equivalence between these theories.

Deductive databases can be viewed as logic programs without function symbols. This implies that Herbrand models of deductive databases are finite. By virtue of the above mentioned results stratified deductive databases admit a unique finite perfect Herbrand model, which is a natural interpretation of a stratified database.

Recent work

Recent work at CWI in the project led by K.R. Apt has concentrated on the analysis of perfect model semantics from the point of view of logic programming, deductive databases and non-monotonic reasoning. The effects of updates of a stratified database on this model were studied. An investigation of the model's recursion theoretic complexity has led to an evaluation of the complexity of various formalisms used for non-monotonic reasoning. Efficient ways were examined of computing closure of a finite set of facts under a finite set of rules - a basic component in the construction of the perfect model. An implementation was proposed for the membership problem with respect to the perfect model for a subclass of stratified deductive databases. It uses the resolution method of PROLOG augmented by a loop-checking mechanism. Finally, a general scheme was provided for proving completeness of several resolution methods, including the resolution method used in logic programming.

BOX 3

Herbrand models

In the semantics of logic programs, *Herbrand models* (named after the French logician J. Herbrand who studied these around 1930) take a prominent place. Herbrand models arise if one considers the interpretations built over the domain of all variable-free terms. Each Herbrand interpretation for a logic program P can be identified with a (possibly empty) subset of the *Herbrand base*, being the set of all ground atoms in the language of P. The atoms present in this subset are assumed to be true. By a Herbrand model for a set S of formulas we mean a Herbrand interpretation in which every formula from S is true. Herbrand models naturally arise when studying logic programs.

Assuming that the elements of the Herbrand base satisfy some priority ordering, we call a Herbrand model of a general program P *perfect* if there are no Herbrand models of P *preferable* to it. A Herbrand model N of P is preferable to a Herbrand model M of P if it is obtained from M by adding/removing some atoms and an addition of an atom to N is always compensated by the simultaneous removal from M of an atom of higher priority. Thus a model is perfect if this form of minimization of higher priority atoms is achieved in it.

Selected references

1. K.R. APT (1988). *Introduction to Logic Programming,* CWI Report CS-R8826 (to appear in the Handbook of Theoretical Computer Science).
2. M. BEZEM (1988). Logic programming and PROLOG. *CWI Quarterly, Vol.1, No.3,* pp. 15-29.
3. Contributions from K.R. APT, H.A. BLAIR and A. WALKER (Towards a theory of declarative knowledge), T. PRZYMUSINSKI (On the semantics of stratified databases), and A. VAN GELDER (Negation as failure using tight derivations for general logic programs) in: *Foundations of Deductive Databases and Logic Programming* (J. MINKER, ed.), Morgan Kaufmann, Los Altos (1988).
4. T. PRZYMUSINSKI (1989). Non-monotonic reasoning vs. logic programming: a new perspective; to appear in *Handbook on the Formal Foundations of Artificial Intelligence* (Y. WILKS and D. PATRIDGE, eds.).

PROJECTS

The following information is given for each project: a short description, the start-up year, research staff (project leader in italic) and cooperating institutions.

Concurrency
Research into the semantic aspects of parallel computation according to various programming styles (imperative, applicative-functional, dataflow, object-oriented); also proof methodology for parallel computation (1984).

J.W. de Bakker, F.S. de Boer, J.J.M.M. Rutten.

ESPRIT, Free Univ. Amsterdam, Univ. Kiel, Univ. Pisa, SUNY Buffalo.

Formal specification methods
Research concerning specification languages, process algebra, executable specifications and systems development methodology. (1982)

J.W. Klop, J.A. Bergstra (advisor), R.J. van Glabbeek, J.F. Groote, A. Ponse, F.W. Vaandrager, W.P. Weijland.

ESPRIT, Univ. Amsterdam, Univ. Utrecht, Free Univ. Amsterdam, Philips.

Extensible programming environments
Algebraic specification of programming environments, incremental development of language definitions, implementation of algebraic specifications. (1982)

P. Klint, J.A. Bergstra (advisor), M.H.H. van Dijk, J. Heering, P.R.H. Hendriks, J.W.C. Koorn, E.A. van der Meulen, J. Rekers.

ESPRIT, Univ. Amsterdam.

Term rewriting systems
Foundational research centering around term rewriting systems, with an emphasis on algebraic and syntactic methods; foundational research in process algebra. (1989)

J.W. Klop, R.J. van Glabbeek, F.J. de Vries.

Free Univ. Amsterdam, Univ. Amsterdam, Univ. Utrecht, Univ. Nijmegen.

Expert systems
Research into the applicability of methods of knowledge representation and automatic reasoning in expert systems. Distributed problem solving in expert systems. The development of prototype expert system tools. (1985/1986)

P.J.F. Lucas, A. Eliëns, P. van Emde Boas (advisor), L.C. van der Gaag, L. Kossen, J.W. Spee, M. Teunisse.

Univ. Rotterdam, Philips Research Lab. Eindhoven, Univ. Leiden, Univ. Utrecht, Techn. Univ. Delft, Univ. Twente, Univ. Amsterdam.

Logical aspects of artificial intelligence
Fundamental research into topics such as: logic programming and the construction of expert system shells, non-monotonic reasoning and reasoning involving time, knowledge representation and epistemic logic, dealing with partial and inconsistent information. (1987)

K.R. Apt, M. Bezem, R.N. Bol, P. van Emde Boas (advisor).

Department of Algorithmics & Architecture

L.G.L.T. Meertens (head of department)
C.A. van den Berg
H. den Boer
J.N.E. Bos
D. Chaum
M.J. Coster
M.M. Fokkinga
L.J.M. Geurts
E.J.L.J. van Heyst
J.T. Jeuring
M.L. Kersten
E. Kranakis
D.D.M. Krizanc
S.J. Mullender
S. Pemberton
G. van Rossum
F.H. Schippers
I. Shizgal
A.P.J.M. Siebes
N.Th. Verbrugge
P.M.B. Vitányi
M.H. van der Voort

programmers:
C. Algeo
E.D.G. Boeve
F. van Dijk
A.J. Jansen
T.J.G. Krijnen
S. van der Zee

trainees:
A.F. Bakker
K.T.L. Blom
H.L. van het Bolscher
P. Bosch
F.A. Bosman
J.-H. Bührmann
K.C. Chan
E.G.M. Embsen
M. Gathier
J.C. van der Heide
K. Kim
F.J.P. Lim
H.E. Lohuis
J.T. Tromp

PRISMA

The PRISMA project (PaRallel Inference and Storage MAchine) is a large-scale research effort in the design and implementation of a highly parallel machine for data and knowledge processing. The PRISMA database machine is a distributed, main-memory database management system (DBMS). It is implemented in a parallel object-oriented language which runs on a multi-computer system. The prototype envisioned consists of 64 processing elements.

Introduction

The design and construction of database machines to improve non-numeric processing has attracted many researchers during the last two decades. At one end of the spectrum, database machines have reduced the amount of data to be manipulated by filtering records when these data are transferred from disk to main-memory and by using several functionally specialized computers linked into a network. The other end of the spectrum is characterized by attempts to harness the processing power and storage capacity offered by large scale integration. Despite the many research efforts, few database machines are currently commercially available (e.g., ICL/CAFS, Britton-Lee IDM, Teradata DBC-1024). This situation can be attributed to provision of partial solutions, rapid evolution of hardware technology, and monolithic architecture of most database systems. Current relational database machines in particular fall short, providing only a fixed set of primitive data types, i.e. integer, float, and fixed/variable length strings.

Although these data types suffice for most business-like database applications, the fixed set of operators, their storage layout, and their use within the query optimizer make it difficult to accommodate new application areas such as statistical databases, CAD/CAM, and office automation. An alternative approach is to build an 'extensible' database system. Such a system provides a mechanism to introduce new data types, a mechanism to enhance the query optimizer, and the storage techniques.

Another observation is that no single DBMS will efficiently support all database applications. Hence, a need arises for a variety of facilities, providing the proper level of abstraction, user interface, and functionality. For example, integration of microcomputers with mainframes pushes the need for cooperative database systems and interfaces with low-end database systems, such as spreadsheet packages. A consequence is that future database systems should be designed with distribution in mind, i.e. a DBMS comprising a set of database managers, each providing part of the required functionality, and coordinated by a distribution manager. The cost for main-memory drops rapidly; so, it becomes feasible and cost-effective to keep a major portion of the database in main-memory. Since one may not assume that 1 GigaByte can be managed by a single processor, due to hardware and performance limitations, it is mandatory to design the database as a distributed system from scratch. Moreover, since dealing with physical limitations has a strong negative effect on the performance, such a new system ought not have provisions for handling, e.g., memory overflow (except for recognition of that event). In fact, if the database does not fit in the available memory, the user should construct a distributed database. It is assumed that the distribution manager takes care of proper duplication of information to guarantee continual service and reconstruction of the database, e.g. by keeping a copy of the database modifications on a (slow) disk drive.

The PRISMA project

The PRISMA project is an attempt to gain experience and knowledge concerning parallel processing of data and knowledge through the construction of a running prototype. This long-term project objective translates into the following concrete goals:

- the construction of a multi-computer system, consisting of a large number of processing elements connected via a message-passing network;
- the definition and efficient implementation of a parallel object-oriented language, called POOL-X;
- the design and implementation of a main-memory database system in POOL-X;
- the design and implementation of an expert system shell in POOL-X that exploits parallelism for inferencing;
- the investigation of using medium to coarse grain parallelism for data and knowledge processing applications, the integration of data and knowledge processing, and the evaluation of the prototype multi-computer.

Key issues in the PRISMA database machine

The most important ideas behind the design of the PRISMA database machine are that:

- it aims at performance improvement by introduction of parallelism and by using a very large main-memory as primary storage;
- it is designed as a tightly coupled distributed database system;
- it provides an SQL and a logic programming interface;
- it uses a knowledge-based approach to exploit parallelism;
- it uses a generative approach for data managers.

A comparison with other systems can be found in [1]. In the remaining sections we will focus on the database system and machine part of the PRISMA project.

Global architecture of the database system

The PRISMA DBMS consists of centralized database systems, called One-Fragment Managers (OFM), running under the supervision of a Global Data Handler (GDH). The architecture of an OFM is explained below. The GDH contains the data dictionary, the query optimizer, the transaction manager, the concurrency control unit, and the parsers for SQL and PRISMAlog (a logic programming language like Datalog). In addition to these components, there is a recovery component and a data allocation manager.

Parallelism will be used both within the DBMS and in query processing. Within the DBMS this will be obtained by running several instances of components of the DBMS in parallel. Examples of these components are the parsers, the query optimizer, the transaction monitor, and the OFM's for intermediate results. For each query a new instance is created, possibly running at its own processor. This means that evaluation of several queries and updates can be done in parallel, except for accesses to the same copy of base fragments of the database.

The logic programming language defined in PRISMA is called PRISMAlog. It is based on definite, function-free Horn clauses and its syntax is similar to Prolog. One of the main differences between PRISMAlog and pure

Photo by Nico Stam

A parallel software system behaves in many respects like a flight of birds. Both consist of a large number of (semi-)autonomous systems, which should exhibit a predictable course (behaviour) under external influences. The study of the behaviour of birds - reaching back to the pre-Christian era - suggests that the design and control of a parallel system will require long-term research, for which time-consuming observations of the system's behaviour will prove inevitable.

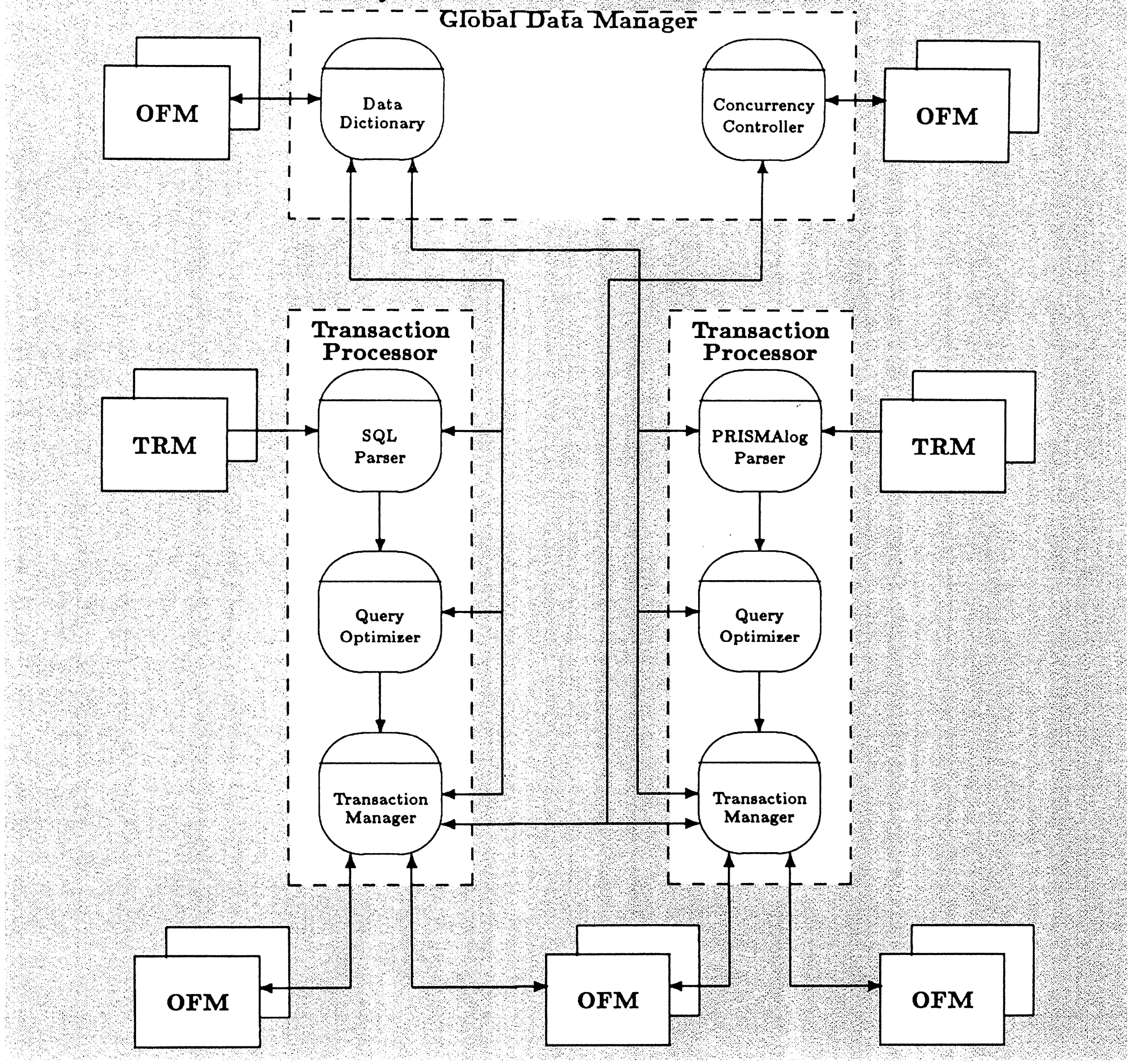
Prolog is that the former is set-oriented, making it more suitable for parallel evaluation. The semantics of PRISMAlog is defined in terms of extensions to the relational algebra. Facts correspond to tuples in relations in the database. Rules are view definitions including recursion.

To exploit parallelism on a large processor pool requires, among others, a choice of the grain size: coarse or fine grain. In the PRISMA-project the coarse grain approach is taken as we expect it to give us better performance in our multi-computer architecture.

A knowledge-based approach to query optimization is chosen to exploit all this parallelism. The knowledge base contains rules concerning logical transformations, estimation of sizes of intermediate results, detection of common subexpressions, and application of parallelism to minimize response time.

The DBMS software is organized as a fully distributed database system in which the

Data flow in the PRISMA database machine



components are One-Fragment Managers. OFM's are customized database systems which manage a single relation fragment. They contain all functions encountered in a full DBMS, such as: local query optimizer, transaction management, markings and cursor maintenance, and various storage structures. More specifically, they support a transitive closure operator for dealing with recursive queries. Several OFM types are envisioned, each equipped with the right amount of tools. For example, OFM's needed exclusively for query processing do not require extensive crash recovery facilities. Moreover, each OFM is equipped with an expression compiler to generate routines dynamically. In this way the architecture of an OFM is tuned towards the requirements which can be derived from the relation definition, and it avoids the otherwise excessive interpretation overhead incurred by a query expression interpreter.

The PRISMA machine

The PRISMA machine implements a parallel object-oriented language (POOL-X) on a multi-computer system. The programming model of POOL-X is a collection of dynamically created processes. Internally the processes have a control flow behaviour and they communicate via message-passing only, i.e. no shared memory. The computational grain of parallelism is medium to coarse. POOL-X is closely related to POOL2 (see [2]), a general purpose object-oriented language. It is strongly typed and hides the multi-computer details. POOL-X is somewhat tailored to the data- and knowledge-processing applications. At a few specific points it introduces dynamic typing to provide efficient support for the implementation of relation types. Furthermore, POOL-X supports explicit allocation of the dynamically created processes onto processing elements. This allows for a proper balance between storage, processing and communication.

The multi-computer architecture envisaged in PRISMA encompasses a number of processing elements connected via a high band-width message-passing network. All processing elements have (data)processing, communication and (local) storage capabilities. The various capabilities have to be balanced in such a way that ultimately the processing elements can be integrated in VLSI. In this way a powerful multi-computer can be implemented cost-effectively, by simple replication of (cheap) components.
In a first prototype set-up the multi-computer will consist of 64 processing elements, each with four communication links running at 10 Mbit/sec, and a local main-memory of 16 MByte. Apart from the local main-memory, some processing elements will also be connected to secondary storage (disk); the multi-computer system uses these to implement stable storage and automatic recovery upon system failures. This approach leads to a simplification in the design of the DBMS.

Organization and status
The project started in October 1986 and is scheduled until September 1990. The project is led, and to a large extent financed, by Philips Research Laboratories in Eindhoven. Other participants are the Universities of Amsterdam, Leiden, Twente and Utrecht, and CWI. CWI's contributions come from two project groups, *Distributed adaptive information systems* (headed by M.L. Kersten) and *Expert systems* (headed by P.J.F. Lucas). Currently approximately 30 people are directly involved. The project is partially funded by the national programme SPIN. During the first phase, 1986 and 1987, the main components of PRISMA, viz. an expert system, DBMS and multi-computer, have been identified and a functional design has been written. In 1988 the first prototype DBMS, called PRISMA/DB, was jointly implemented with the University of Twente. The resulting program, thirty thousand lines of POOL-X statements, runs on a SUN workstation and shows the feasibility of a parallel object-oriented language for implementing a non-trivial software system. Moreover, the architecture of the DBMS has shown that labour can be successfully divided over several research sites, and that components can indeed be modified with relative ease. The first machine with operating system and compiler will be available for experimentation in early 1989: we will then learn whether the software and hardware architecture performs as expected. We will use the remaining period of the project to focus on specific research topics, such as handling integrity enforcement within a distributed system, and compiling specialized one-fragment managers from their specification. Subsequently, the PRISMA/DB system will be used in the ESPRIT II project TROPICS, where it will be further enhanced to support multi-media documents within an office environment.

References

1. M.L. KERSTEN, P.M.G. APERS, M.A.W. HOUTSMA, H.J.A. VAN KUIJK, R.L.W. VAN DE WEG (1987). A distributed, main-memory database machine. *Proc. of 5th International Workshop on Database Machines,* Karuzawa, Japan, 353-369.
2. A.W. BRONNENBERG, A. NIJMAN, E. ODIJK, R. VAN TWIST (1987). DOOM: a decentralized object-oriented machine. *IEEE Micro.*

PROJECTS

The following information is given for each project: a short description, the start-up year, research staff (project leader in italic) and cooperating institutions.

Complexity and algorithms

The design of efficient algorithms, in particular for distributed computations, and fundamental research into the concrete complexity of algorithms and Kolmogorov complexity with applications to the mentioned subjects. (1980)

P.M.B. Vitányi, E. Kranakis, D.D.M. Krizanc, J.T. Tromp.

Univ. Amsterdam, Univ. Utrecht, Univ. Rochester, Univ. Washington, MIT, Harvard, York Univ., North-Eastern Univ., Boston Univ., Boston College, Technion.

Distributed systems

The research in this project is centred on the design and implementation of the distributed operating system Amoeba. This system consists of workstations, a processor pool, file servers and other specialized server machines, all connected through a fast local network. Research now focusses on two important fundamental problems: extensibility and fault tolerance. Development work concentrates on building an Amoeba system suitable for day-to-day work for the Open Software Foundation. (1980)

S.J. Mullender, C. Algeo, P. Bosch, J.-H. Bührmann, A.J. Jansen, K. Kim, G. van Rossum, I. Shizgal, S. van der Zee.

Free Univ. Amsterdam, Cambridge Univ.

Computer systems and ergonomics

This project is concerned with the methodology of integration of functions and applications in computer systems in order to provide end-users with easily manageable tools. There are two subprojects:

- ABC. The aim of this project is the design, implementation and distribution of a simple, structured, interactive programming language, built in into an integrated environment and meeting the requirements of modern personal computing. (1975)
- Human-computer interfaces (Views). The design and pilot implementation of a direct-manipulation, open-architecture, WYSIWYG, computing environment, where consistency of user-interface is guaranteed across applications. (1988)

S. Pemberton, K.T.L. Blom, H. van het Bolscher, E.D.G. Boeve, F. van Dijk, E.G.M. Embsen, L.J.M. Geurts, J.C. van der Heide, T.J.G. Krijnen, F. Lim, H.E. Lohuis, L.G.L.T. Meertens.

NGI section SAIA, Dutch Association for Ergonomics.

Distributed adaptive information systems

The development of software techniques and theory for the realization of flexible distributed information systems. (1985)

M.L. Kersten, A.F. Bakker, C.A. van den Berg, F.A. Bosman, K.C. Chan, M. Gathier, F.H. Schippers, A.P.J.M. Siebes, N.Th. Verbrugge, M.H. van der Voort.

Free Univ. Amsterdam, Univ. Twente.

Constructive algorithmics

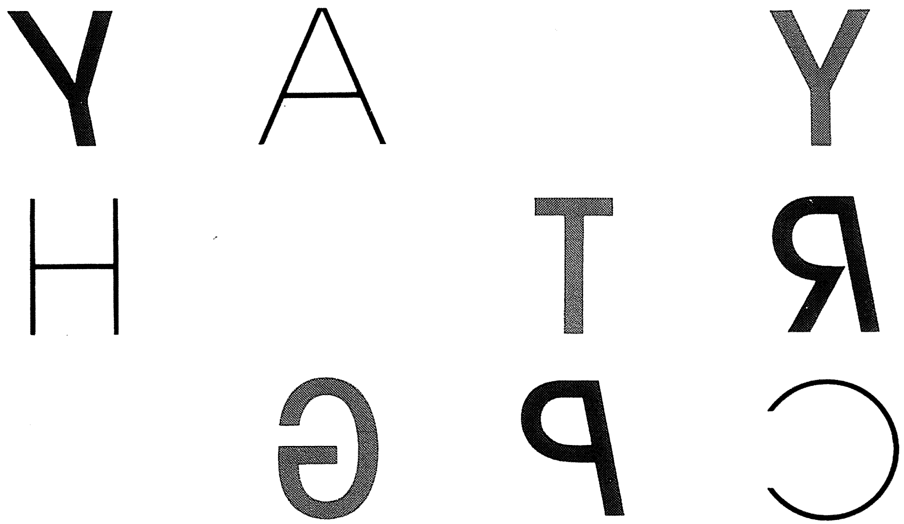
The development of formalisms and methods to derive algorithms from a specification, with unification of the specification formalism and the algorithmic formalism proper, and the development of (pre)-algorithmic concepts and notations on a high level of abstraction. The notion of 'algorithm' as used above comprises traditional computer programs, as well as process-defining system descriptions built in accordance with a recursive syntax from discrete basic elements. (1977)

L.G.L.T. Meertens, M.M. Fokkinga, J.T. Jeuring.
IFIP Working Group 2.1, Univ. Groningen, Univ. Nijmegen, Univ. Utrecht, Univ. Oxford.

Cryptology
The research in this project concerns all aspects of cryptology related to information security. This involves in particular the construction and analysis (from the points of view of crypto-analysis, information theory, and complexity theory) of cryptographic protocols and their underlying cryptographic algorithms, and the mathematical proofs of their soundness and reliability.
There is special emphasis on the protection of privacy of individuals in protocols for the transmission of messages, payment systems, and the treatment of personal data by various organizations. (1980)

D. Chaum (NFI), H. den Boer (NFI), J.N.E. Bos, M.J. Coster (NFI), E.J.L.J. van Heijst, A.G. Steenbeek (CWI - STO).

Univ. Rotterdam, Free Univ. Brussels, Univ. Michigan, Univ. Eindhoven, Univ. Freiburg, Cal. Tech. Pasadena.



Department of Interactive Systems

P.J.W. ten Hagen (head of department)
V. Akman
F. Arbab
P. Bernus
E. Blake
C.L. Blom
M. van Dijk
W. Eshuis
I. Herman
A.A.M. Kuijk
J.L.H. Rogier
M.M. de Ruiter
H.J. Schouten
P. Spilling
T. Tomiyama
C.G. Trienekens
P.J. Veerkamp
J. van de Vegt

programmer:
R. van Liere

trainees:
R.J. van Bavel
P. Booyen
R. Pieters-Kwiers
E.J. Weijers
R. Willemsen

ARCHITECTURES FOR INTERACTIVE RASTERGRAPHICS

Introduction

High resolution displays and fast interaction facilities are becoming standard features on today's desk-top workstations. The increased capabilities of such personal workstations gave rise to a more visually oriented communication via user interfaces. At the same time as these (two-dimensional) user interfaces have become a powerful tool, they are a significant drain on computing resources. It is quite foreseeable that the next generation of workstations will need even more demanding visualization facilities (e.g. rendering realistic images of three-dimensional objects which can be manipulated in real-time). Realistic images involve high resolution systems and advanced shading models including high quality illumination, distance attenuation, shadow casting and texturing. Rendering these images in real-time (typically < 0.1 sec) takes considerably more computing resources than offered by present day workstations. Even so, there is a growing need for such systems in areas like design, engineering, simulation and animation. With the above in mind a CWI research project aims at the design of a new workstation architecture including hardware for time-critical functions.

Rastergraphic architectures

Conventional rastergraphic architectures are based on a pipeline of processes which generate an image. Traversing the image generation pipeline takes longer than the persistance time of the phosphor of the screen (typically 10-60 milliseconds). For this reason, resulting colour values of individual picture elements (pixels) are stored in a 'frame buffer' from which a screen refresh process can be initiated (see Figure 1).

A cut in interaction response time is needed to make rastergraphics more interactive. This is generally pursued by speeding up the image generation pipeline. Given that a high quality image consists of about one million pixels, and interactions have to have a characteristic response time of 0.1 second, it is clear that adequate interaction support can only be achieved by multi-processor architectures. Based on the way the image generation process is partitioned and scheduled over the multi-processor system, one can distinguish three classes of partitioning:

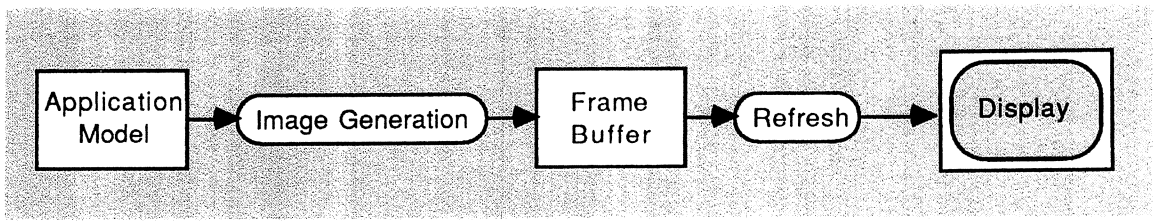
- image space subdivision: a processor allocated for each (block of) pixel(s);
- object space subdivision: a processor allocated for each graphical element (e.g. lines, characters, facets);
- functional subdivision: a processor allocated for each function (e.g. view transformation, clipping, shading) in the image generation pipeline.

It is not obvious which of the three classes of partitioning is best suited for interaction; a study of interaction mechanisms was needed to establish this.

Interactions

An important question has to be answered: which functional elements of the image generation pipeline are needed for interactions? Figure 1 shows that interactions which only manipulate the frame buffer would be fastest,

Figure 1: Conventional rastergraphic architecture. An image generation pipeline converts the application level description to an image represented by individual pixels stored in a frame buffer. This pixel representation is used for the refresh process.



as this would not necessitate execution of any pipeline function. On the other hand, interactions manipulating the application model require at least the pipeline traversal time, as all pipeline functions must be executed.

An inventory of manipulations which ought to be handled by an interactive system was made in order to discover from which image representation levels it would be possible to initiate the pipeline interactions. This produced the following three levels:

- visible parts of objects;
- objects or groups of objects;
- the entire image.

Note that interactions operating on individual pixels do not occur. A further outcome of the inventory was that these levels also showed some relation with the complexity of the interaction from the user point of view. In general, interactions on the entire image are more complex than interactions dealing with visible parts of objects only. During the quest for a suitable architecture it became clear that the following aspects of interaction also had to be considered and exploited:

- interactive changes are typically incremental, i.e., an existing value is changed;

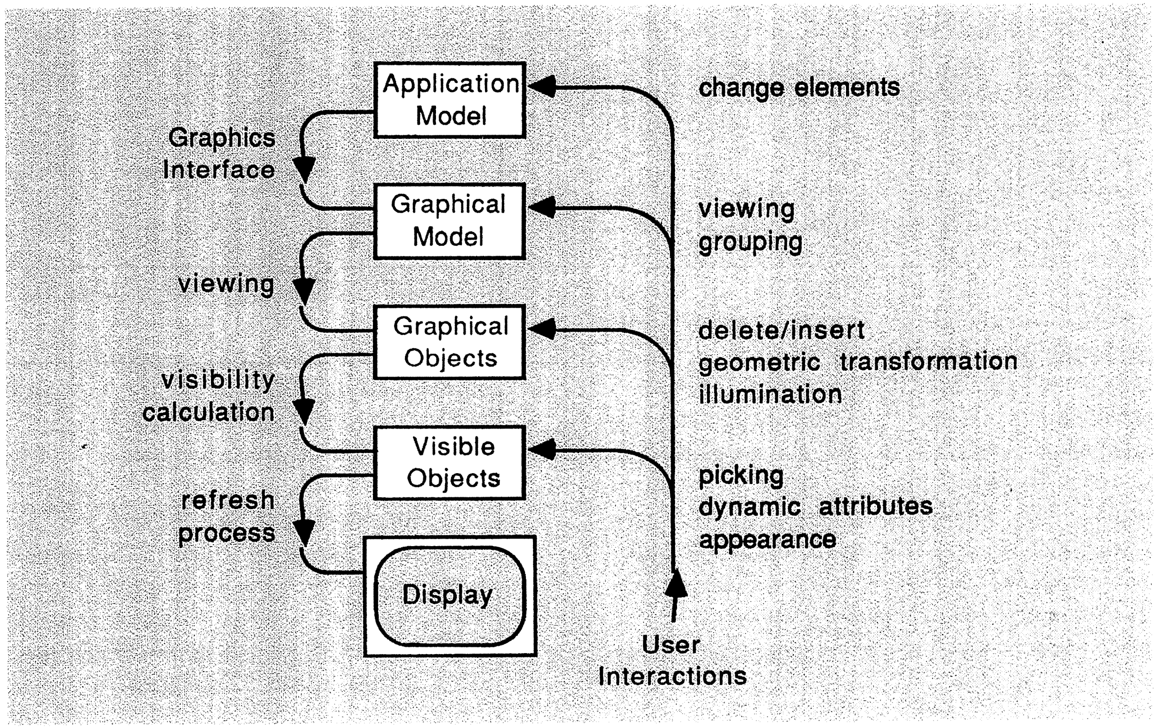


Figure 2: An architecture for interactive rastergraphics. For interaction purposes, three levels of display files are exploited. Functional elements perform the mapping processes between successive representation levels. For each type of interaction is indicated on which level it can be initiated.

- a frequent property of interaction is locality: changes only affect a small part of the image;
- global changes may well be a change to a single aspect.

A new architecture

The aspects of interactions as listed above determine the structuring of a display file. This is a data structure in which the information needed to generate the image is stored. We concluded from the inventory of changes, that three levels of display files should be accessible for interaction purposes. Based on this we arrived at the global architecture as shown in Figure 2. In order to drive the display controller which handles the screen refresh process, the application model is progressively processed in a number of steps which all provide facilities for interactive modification. These steps are performed by functional elements. In the mapping process of the graphical model on the graphical objects all original graphical elements are mapped on to just one single type of graphical 'primitive'. This primitive, called a 'pattern', consists of a domain as well as a colour description. One of the steps mentioned above is a new hidden surface algorithm which was developed to produce a low level display file of the visible graphics primitives only. Typical features of this algorithm are:

- it operates in object space; input as well as output are primitives of the same kind;

In recent years the field of image synthesis has been dominated by two factors: visual realism and interactivity. Within this context, novel algorithms are being developed which allow for illumination to be computed in real time. The figure shows an example of the type of images which could possibly be rendered in real time. Note the interreflection of the objects in the image. The illumination model being applied here is based on radiosity and uses energy equilibrium as the underlying physical principle. The model demands great computational and storage resources. However, the ongoing fall in the cost of realizing advanced workstation architectures and improved performance, should make variants on this model quite common.

- it can handle incremental operations, i.e. objects can be added or removed without having to recalculate the whole image;
- it can handle transparent objects.

The following aspects of this architecture are worth noting. The architecture is a hybrid system. Globally speaking it is a functionally subdivided system; but at a more detailed scale, where needed, object space subdivision and even image space subdivision are also performed. An example of this will be discussed in the next section. Changes can be initiated on the lowest level possible, thereby reducing the computations needed and thus optimizing the performance. This goes well with the above mentioned relation of interaction complexity and representation levels: a user will expect immediate response for simple interactions, whereas for complex interactions requiring initiation from a higher representation level, more relaxed response times are acceptable (although within seconds rather than in minutes). The display file from which the screen refresh process is initiated is a structured representation of the image, built out of graphics primitives. This is a remarkable difference with conventional frame buffer systems which, at the lowest level, store raw pixel data. As no interactions work on individual pixels, there is no need to have access to such a low level representation. All pixel-related operations are handled by the display controller.

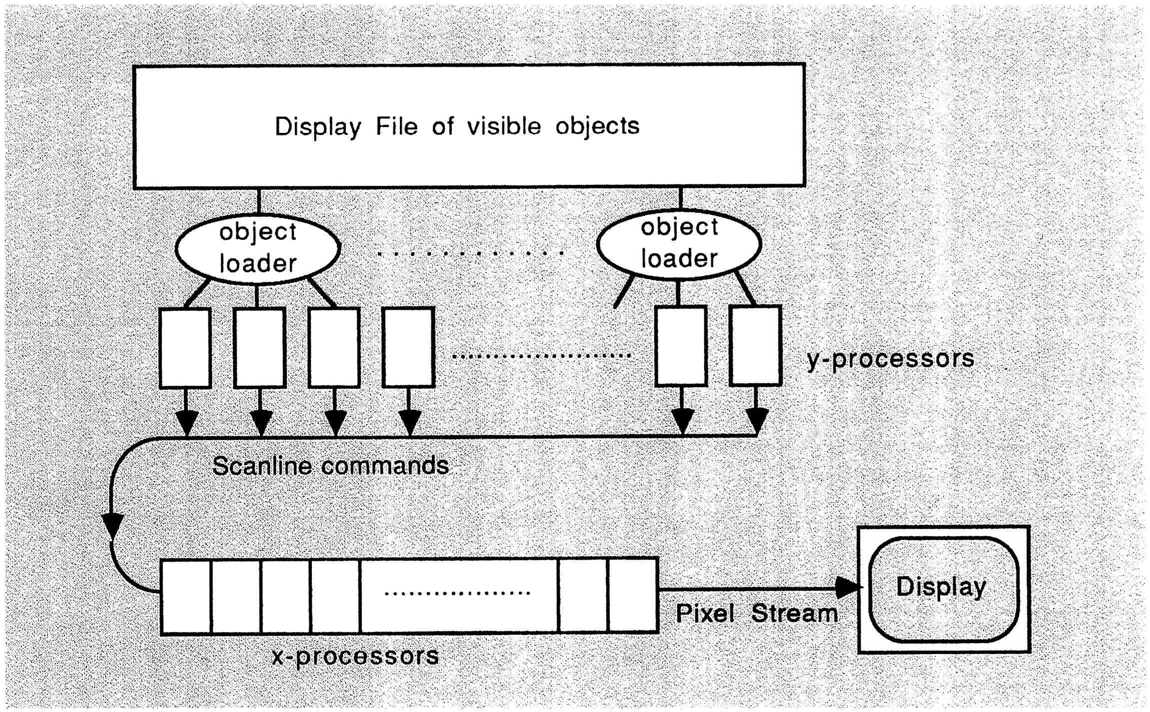


Figure 3: The Display Controller. Object loaders are assigned to load all active objects on a scanline in the y-processors. With each incremental step in y-direction, these y-processors issue scanline commands containing the shading information for the systolic array of x-processors. This array, which has as many processors as there are pixels in a scanline, produces the pixel stream.

The display controller

Technically, the most demanding element of the architecture is the display controller. It has to scan, convert and shade the graphical primitives at a refresh rate of about 60 Hz. This could only be performed by a well-partitioned multiprocessor system. The design of the display controller was a joint effort by CWI and the University of Twente. The refresh process generates a video signal containing pixel intensity information. The order in which the pixels are scanned (per horizontal scanline) already leads to a subdivision of the refresh process in vertical (y) and in horizontal (x) direction. The high scan frequency of the pixels in the x-direction can be handled by a systolic array of processors. This is an example of image space subdivision, each vertical pixel column is assigned to a processor from the array. Information for this systolic array is provided by an array of processors which scan primitives in the y-direction. In that these processors operate on one active primitive at a time, we have here an example of object space subdivision. The resulting hybrid display controller (see Figure 3) can be scaled according to the specifications. The number of x-processors can be adapted to obtain the desired resolution of the system, whereas the number of y-processors can be adapted to the desired complexity of images to be displayed. For implementation of the display controller, full-custom VLSI chips are needed. These will be designed by the University of Twente.

PROJECTS

The following information is given for each project: a short description, the start-up year, research staff (project leader in italic) and cooperating institutions.

Computer graphics
The design of functionally complete basic graphics systems, with special support for interactive use. Results to be made available, on the one hand as (contribution to) international standards, on the other hand as implementations, again with special attention to efficiency required for high quality interaction. (1980)

A.A.M. Kuijk, I. Herman, M. Bakker (CWI-STO), E. Blake (STW), P. Booyen, F.J. Burger (CWI-STO), M. van Dijk, B.P. Rouwhorst (CWI-STO), C.G. Trienekens (STW).

Techn. Univ. Eindhoven, Techn. Univ. Delft, Univ. Twente, TNO-IBBC, ECN, MARIN, ACCU, ISO-working group TC97/SC21/WG5-2, Dataflow Technology Nederland BV, Parallel Computing, Philips, Systeem Experts, Hoogovens, Techn. Hochschule Darmstadt, INRIA Paris, Rutherford Labs Abingdon, George Washington University.

User interfaces
Information systems should be addressed in high level, natural user languages. The user interface is then to provide the mappings between the user language and the abstract system concepts. Attempts are being made to enrich user languages by supporting speech-recognition and -generation, natural language instructs and picture elements (e.g. sketches). This project focusses on picture interpretation. This is a new area. The major difference with computer vision is that with picture interpretation the computer is actively involved in the picture construction process. The emphasis therefore is on correlating pictures with other information. (1984)

M.M. de Ruiter, C.L. Blom, P.J.W. ten Hagen, R.J. van Bavel, J. van de Vegt, R. Willemsen.

PTL Groningen, TNO-IBBC, Univ. Twente, Techn. Hochschule Darmstadt, Rutherford Labs Abingdon, GMD St. Augustin.

Dialogue programming
The project is aimed at the development of a complete programming method for interactive dialogues. According to this method dialogue programs will be written which specify the syntax of a dialogue language for a given application. In addition the dialogue program also determines all external effects associated with this syntax, such as the specification of all input-output procedures and the associations with application processes. (1983)
P.J.W. ten Hagen, M. van Dijk, W. Eshuis, H.J. Schouten, R. van Liere, D. Soede (CWI-STO).

TNO-IBBC, NLR, Océ, Philips, Univ. Amsterdam, Techn. Hochschule Darmstadt, Univ. Tokyo.

Intelligent CAD systems
The project will, through the use of AI-based methods and techniques, attempt to produce CAD-systems which will be more complete, integrated and have a high quality user interface. (1985)

V. Akman (NFI), F. Arbab, P. Bernus, P.J.W. ten Hagen, R. Pieters-Kwiers, J.L.H. Rogier, T. Tomiyama, P.J. Veerkamp (NFI).

TNO-IBBC, Univ. Tokyo, Helsinki Univ. of Technology, Computer and Automations Institute Budapest, Univ. of Southern California.

User controlled systems
User controlled systems are information systems in which databases and program libraries are integrated. This type of systems is needed for making the various autonomous components of a complex computer system cooperate (for instance, a complete design and manufacturing system). With this technology it is hoped to realize CIM (computer integrated manufacturing). (1987)
W. Eshuis, P.J.W. ten Hagen, D. Soede, P. Spilling.

TNO, Univ. Twente, TH Darmstadt.

D.C.A. Bulterman (head of department)
P. Beertema
D.F. Karrenberg
E.S. Mullender
D.L. Draper
M. Carrasquer

programmers:
J.N. Akkerhuis
E.P. Gronke
R. ten Kroode
F. Kuiper
C. Orange

EUROMATH

Euromath started up in 1987. It is an international project, initiated and monitored by the European Mathematical Trust, and sponsored by the European Commission. The aim is to stimulate the research potential of European mathematicians by creating a research environment, the Euromath system, based on modern information technology specifically adapted to the needs of the mathematical community. CWI is one of the technical partners in the project with main responsibility for the functional design of the Euromath system.

Aims

Information technology can serve to improve the preparation of mathematical documents, to provide highly efficient means of communication between research scientists, and to make information relevant to research, such as bibliographic databases, more readily available and accessible. Such services exist already, but absence of standards, lack of integration between different services, and low awareness among software designers of issues important to mathematicians, all conspire to make them unnecessarily cumbersome in use. And so, much of information technology's potential remains unfulfilled.

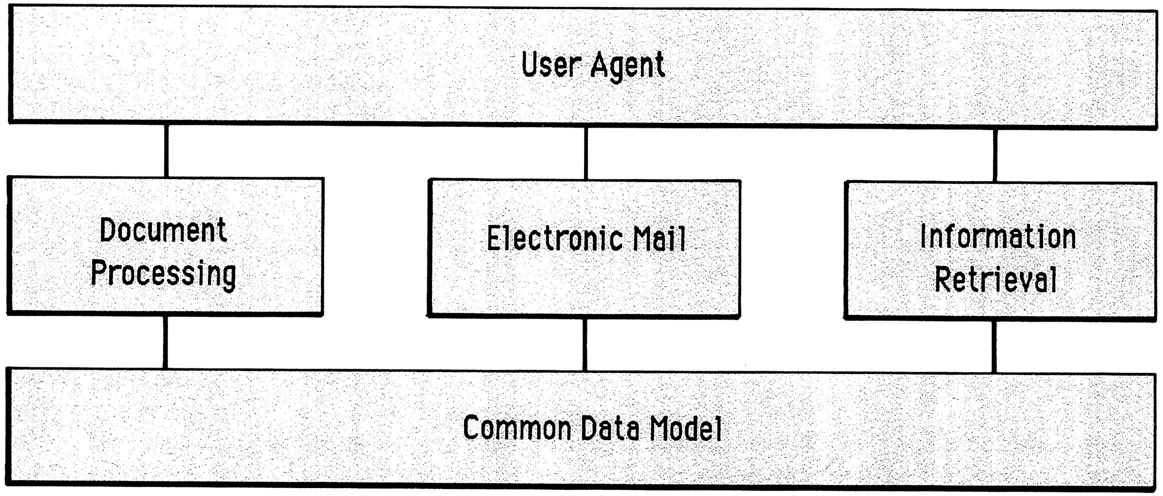
Even so, an appropriately designed research environment could offer substantial advantages to the working mathematician. In addressing this issue, Euromath aims to increase the rate of progress of mathematical research within Europe, and to improve significantly the availability and interchange of the results of that research. Throughout the project emphasis is put on achieving this aim by providing integrated interfaces between the facilities needed by mathematicians.

Among features contributing to success will be a high level structure facilitating the handling of all entities - including mail messages, mathematical papers and document folders - going via the Euromath system. Internal representation will be based on a common Euromath standard, making it possible to use information from one type of entity in another type of entity without the worry of format conversions. The meaning of - and relationships between - various entities will be dealt with by the system itself in a way transparent to users. This extends to the exchange of information between Euromath users at different sites.

This fact, as well as a user interface design based on Direct Manipulation with a very limited but powerful set of commands, will make the system easy to use. Hence, it will be possible to import information obtained from a database literature search directly into a mathematical paper, with only two or three keystrokes, and regardless of any discrepancy between the format as stored in the database and the desired final form of presentation for bibliographic references when the paper is printed.

Like all presentations, the style in which references in papers are shown can be customized, both in advance and later, according to user preference. Such references, and indeed any other type of information, can just as easily be incorporated in a mail message to a fellow researcher, and the receiving installation will recognize the type of information and treat it appropriately.

One will also be able to mix tasks arbitrarily. So, it will be possible to perform a database search while composing a document, start



A global view on the Euromath system

sending a mail message to another user during that database search, interrupt that to finish first the database search, continue with the mail message, and read any incoming mail in between.

Euromath will allow mathematicians to use the full strength of modern information technology with no distraction from the actual purpose of their work: the application and development of mathematical knowledge. Ultimately, operating the Euromath system will be almost as simple as working with pencil and paper - but with a tremendous increase in potential benefit. Notably, by creating a common European context for mathematical research, Euromath will provide a basis for maintaining, and improving, the high quality of that research within Europe.

Some technical aspects

The overall technical objective of Euromath can be seen as the definition and implementation of an integrated environment to provide the mathematical community in Europe with an open, extendible set of services in the field of information technology. Integration of the user's environment means two things.

Firstly, the user accesses the various services in a uniform manner, instead of having to use a different user interface for each service. To achieve this, the various basic services will be accessed through a common channel, called the user agent. All interaction of the user with the system is handled via this user agent; it interprets the operations requested by the user, directs them in appropriate form to the appropriate service(s), collects the results, and presents these to the user.

Secondly, integration means that results of one service can be used in another service without the usual problems caused by incompatible data formats. This requires that the various services understand the same representation of the various mathematical and other entities in the Euromath system. To make this possible, a common data model is defined, shared by all services.

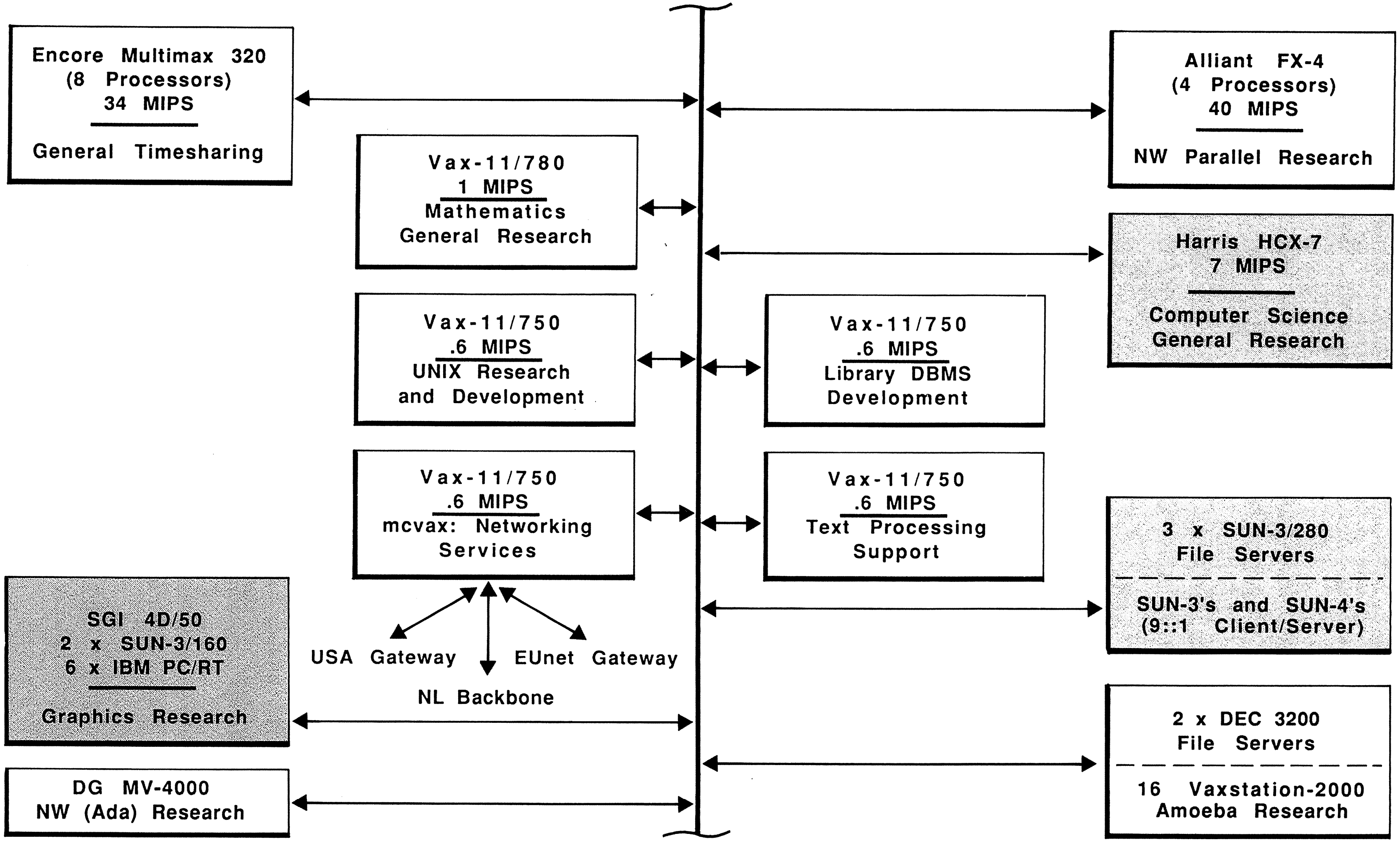
The general structure of the Euromath system is consequently based on two internal interfaces, which together define the standards with which all services must comply: on the one hand the interface for the communication between the services and the user agent, and on the other hand the common data model, defining the access to the entities processed and stored in the system. Not only will the transparent interchange of results be possible between different services within one user's installation of Euromath, but also via the interpersonal communication service, between Euromath users. When a Euromath document is transmitted to another Euromath user, or submitted to an electronic Euromath conference, information describing the document type is transmitted with it as an inseparable part. Thus, the receiving system will be able to interpret and handle the document appropriately without requiring separate user intervention. This is obviously not possible for mail to non-Euromath users, or submissions to existing non-Euromath conferences. In such cases, the additional Euromath-specific information will be stripped, and the remaining information transformed (to the extent possible) into a human-readable ASCII form.

Among the future services that may be integrated with the Euromath system are facilities for computer algebra and other forms of symbolic manipulation. This is currently under consideration. The interfaces on which the general structure of the system is based will already contain the necessary provisions for such an extension. If such facilities are added, it will, for example, become possible to perform symbolic manipulations on formulae contained within any Euromath document.

User interface

To achieve the uniformity required for integration, a unifying model has been developed for the interaction between the user and the system. This approach was adopted from the research results of the CWI project 'Human-Computer Interfaces' (department of Algorithmics and Architecture). The model is that of the user agent as a generalized editor, the meaning of whose operations is defined in terms of the structure of the entities with which it is dealing. Every entity in the Euromath system can be viewed as a (generalized) document with a structure. Not only can standard mathematical documents be seen in this way (structured into chapters, sections, formulae, references, ...), but also mail messages, collections of documents like folders, mailboxes and conferences, and databases. An editor is a facility that can be used to create, view, search and modify documents. Consequently, a generalized structure editor can provide an appropriate and unified facility for handling entities within the Euromath system. Moreover, the editor is tailored to each particular service for which it is used in the sense that the editor (being the user agent) 'drives' the service by the structure of the document it manipulates. For example, on textual documents edit operations like 'delete', 'copy' and 'paste' can be used to delete, copy or move words or other textual elements. The same edit operations can be used on a folder of documents to delete, copy or move entire documents, and in order to post a message, the 'paste' command can be applied to the mailbox of outgoing letters. A window manager allows the Euromath user to view and even edit different documents (and therefore use different services) simultaneously. This means that it is extremely easy to interrupt an ongoing task for a new one, and to resume the original task at any later time, even if the new task is not yet finished. The traditional notion of applications that are 'entered' and 'quit' entirely disappears in the model developed for the Euromath user interface. Future services to Euromath can be added in the form of new document classes and also in the form of new edit operations on entities of existing classes. For example, 'formula' will be one of the standard Euromath classes, and a symbolic manipulation facility can then be introduced by the addition of specialized 'edit operations' on formulae.

CWI Computing Equipment Resources
(as of December 31, 1988)



PROJECTS

The following information is given for each project: a short description, the start-up year, research staff (project leader in italic) and cooperating institutions.

Networked document retrieval and manipulation

EUROMATH - a CODEST project monitored by the European Mathematical Trust - is aimed at investigating the retrieval and manipulation, with an integrated user interface, of mathematical documents residing in local, national and international databases throughout European countries. The EUROMATH project consists of a number of components, including mechanisms for database access, communication, text formatting and text processing. (1988)

L.G.L.T. Meertens (CWI - AA), M. Carrasquer, D.L. Draper, D.F. Karrenberg, S. Pemberton (CWI - AA).

NIHE Dublin, DDC Lyngby, FIZ Karlsruhe. Overall project direction is monitored by the European Mathematical Trust (EMT).

Internet/ISO protocol development

As the desire to communicate electronically among researchers within Europe (and world-wide) increases, it becomes important to expand the reach of individual computer networks. The Internet/ISO protocol development project is aimed at realizing this goal by investigating means of implementing protocols and protocol converters which will allow user-level network traffic to be routed between networks that support varying protocols. In particular, this project is aimed at providing protocol translation facilities between Internet protocols (primarily RFC-822) and ISO protocols (X.400) for message and mail traffic. (1988)

D.F. Karrenberg, P. Beertema.

University College London, Nottingham Univ., RARE, other network members (EARN, EUnet, Janet).

Network-based job entry and performance monitoring

The Networked Execution Server (NES) project is aimed at studying the use of a collection of compute server computers in a coordinated manner for remote execution (and parallel execution) of user programs in a workstation-oriented environment. In particular, three aspects are studied:

- Task Allocation and Resource Sharing within a network of compute server, compute client, and monitoring computers;
- Communications Structures for supporting high-speed communication, possibly including hardware interconnection issues and hardware/software protocol issues;
- User Interfaces for graphically defining execution streams as collections of user-defined and system-defined components located across the network, and for displaying the status of both the execution stream and the system as a whole in user- and system-defined forms.

The work is constrained by the desire to use existing communications equipment where practical (i.e., Ethernet), although not necessarily existing network communication protocols. (1989, preparations made in 1988)

D.C.A. Bulterman, D.F. Karrenberg, E.S. Mullender.

Brown University, Encore Computer Corporation.

General
CWI's Policy Document 1988-1993 goes into some detail on three significant aspects of SMC's statutory aims vis-à-vis CWI: conducting excellent research, the promotion of knowledge transfer and expert training, and the function as international meeting point. The first aspect remains by far the most important. However, attention devoted to the others in recent years has grown apace: in part this is due to CWI's increased emphasis on strategic and application-oriented research, and on applied research and development. A grant from the Dutch government's Information Technology Promotion Plan (INSP) provided the basis for this broader approach. The additional funds helped put CWI in a position to take part in programmes such as ESPRIT, RACE, SPIN, IOP, etc.; this participation in turn produced income approximately equal to the original INSP grant. (For CWI income development during recent years see the diagrams in the chapter Financial Data.) There was, however, a less rosy side to the picture. Particularly in CWI's computer science departments there was a serious loss of equilibrium with contract research booming at the cost of pure scientific activities.
Termination of INSP-funds at end 1988 motivated CWI to organize the National Workshop on Strategic Research in Computer Science and Mathematics in September. Focal point in the discussions was the problem of knowledge transfer. An evaluation report on INSP, commissioned by the government and published in June, had stated that, in general, the attitude of Dutch research institutes towards transferring their research results to other sectors of society was still too passive. However, CWI is alert to this problem, and has devoted special attention to it in recent years. We recognize that selection of excellent researchers has to be matched by excellence in diffusing their results. One method we are currently exploring is to carry out research in programmes, or with partners, with an existing, automatic knowledge transfer mechanism. At the workshop it was emphasized that CWI should, at the very least, maintain its traditional - and still highly efficient - method of knowledge transfer: training researchers who will eventually join universities, industry, etc. A more systematic exchange of researchers with industry would be highly desirable. Some industrial representatives, including the software sector, stressed the importance of the very existence of institutes for fundamental research like CWI in their direct vicinity. However, they felt there was room for further improvement in attuning CWI's research programme to industry-oriented strategic goals.

GMD-INRIA-CWI
The single most important development in international relations during 1988 was the closer cooperation between GMD (West-Germany), INRIA (France) and CWI. Research contacts with INRIA developed further in a 'twinning' workshop, held at INRIA's Centre Sophia-Antipolis in March, as part of a separate Franco-Dutch scientific cooperation programme. Sponsorship came from the French Foreign Ministry and the Ministry of Research and Higher Education, and the Dutch Ministry of Education and Science. Twenty-five INRIA researchers and eleven from CWI participated. The workshop considered three themes for closer cooperation: performance evaluation, and control and system theory; scientific and industrial computation; and databases.
The first joint workshop involving all three partners was organized at CWI in November; with more than 100 researchers participating it proved a great success. The research themes discussed were: scientific computing, theoretical and pragmatic issues in programming, and man-machine communication. A common policy document, to be finalized early in 1989, will define joint research projects, an important guideline being 'more quality by complementarity'. Possible programmes for scholarships and for advanced training were also discussed. The next meeting, to be organized at GMD, will take place in April 1989.

Research contracts
In 1988, CWI became prime contractor in the RIPE project (RACE Integrity Primitives Evaluation). RIPE is part of the European Community's RACE programme (R&D in Advanced Communications-technologies in Europe), which aims to pave the way towards commercial use of Integrated Broadband Communications (IBC) in Europe by 1995.

Forum discussion on the first day of the National Workshop on Strategic Research in Computer Science and Mathematics. Knowledge transfer was a central issue at this event organized by CWI at Noordwijk-on-Sea in September. The approximately sixty participants came from industry, government, major technical institutes and universities.

RIPE will put forward a package of techniques to meet IBC's anticipated security requirements. The other consortium members are: Siemens AG, Philips Usfa BV, The Netherlands PTT Research, and the Universities of Leuven and Aarhus. A representative example of the various ongoing contract research at CWI is the *Multigrid for Hermes* project. This comes under Avions Marcel Dassault - Bréguet Aviation's aerothermodynamics programme, which started mid-1987, and is part of the European Space Agency's Hermes space shuttle project. It examines the applicability of a geometrical multigrid method for the solution of two-dimensional stationary Euler equations, with special attention to flows around airfoils at high Mach numbers and high angle of attack. After extension to a steady full Navier-Stokes method, a further convergence improvement and extension to hypersonic speeds were investigated in 1988.

Central role

One of the means of knowledge transfer particularly suited to a research institute with a central function is the organization of conferences, symposia, workshops, courses, etc. Highlights of this work during 1988 are summarized in the Introduction. However, one project at least deserves coverage here. The particular aim of the *Planning and Control in Traffic* symposium was to examine fields of application where CWI's potential in fundamental research could make a meaningful contribution. Subjects treated at the symposium included equilibrium theory in traffic networks, 3D-assignment in the time-space for overloaded networks, the Eureka project CARMINAT, and stochastic models for road traffic. CWI plans to organize similar symposia on a more regular basis.

Involvement in certain scientific organizations is another part of our central function. CWI was a major party in supporting the foundation of CAN: the Stichting Computer Algebra Nederland (Dutch Computer Algebra Foundation). CWI's role in CAN will continue as coordinator for use of the government's grant

```
LiE       version 1.0
Authors:  Arjeh M. Cohen, Bert Lisser, Bart de Smit, Ron Sommeling

          type '?' for information
          type '?functions' for a list of functions.

          > diagram(A12E8D14)

          O---O---O---O---...---O---O---O---O
          1   2   3   4         9   10  11  12
          A12
                  O 14
                  |
                  |
          O---O---O---O---O---O---O
          13  15  16  17  18  19  20
          E8                             O 33
                                         |
                                         |
          O---O---O---O---...---O---O---O---O
          21  22  23  24        30  31  32  34
          D14

          >quit
```

In 1988 CWI's Computer Algebra project saw development of the **LiE** *package for the analysis of Lie groups. In this very small session in* **LiE** *the Dynkin diagram of a Lie group of type* $A_{12}E_8D_{14}$ *is printed.*
Computer algebra has become an important tool for the mathematician to perform symbolic manipulations like evaluation of complicated polynomial expressions, differentiation and integration by computer. Starting in 1989, CWI will host a government-sponsored national expertise centre in computer algebra.

for equipment and manpower. CAN aims to offer centralized national facilities and services to researchers and users of computer algebra. In fact CWI is more than a coordinator here: in 1988 computer algebra became part of a project in our department of Algebra, Analysis & Geometry.
The Open Software Foundation OSF was founded in May 1988 by a consortium of nine major computer manufacturers: IBM, DEC, Apollo and Hewlett-Packard in the USA; Siemens, Nixdorf, Bull and Philips in Europe; and Hitachi in Japan. OSF aims at developing system software for its members (any company, university or research institute can join). There will be OSF institutes for research, development and marketing in both the USA and Europe. OSF also has Academic and Industrial Advisory Boards. CWI participates in the European Academic Board.

Finally, we summarize the various large-scale national and international joint projects.

CWI Participation in (Inter)National Programmes
The following data are given for each project:
- title,
- period,
- cooperation with other institutes,
- CWI project leader(s).

European Programmes

ESPRIT

METEOR (432): An integrated formal approach to industrial software development
October 1984 - October 1989
Philips (PRLB, PRLE), CGE Paris, AT&T/Philips, COPS, TXT, Univ. Passau
J.A. Bergstra

GIPE (348): Generation of Interactive Programming Environments
November 1984 - November 1989
INRIA, SEMA, BSO
P. Klint

415: Parallel architectures and languages for AIP - a VLSI directed approach
November 1984 - November 1989
Subcontractor of Philips
J.W. de Bakker

DIAMOND (1072): Development and Integration of Accurate Mathematical Operations in Numerical Data processing
January 1986 - January 1989
NAG, Siemens, Univ. Karlsruhe
J. Kok

VIP (1229(1283)): VDM Interfaces for PCTE
November 1986 - November 1988
Praxis, Dr. Neherlab. PTT, Océ, Univ. Leicester
J.A. Bergstra

RACE

RIPE: RACE Integrity Primitives Evaluation
November 1988 - April 1992
Prime contractor
Other consortium members: Siemens AG, Philips Usfa BV, The Netherlands PTT Research, Universities of Leuven and Aarhus
D. Chaum

SPECS (1046): Specification and Programming Environment for Communication Software
January 1988 - January 1993
Subcontractor of Dr. Neher lab. PTT
F.W. Vaandrager

Other programmes

ESA project HERMES: Convergence acceleration of a finite volume Euler solution with a geometric and algebraic adapted multigrid method in finite volume Euler solutions
July 1987 - July 1989
P.W. Hemker

CODEST project EUROMATH: The integrated database and communications system for European mathematicians
January 1988 - June 1989
DDC, EMT, NIHE
L.G.L.T. Meertens

National Programmes

SPIN (Stimulation Project Team Computer Science)

PRISMA: Parallel Inference and Storage Machine
October 1986 - October 1990
Philips (main contractor), Universities of Twente, Utrecht and Amsterdam
M.L. Kersten/P.J.F. Lucas

FLAIR: Flexible automation
January 1987 - January 1991
Univ. Twente
P.J.W. ten Hagen

SION (Netherlands Foundation for Computer Science)
National Concurrency Project
May 1984 - February 1989
Techn. Univ. Eindhoven, Univ. Leiden
J.W. de Bakker

NFI (National Facility Computer Science)

Design methods for decision support systems
September 1985 - September 1989
Technical Univ. Delft, Technical Univ. Eindhoven, Erasmus Univ. Rotterdam
J.K. Lenstra

REX: Research and Education in Concurrent Systems
January 1988 - January 1993
Technical Univ. Eindhoven, Univ. Leiden
J.W. de Bakker

Transformational programming
Jaunuary 1988 - January 1993
Univ. Nijmegen, Univ. Utrecht
L.G.L.T. Meertens

Cryptography and computer security
September 1984 - September 1990
D. Chaum

Intelligent CAD systems
October 1986 - October 1990
TNO/IBBC
P.J.W. ten Hagen

STW (Foundation for the Technical Sciences)

Two-dimensional time-dependent Boussinesq model
August 1988 - July 1990
P.J. van der Houwen, F.W. Wubs (RUG)

Statistical analysis of traffic flows
April 1986 - April 1990 (until August 1988 at CWI)
Univ. Amsterdam, Technical Univ. Delft
P. Groeneboom

Prediction and control problems for the Dutch freeway control and signalling system
January 1986 - January 1990
Univ. Twente
J.H. van Schuppen

Overload control for communication systems
February 1986 - February 1990
Philips Telecommunication, Univ. Twente
J.H. van Schuppen
Adaptive grid techniques for evolutionary partial differential equations
September 1987 - September 1990
Shell
J.G. Verwer
New architecture for interactive raster graphics on the basis of VLSI
April 1987 - April 1990
Univ. Twente
P.J.W. ten Hagen

IOP (Innovative Research Programmes)

IC-Technology: numerical methods for semiconductor device modelling
October 1987 - October 1989
FOM, Technical Univ. Delft, Philips CAD-Centre Eindhoven
P.W. Hemker

Shell fellowships

Mixed integer programming models for distribution and production planning
November 1987 - November 1989
Shell Research
J.K. Lenstra

Inverse scattering and image processing of seismic data
January 1988 - January 1990
Shell Research
J.H. van Schuppen

Supporting Sectors

CWI support staff are organized in five sectors: Library & Information Service, Computer Systems & Telematics, Research Management & Presentation, Social-economic Affairs, and Technical Support. Computer Systems & Telematics is developing into a more research-oriented unit, hence its activities are presented together with the scientific departments. The responsibilities of Social-economic Affairs include CWI finance and personnel; the relevant data are also presented in a separate chapter. Most of Research Management & Presentation activities have been covered in the Introduction and the chapter on Knowledge Transfer, Co-operation & Central Role. These include organization of conferences and workshops, development of documentation (policy documents, annual reports, etc.), science information for a broad public, knowledge transfer to industry and other groups, legal support in connection with contracts, international relations, and the management of SMC's National Working Communities in mathematics. All that remains is for this chapter to present a brief overview of the activities of the two remaining sectors, the Library & Information Service and Technical Support.

Library & Information Service

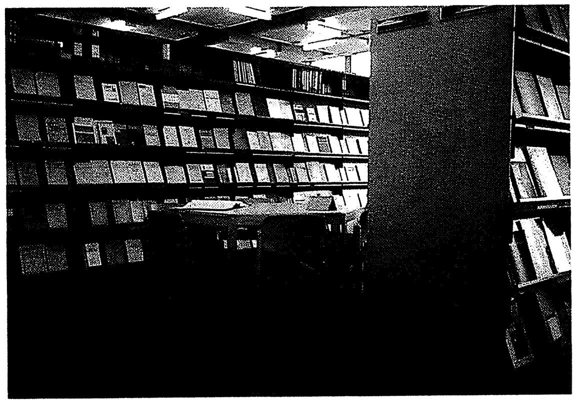
The Library and Information Service provides direct support for scientific research activities. Considerable effort over the years has resulted in an excellent and extensive collection of books, periodicals and reports (see chart). The library is of national importance and the collection is frequently consulted by other institutes - from home and abroad. This is in line with CWI's aim to fulfill a central function. Frequent exchange contacts with foreign institutes are an important factor in building up the collection. The library also houses the Dutch Mathematical Society's collection of periodicals.

Library: accretion

	1985	1986	1987	1988
books	1120	1070	1215	1176
subscriptions on journals	67	87	61	72
reports	5455	5891	6566	6873

Library: collection ultimo 1988

books	34820
subscriptions on journals	1309
reports	68780



Initiatives were undertaken in 1988 to improve retrieval of on-line literature from external databases via hosts like Dialog, ESA and STN. Third-parties can now also use this type of service.

A start was recently made on providing interactive on-line access to the library catalogues. The collection's potential deserves faster, more advanced retrieval methods. Here too, interest extends beyond CWI - once again underlining the library's central role. Hence, it is planned to extend these facilities to outsiders, e.g. via networks.

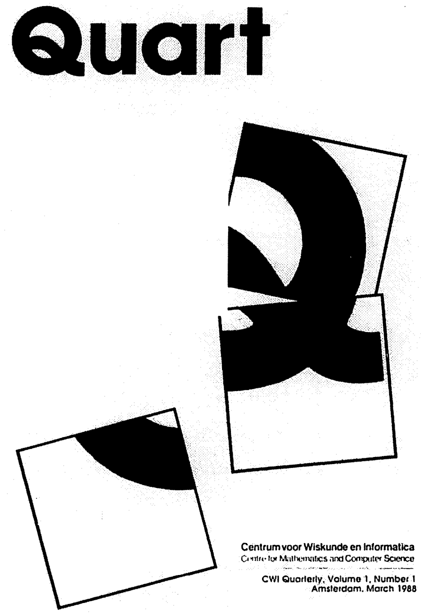
The library is not immune to CWI's chronic shortage of space; and steps are underway to maintain the major collection of international research reports by transfering a proportion onto microfilm. The library's AGFA LKI6-B microfilm reader will provide fast retrieval and print-out facilities.

Technical Support

This sector operates in two different areas: programming and publishing. The programming support concentrates on internal CWI activities. Technical Support participated in

CWI Monographs

nr.	*Title*	*Authors/editors*
1	Mathematics and Computer Science Proceedings of the CWI Symposium, November 1983	J.W. de Bakker, M. Hazewinkel and J.K. Lenstra, editors (1986)
2	Stability of Runge-Kutta Methods for Stiff Nonlinear Differential Equations	K. Dekker and J.G. Verwer (1984)
3	The Numerical Solution of Volterra Equations	H. Brunner and P.J. van der Houwen (1986)
4	Mathematics and Computer Science II Fundamental Contributions in the Netherlands since 1945	M. Hazewinkel, J.K. Lenstra and L.G.L.T. Meertens, editors (1986)
5	One-Parameter Semigroups	Ph. Clément, H.J.A.M. Heijmans, S. Angenent, C.J. van Duijn and B. de Pagter (1987)
6	Program Correctness over Abstract Data Types with Error State Semantics	J.V. Tucker and J.I. Zucker (1988)
7	Queueing Theory and its Applications Liber Amicorum for J.W. Cohen	O.J. Boxma and R. Syski, (editors) 1988

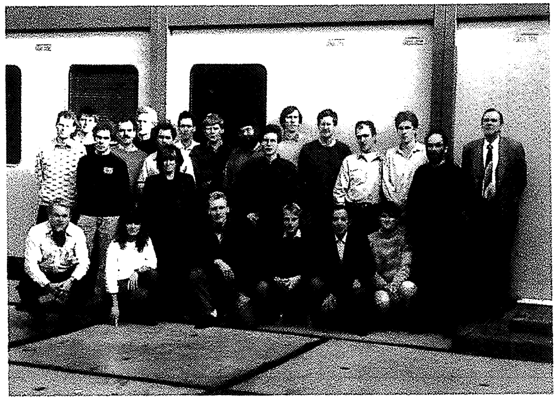


Publications

	1985	1986	1987	1988
syllabi	4	3	3	7
tracts	6	12	14	12
reports	94	108	142	140
publications in journals, proceedings, etc.	129	146	125	174
Ph.D. Theses	5	0	6	4

various research projects including the development of a numerical program library in Ada, cryptography applied to an electronic payment system, the symbolic manipulation software package LiE developed at CWI, computer graphics (in particular work on a highly advanced graphics system based on dataflow processors) and the interactive software packages S (data analysis and statistics) and Z (image analysis). Attention in the field of office and library automation focussed on further development of the relational database management system INGRES, with the emphasis on library applications. External programming commissions are still accepted, but manpower available for this will gradually reduce. In 1988 Technical Support carried out eight larger projects for research institutes, government institutions and industry. Computer services and support concentrated on CWI staff use of the internal computer systems (UNIX-systems, Macintoshes and MS-DOS machines).

As its name implies, the publication department is responsible for production of a range of publications in CWI research: Tracts, Syllabi, Reports, Monographs (jointly with North-Holland Publishing Company) and the CWI Quarterly, as well as other items including annual reports and doctoral theses. A good deal of work is also carried out on behalf of bodies such as the Dutch Mathematical Society.



Social-Economic Affairs Department tasks include accommodation. During 1988, Portakabins were brought in as a stop-gap solution to an acute lack of space due to CWI's ongoing expansion. In November, the entire Analysis, Algebra & Geometry Department moved into its new, temporary accommodation.

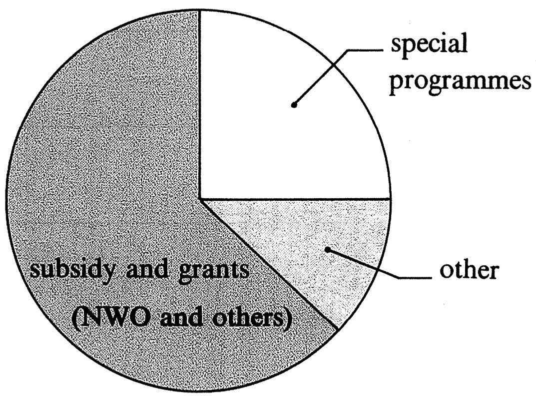
Financial Data, Personnel

FINANCES 1988

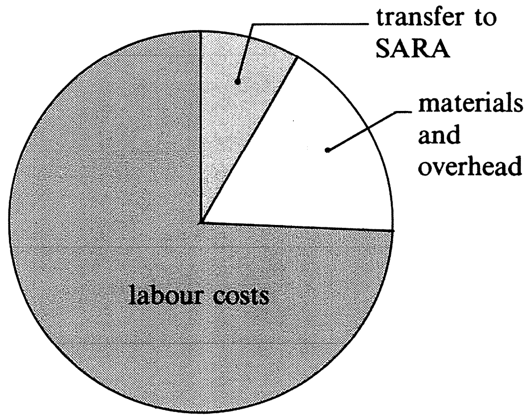
In 1988, SMC spent Dfl. 19.84 million, of which about Dfl. 1.61 million was allocated to research by the national working parties and Dfl. 18.23 million to CWI.
The expenses were covered by a subsidy from NWO (Dfl. 12.62 million), other subsidies and grants (Dfl. 0.51 million), from the European Community for its ESPRIT, CODEST and RACE projects (Dfl. 2.10 million), and from national programmes (Dfl. 2.49 million). Finally, an amount of about Dfl. 2.23 million was obtained as revenues out of third-party-services and other sources.
During 1988 CWI also employed 21 researchers in externally financed positions, for example by STW and industry. These are not included in the adjacent financial summary.

	national working parties	*CWI*	*SMC*
	× *Dfl.* 1000		
INCOME			
subsidy and grants			
- NWO	1712	10911	12623
- other	-	507	507
national programmes			
- INSP	-	2000	2000
- SPIN	-	459	459
- IOP	-	28	28
international programmes			
- ESPRIT	-	1755	1755
- CODEST	-	255	255
- RACE	-	81	81
other			
- proceeds from services and courses	-	1308	1308
- sales of publications	-	122	122
- miscellaneous income	-	802	802
total income	1712	18228	19940
EXPENSES			
labour costs	1597	13423	15020
materials and overhead	15	3254	3269
transfer to SARA	-	1550	1550
total expenses	1612	18227	19839

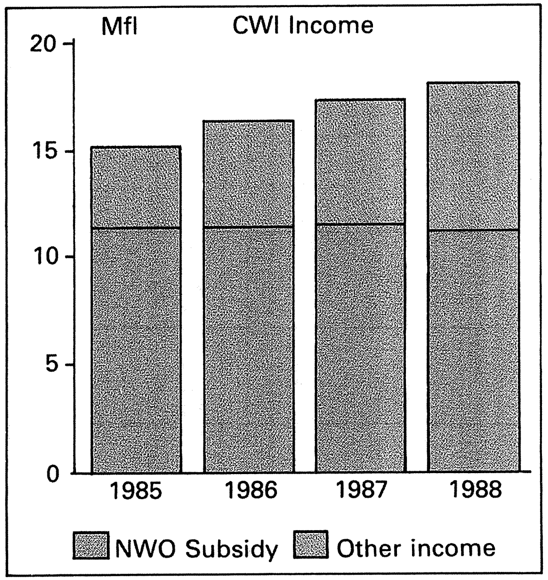
income CWI



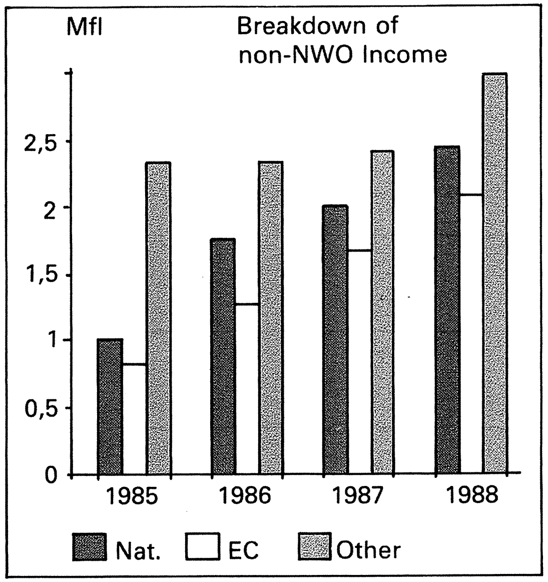
expenses CWI



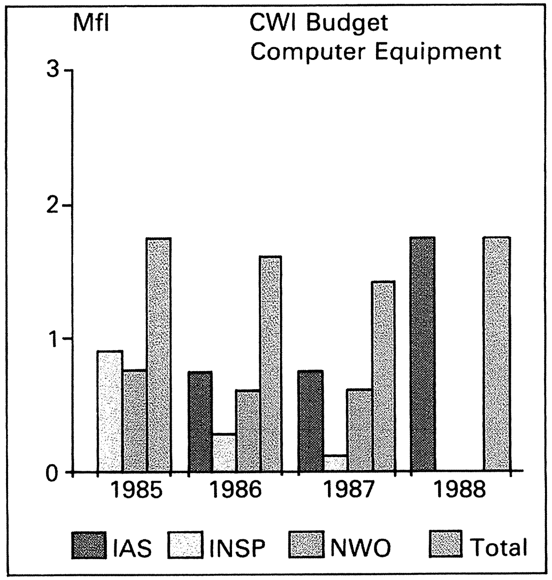
FINANCES 1985-1988



NWO grant as proportion of total operating costs for 1985-1988. Income from other sources continues to increase.

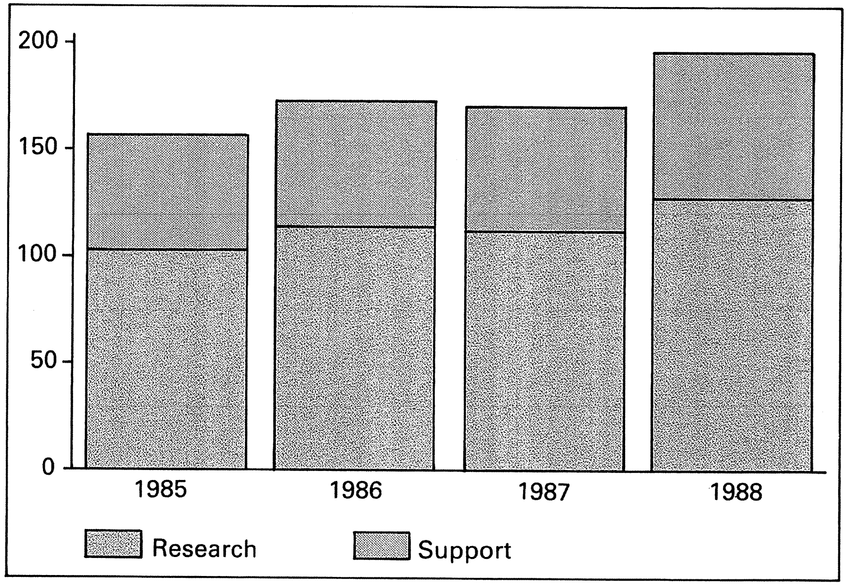


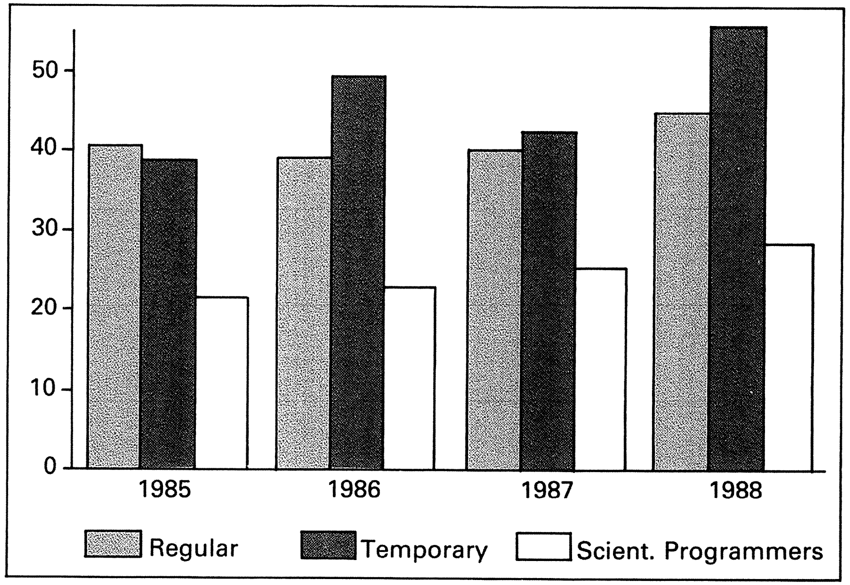
A growing share of funding comes from involvement in national and international application-oriented computer science research programmes (ESPRIT, INSP, SPIN, etc.).



For some years CWI has suffered a steady erosion of the funding for computer equipment. Historical sources for this funding include the INSP programme, and grants from NWO and the IAS government support scheme. Whilst there were no contributions from the first two in 1988, the IAS grant was more than doubled; this meant a modest overall increase - and the reversal of a trend. However, an expert analysis of CWI's computer equipment situation, made in 1987, shows that funding is still quite inadequate by international standards.

PERSONNEL 1985-1988





The size of the personnel force is expressed in full-time equivalents, averaged over the year in question.
Not included are externally financed positions (e.g. from STW and industry). For the years 1985-1988 these amounted to 7, 10, 17 and 21 respectively. To the right the breakdown of the research personnel is shown.

Foreign Visitors

Pure Mathematics

W. Aspray (USA)
J. Cannon (Australia)
Y. Desmedt (Canada)
J. Faraut (France)
F. Guerra (Italy)
R. Hermann (USA)
R. Impegliazzo (USA)
A.A. Ivanov (USSR)
N. Lazhari (Tunisia)
D.A. Leites (Sweden)
M.W. Liebeck (UK)
I.G. Macdonald (UK)
B. Ørsted (Denmark)
G. Purdy (USA)
O. Staffelbach (Switzerland)
D. Stinson (Canada)
J. Stoyanov (Bulgaria)
L. Streit (FRG)
F.H. Szafraniec (Poland)
S.L. Woronowicz (Poland)

Applied Mathematics

J.E. Besag (UK)
R. Bolle (USA)
R. Bürger (Austria)
A. Grabosch (FRG)
J. Gracia-Bondia (Costa Rica)
G. Greiner (FRG)
M. Gyllenberg (Finland)
Y. Hosono (Japan)
K. Keimel (FRG)
V. Kertész (Hungary)
M. Kretzschmar (FRG)
A. Louis (FRG)
G. Lumer (Norway)
T. Naito (Japan)
F. Natterer (FRG)
Y. Nishiura (Japan)
J. Prüss (FRG)
C. Ronse (Belgium)
H.R. Thieme (USA)

Mathematical Statistics

J. Antoch (Czechoslovakia)
R.J. Chitashvili (USSR)
W.S. Cleveland (USA)
M.L. Eaton (USA)
P. Greenwood (Canada)
W. Härdle (FRG)
S. Kalikow (Israel)
R.H. Randles (USA)
G. Stone (UK)
H. Thorisson (Sweden)
E. Valkeila (Finland)
J.A. Wellner (USA)
J. Wilson (UK)

Operations Research and System Theory

R.R. Bitmead (Australia)
J.H. Bookbinder (Canada)
F.M. Callier (Belgium)
R.J. Chitashvili (USSR)
E.G. Coffman, Jr. (USA)
M. Deistler (Austria)
M. Desrochers (Canada)
M.I. Dessouky (USA)
R. Elliott (Canada)
G. Fayolle (France)
P.A. Fuhrmann (Israel)
M. Goetschalckx (USA)
D. Granot (Canada)
F. Granot (Canada)
M. Green (UK)
P. Greenwood (Canada)
C.V. Jones (USA)
G. Kallianpur (USA)
K. Malik (USA)
B. Mazbic-Kulma (Poland)
M. Queyranne (Canada/France)
B. Reed (Canada)
D.B. Shmoys (USA)
L. Slominski (Poland)
D. Songkang (Denmark)
R. Syski (USA)
J. Walrand (USA)
G. Weiss (Israel)
A.S. Willsky (USA)
Wu Fang (China)
J. Wynkin (Belgium)

Numerical Mathematics

M.J. Baines (UK)
M. Berzins (UK)
H. Brunner (Canada)
P. Conradi (FRG)
D. Elliot (Australia)
J.E. Flaherty (USA)
K. Miller (USA)
L.R. Petzold (USA)
M. Revilla (Spain)
J. Schneid (Austria)
W. Schönauer (FRG)
D. Schröder (FRG)
F. Uson (Spain)
R. Vichnevetsky (USA)
G. Wittum (FRG)

Software Technology

C. Cecchi (Italy)
D. Clement (France)
H. Comon (France)
C. Cousineau (France)
W. Damm (FRG)
R. De Nicola (Italy)
P. Degano (Italy)
M.H. van Emden (Canada)
U. Goltz (FRG)
L. Fribourg (France)
R.N. Horspool (Canada)
J. Incerpi (France)
J. Jaffar (USA)
B. Jonsson (Sweden)
B. Josko (FRG)
S. Kaplan (Israel)
C. Lengauer (USA)
D. Lester (UK)
G. Levi (Italy)
J. Maluszynski (Sweden)
M. Martelli (Italy)
F.G. McCabe (UK)
L. Monteiro (Portugal)
E.-R. Olderog (FRG)

C. Palamidessi (Italy)
N. Plouzeau (France)
A. Rabinovitch (Israel)
Ph. Schnoebelen (France)
U. Schuerfeld (FRG)
S.A Smolka (USA)
S. Sokolowski (Poland)
S. Tsur (USA)
J. Zeleznikow (Australia)
J.I. Zucker (USA)

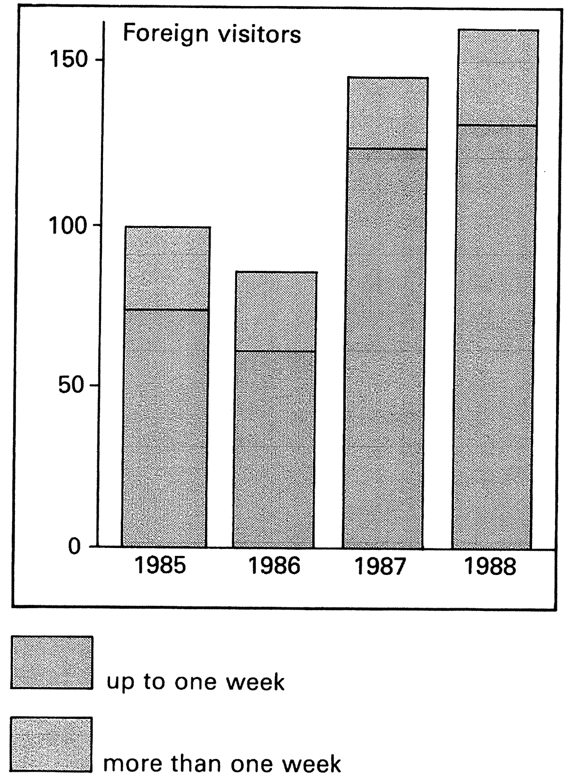
Algorithmics and Architecture

L. Barfield (UK)
M. Burrows (UK)
P. Clote (USA)
M. Gien (France)
K. Kim (Korea)
G. Kissin (Israel)
M. Li (Canada)
N.A. Lynch (USA)
D. McAuley (UK)
J.R. Nicol (UK)
K. Palem (USA)
A. Pheidas (USA)
K. Ramamritham (UK)
D. Riches (UK)
J. Steiner (USA)
L. Stewart (USA)
D. Tygar (USA)
W.E. Weihl (USA)
C.K. Yap (USA)
J. Zahorjan (USA)

Interactive Systems

A. Agogino (USA)
F. Arbab (USA)
D. Duce (UK)
E. Knuth (Hungary)
Zs. Ruttkay (Hungary)
T. Tomiyama (Japan)

FOREIGN VISITORS 1985-1988



List of Publications

Department of Pure Mathematics

Report series

PM-R8801 M. Hazewinkel. *Lectures on linear and nonlinear filtering.*
PM-R8802 M. Hazewinkel. *A short tutorial on Lie algebras.*
PM-R8803 M. Hazewinkel. *A tutorial introduction to differentiable manifolds and calculus on manifolds.*
PM-R8804 J.T.M. van Bon, A.M. Cohen. *Prospective classification of distance-transitive graphs.*
PM-R8805 J.T.M. van Bon, A.M. Cohen. *Linear groups and distance-transitive graphs.*
PM-R8806 T.H. Koornwinder. *Meixner-Pollaczek polynomials and the Heisenberg algebra.*
PM-R8807 T.H. Koornwinder. *Jacobi functions as limit cases of q-ultraspherical polynomials.*
PM-R8808 J.T.M. van Bon. *On distance-transitive graphs and involutions.*
PM-R8809 T.H. Koornwinder. *Representations of the twisted SU(2) quantum group and some q-hypergeometric orthogonal polynomials.*
PM-R8810 M. Hazewinkel. *Nongaussian linear filtering, identification of linear systems, and the symplectic group.*
PM-R8811 S.N.M Ruijsenaars. *Index formulas for generalized Wiener-Hopf operators and Boson-Fermion correspondence in 2N dimensions.*
PM-N8801 J. de Vries. *Invariant measures in abstract topological dynamics.*

Publications in Journals, proceedings, etc.

Z1 H. den Boer (1988). Cryptanalysis of F.E.A.L. *Proceedings Eurocrypt 88*, LNCS 330, Springer, Berlin, 293-299.

Z2 J.T.M. van Bon, A.E. Brouwer (1988). The distance-regular antipodal covers of classical distance-regular graphs. *Proc.: Combinatorics* (Eger, Hongarije, 1987), Colloquia Mathematica Societatis Janos Bolyai 52, North-Holland, 1987, 141-166.

Z3 G. Brassard, D. Chaum, C. Crepeau (1988). Minimum disclosure proofs of knowledge. *J. Comp. Sys. Sciences*, 156-189.

Z4 D. Chaum (1988). The dining cryptographers problem: unconditional sender untraceability. *J. Cryptology 1*, 65-75.

Z5 D. Chaum (1988). Privacy protected payments: unconditional payer and/or payee untraceability. *Smart Card 2000* (Proc. Conf. in Laxenburg, Austria, 1987), North-Holland, 69-93.

Z6 D. Chaum (1988). Elections with unconditionally secret ballots and disruption equivalent to breaking RSA. *Proceedings Eurocrypt '88*, LNCS 330, Springer-Verlag, 177-182.

Z7 D. Chaum (1988). Blinding for unanticipated signatures. *Proceedings Eurocrypt '87*, Springer-Verlag.

Z8 D. Chaum, J. van de Graaf (1988). An improved protocol for demonstrating posession of a discrete logarithm and some generalizations. *Proceedings Eurocrypt '87*, Springer-Verlag.

Z9 D. Chaum, E. Brickel, I. Damgard, J. van de Graaf (1988). Gradual and verifiable release of a secret. *Proceedings Crypto '87*, LNCS 293, Springer-Verlag, 156-166.

Z10 D. Chaum, C. Crepeau, I. Damgard (1988). Fundamental primitives for multiparty unconditionally secure protocols. *Proc. Symp. on Theory of Computing* (Chicago, 1987), 11-19.

Z11 D. Chaum, I. Damgard, J. van de Graaf (1988). Multiparty computations ensuring secrecy of each party's input and correctness of result. *Proceedings Crypto 87*, LNCS 293, Springer-Verlag, 87-119.

Z12 A.M. Cohen, A.G. Helminck (1988). Trilinear alternating forms on a vector space of dimension 7. *Comm. Algebra 16*, 1-25.

Z13 A.M. Cohen, B.N. Cooperstein (1988). The 2-spaces of the standard E6-module. *Geometriae Dedicata 25*, 467-480.

Z14 A.M. Cohen (1988). Mathematical formula manipulation from a user's point of view. *CWI Quarterly 1*, 53-63.

Z15 A.M. Cohen, R.L. Griess Jr. (1987). On finite simple subgroups of the complex Lie group of type E_8. *Proc Symp. Pure Math 47*, 367-405.

Z16 J.-H. Evertse (1988). Linear structures in block ciphers. D. Chaum, W. Price (eds.). *Proceedings Eurocrypt '87*, Springer-Verlag.

Z17 J. van de Graaf, R. Peralta (1988). A simple and secure way to show the validity of your public key. *Proceedings Crypto '87*, LNCS 293, Springer-Verlag.

Z18 M. Hazewinkel (1988). An introduction to nilpotent approximation filtering. H. Neunzert (ed.). *Proc. 2nd European Symp. on Mathematics in Industry*, Teubner/Kluwer Academic, 115-120.

Z19 M. Hazewinkel (1988). A tutorial introduction to differentiable manifolds and calculus on manifolds. W. Schiehlen, W. Wedig (eds.). *Analysis and Estimation of Stochastic Mechanical Systems* (CISM course, 1987), Springer-Verlag, 316-340.

Z20 M. Hazewinkel (1988). Lectures on linear and nonlinear filtering. W. Schiehlen, W. Wedig (eds.). *Analysis and Estimation of Stochastic Mechanical Systems* (CISM course, 1987), Springer-Verlag, 103-136.

Z21 M. Hazewinkel (1988). A short tutorial on Lie algebras. W. Schiehlen, W. Wedig (eds.). *Analysis and Estimation of Stochastic Mechanical Systems*

(CISM course, 1987), Springer-Verlag, 341-350.
Z22 M. HAZEWINKEL (1988). The philosophy of deformations. M. HAZEWINKEL, M. GERSTENHABER (eds.). *Deformations of Algebras and Applications*, KAP, 1-7.
Z23 M. HAZEWINKEL (1988). Idiosyncratic remarks by a biblomaniak: 5. a random sample of structured chaos. *Acta Appl. 13,* 203-219.
Z24 T.H. KOORNWINDER (1986). A group theoretic interpretation of the last part of de Branges' proof of the Bieberbach conjecture. *Complex Variables Theory Appl 6,* 309-321.
Z25 T.H. KOORNWINDER (1988). Group theoretic interpretations of Askey's scheme of hypergeometric orthogonal polynomials. M. ALFARD et al (eds.). *Orthogonal Polynomials and their Applications*, LNM 1329, Springer-Verlag, 46-72.
Z26 T.H. KOORNWINDER, B. HOOGENBOOM (1988). Fonctions d'entrelacement sur les groupes de Lie compacts et polynomes orthogonaux de plusieurs variables. *Seminaire d'Analyse Harmonique, Ecole d'Eté 1984*, Tunis, 78-93.
Z27 S.N.M. RUIJSENAARS (1988). Action-angle maps and scattering theory for some finite-dimensional integrable systems, I: the pure soliton case. *Comm. Math. Phys. 115,* 127-165.
Z28 G.C.M. RUITENBURG (1988). The $Gl(n)$-invariant ideals of the coordinate ring of pairs of symmetric matrices with product zero. *Comm. in Algebra 16,* 1993-2011.
Z29 J. DE VRIES (1988). Problems and results in the category of topological transformation groups. *CWI Quarterly 1,* 29-35.
Z30 J. DE VRIES, M. HUŠEK (1988). Compactifications of products of semigroups. Z. FROLIK (ed.). *General Topology and its Relations to Modern Analysis and Algebra VI* (Proc. 6th Prague Top. Sym.), Helderman-Verlag, Berlin, 667.

Other publications

Z31 M. ASCHBACHER, A.M. COHEN, W.M. CANTOR (1988). *Geometries and Groups* (Proc. Conf. Geometries and groups, finite and algebraic, Noordwijkerhout, 1986), Reidel, Dordrecht.
Z32 D. CHAUM, W. PRICE (eds.) (1988). *Proceedings Eurocrypt '87*, Springer-Verlag.
Z33 M. HAZEWINKEL, S. ALBEVERIO, P. BLANCHARD, L. STREIT (eds.) (1988). *Stochastic Processes in Physics and Engineering*, Reidel.
Z34 M. HAZEWINKEL, R.M.M. MATTHEIJ, E.W.C. VAN GROESEN (eds.) (1988). *Proceedings of the first European Symposium on Mathematics in Industry*, Teubner/Kluwer Academic.
Z35 M. HAZEWINKEL, M. GERSTENHABER (eds.) (1988). *Deformation Theory of Algebras and Structures and Applications*, KAP.
Z36 T.H. KOORNWINDER, G.C. WALTER (1988). *The Finite Continuous Jacobi Transform*. Report of the Dept. of Math. of the Univ. of Wisconsin-Milwaukee.
Z37 H.T. KOELINK, T.H. KOORNWINDER (1988). *The Clebsch-Gordan Coefficients for the Quantum group* $S_\mu U(2)$ *and q-Hahn Polynomials.* Report W88-12, Math. Inst., Univ. of Leiden.
Z38 G.C.M. RUITENBURG (1988). *Invariant Ideals of Multiplicity Free Algebraic Group Actions.* Thesis, CWI, Amsterdam.

Department of Applied Mathematics

Report series

AM-R8801 H.N.M. ROOZEN. *Reliability of stochastically forced systems (extended version).*
AM-R8802 PH. CLÉMENT, O. DIEKMANN, M. GYLLENBERG, H.J.A.M. HEIJMANS, H.R. THIEME. *Perturbation theory for dual semigroups IV. The intertwining formula and the canonical pairing.*
AM-R8803 J.B.T.M. ROERDINK, H.J.A.M. HEIJMANS. *Mathematical morphology for structures without translation symmetry.*
AM-R8804 O. DIEKMANN, J.A.J. METZ, M.W. SABELIS. *Mathematical models of predator-prey-plant interactions in a patchy environment.*
AM-R8805 O. DIEKMANN, J.A.J. METZ, M.W. SABELIS. *Reflections and calculations on a prey-predator-patch problem.*
AM-R8806 N.M. TEMME. *Uniform asymptotic expansions of a class of integrals in terms of modified Bessel functions, with application to confluent hypergeometric functions.*
AM-R8807 H.J.A.M. HEIJMANS, C. RONSE. *The algebraic basis of mathematical morphology Part I: Dilations and erosions.*
AM-R8808 P.P.B. EGGERMONT. *Multiplicative iterative algorithms for convex programming.*
AM-R8809 O. DIEKMANN. *On semigroups and populations.*
AM-R8810 PH. CLÉMENT, O. DIEKMANN, M. GYLLENBERG, H.J.A.M. HEIJMANS, H.R. THIEME. *A Hille-Yosida type theorem for a class of weakly * continuous semigroups.*
AM-R8811 J.B.T.M. ROERDINK. *The biennial life strategy in a random environment.* Supplement.
AM-R8812 F. VAN DEN BOSCH, J.A.J. METZ, O. DIEKMANN. *The velocity of spatial population expansion.*

AM-R8813 A. GRABOSCH, H.J.A.M. HEIJMANS. *Cauchy problems with state-dependent time evolution.*

AM-R8814 A.M. DE ROOS, O. DIEKMANN, J.A.J. METZ. *The escalator boxcar train: basic theory and an application to Daphnia population dynamics.*

Publications in Journals, proceedings, etc.

T1 PH. CLÉMENT, O. DIEKMANN, M. GYLLENBERG, H.J.A.M. HEIJMANS, H.R. THIEME (1988). Perturbation theory for dual semigroups II. Time-dependent perturbations in the sun-reflexive case. *Proceedings of the Royal Society of Edinburgh,* 109A, 145-172.

T2 O. DIEKMANN, M.W. SABELIS (1988). Overall population stability despite local extinction: The stabilizing influence of prey dispersal from predator invaded patches. *Theor. Pop. Biol. 34,* 169-176.

T3 O. DIEKMANN, J.A.J. METZ, M.W. SABELIS (1988). Mathematical models of predator-prey-plant interaction in a patchy environment. *Exp. Appl. Acarology 5,* 319-342.

T4 O. DIEKMANN, J.A.J. METZ (1988). Exploring linear chain trickery for physiologically structured populations. *TW in Beeld, bij het afscheid van prof.dr. H.A. Lauwerier,* CWI, Amsterdam, 73-84.

T5 H.J.A.M. HEIJMANS (1988). Iteration of morphological transformations. *TW in Beeld, bij het afscheid van prof.dr. H.A. Lauwerier,* CWI, Amsterdam, 55-72.

T6 H. INABA (1988). A semigroup approach to the strong ergodic theorem of the multistate stable population process. *Mathematical Population Studies,* Vol. 1(1), 49-77.

T7 H. INABA (1988). Asymptotic properties of the inhomogeneous Lotka-Von Foerster system. *Mathematical Population Studies,* Vol. 1(3), 247-264.

T8 J.B.T.M. ROERDINK (1988). The biennial life strategy in a random environment. *J. Math. Biol. 26,* 199-215.

T9 J.B.T.M. ROERDINK (1988). Products of random matrices or 'why do biennials live longer than two years'? *TW in Beeld, bij het afscheid van prof.dr. H.A. Lauwerier,* CWI, Amsterdam, 11-18.

T10 J.B.T.M. ROERDINK, H.J.A.M. HEIJMANS (1988). Mathematical morphology for structures without translation symmetry. *Signal Processing 15,* 271-277.

T11 H. ROOZEN (1987). Equilibrium and extinction in stochastic population dynamics. *Bulletin of Mathematical Biology,* Vol. 49, No. 6, 671-696.

T12 H. ROOZEN (1988). A short introduction to exit problems. *TW in Beeld, bij het afscheid van prof.dr. H.A. Lauwerier,* CWI, Amsterdam, 33-54.

T13 H.A.J.M. SCHELLINX, J.A.P. HEESTERBEEK (1988). On sums of remainders and almost perfect numbers. *TW in Beeld, bij het afscheid van prof.dr. H.A. Lauwerier,* CWI, Amsterdam, 1-10.

T14 N.M. TEMME (1988). Asymptotic expansion of a special integral. *TW in Beeld, bij het afscheid van prof.dr. H.A. Lauwerier,* CWI, Amsterdam, 19-24.

T15 M. ZWAAN (1988). A Radon transform in circles through the origin in $\mathbb{R}^2$. *TW in Beeld, bij het afscheid van prof.dr. H.A. Lauwerier,* CWI, Amsterdam, 25-32.

Other publications

T16 J. GRASMAN, J.B.T.M. ROERDINK (1988). *Stochastic and Chaotic Relaxation Oscillations.* Reprint no. 540, October, Mathematisch Instituut, RU Utrecht.

T17 H.A. LAUWERIER (1988). *Symmetrie,* Aramith Uitgevers, Amsterdam.

T18 N.M. TEMME (red.) (1988). *TW in Beeld, bij het afscheid van prof.dr. H.A. Lauwerier,* CWI, Amsterdam.

Department of Mathematical Statistics

Report series

MS-R8801 W. VERVAAT. *Random upper semicontinuous functions and extremal processes.*

MS-R8802 S. TARDIF. *Conditionally and strictly distribution-free tests for randomized block designs that are asymptotically optimal.*

MS-R8803 P.K. ANDERSEN, Ø. BORGAN, R.D. GILL, N. KEIDING. *Censoring, truncation and filtering in statistical models based on counting processes.*

MS-R8804 E.V. KHMALADZE. *The statistical analysis of a large number of rare events.*

MS-R8805 S.A VAN DE GEER. *Estimating a regression function.*

MS-R8806 S.A VAN DE GEER. *Asymptotic normality of minimum L_1-norm estimators in linear regression.*

MS-R8807 W.A.J. GEURTS, M.M.A. HASSELAAR, J.H. VERHAGEN. *Large sample theory for statistical inference in several software reliability models.*

MS-R8808 R. HELMERS, P. JANSSEN, R. SERFLING. *Berry-Esseen rates and bootstrap results for generalized L-statistics.*

MS-R8809 A.J. VAN ES, A.W. HOOGENDOORN. *A kernel approach to estimation of the sphere radius density in Wicksell's Corpuscle Problem.*

MS-R8810 H.C.P. BERBEE, W.TH.F. DEN HOLLANDER. *Tail triviality for sums of stationary random variables.*

MS-R8811 A.W. HOOGENDOORN. *Estimating the weight undersize distribution* *for the Wicksell problem.*

MS-R8812 S.A. VAN DE GEER, L. STOUGIE. *On a rate of convergence of the multiknapsack value function.*

MS-R8813 M.J. ROTTSCHÄFER, L.G. BARENDREGT. *A statistical analysis of spatial point patterns. A case study.*

MS-R8814 A.P. VAN DER PLAS. *A semiparametric model for citation counts.*

MS-R8815 E.A.G. WEITS. *Stochastic model of traffic flow on freeways.*

MS-R8816 R.D. GILL, N. KEILMAN. *On the estimation of multidimensional demographic models with population registration data.*

MS-R8817 N. KEIDING, R.D. GILL. *Random truncation models and Markov processes.*

MS-R8818 K.O. DZHAPARIDZE, E. VALKEILA. *On the Hellinger type distances for filtered experiments.*

MS-R8819 R.J. CHITASHVILI. *On the smooth fit boundary conditions in the optimal stopping problem for semimartingales.*

Publications in Journals, proceedings, etc.

S1 P.K. ANDERSEN, Ø. BORGAN, R.D. GILL, N. KEIDING (1988). *Censoring, truncation and filtering in statistical models for counting processes. Contemporary Mathematics 80* (Statistical Inference from Stochastic Processes, ed. U. Prabhu), AMS.

S2 R.J.M.M. DOES, R. HELMERS, C.A.J. KLAASSEN (1988). Approximating the distribution of Greenwood's statistic. *Statistica Neerlandica, 42,* 153-161.

S3 S.G.A.J. DRIESSEN (1988). The sieve method, a sampling method for audit practice. *Statistica Neerlandica, 42,* 117-129.

S4 A.J. VAN ES, R. HELMERS (1988). Elementary symmetric polynomials of increasing order. *Probab. Th. Rel. Fields, 80,* 21-35.

S5 R.D. GILL, Y. VARDI, J.A. WELLNER (1988). Large sample theory of empirical distributions in biased sampling models. *The Annals of Statistics, 16,* 1069-1112.

S6 R.D. GILL (1988). Regression analysis for mixed cross-section and time-series data with reference to some incomplete observations techniques. *Sankya Series, B 50,* 95-102.

S7 R. HELMERS, P. JANSSEN, R. SERFLING (1988). Glivenko-Cantelli properties of some generalized empirical df's and strong convergence of generalized L-statistics. *Probab. Th. Rel. Fields, 79,* 75-93.

S8 R. HELMERS, F.H. RUYMGAART (1988). Asymptotic normality of generalized L-statistics with unbounded scores. *Journal of Statistical Planning and Inference, 19,* 43-53.

S9 E. KHMALADZE (1988). An innovation approach to goodness-of-fit tests in R^m. *The Annals of Statistics, 16,* 1503-1516.

Other publications

S10 S.A. VAN DE GEER (1988). *Regression Analysis and Empirical Processes.* CWI Tract 45, CWI, Amsterdam.

Department of Operations Research and System Theory

Report series

OS-R8801 J.L. VAN DEN BERG, O.J. BOXMA. *Sojourn times in feedback and processor sharing queues.*

OS-R8802 W.P. GROENENDIJK. *Waiting-time approximations for cyclic-service systems with mixed service strategies.*

OS-R8803 P.R. DE WAAL. *A sufficient condition for a product form distribution of a queueing network with controlled arrivals.*

OS-R8804 J.M. SCHUMACHER. *Analytic methods for the modeling of flexible structures.*

OS-R8805 J.M. ANTHONISSE, J.K. LENSTRA, M.W.P. SAVELSBERGH. *Behind the screen: DSS from an OR point of view.*

OS-R8806 S.A. SMULDERS. *Filtering of freeway traffic flow.*

OS-R8807 J.M. SCHUMACHER. *State representations of linear systems with output constraints.*

OS-R8808 S.L. VAN DE VELDE. *Minimizing total completion time in the two-machine flow shop by Lagrangian relaxation.*

OS-R8809 P.J.M. VAN LAARHOVEN, E.H.L. AARTS, J.K. LENSTRA. *Job shop scheduling by simulated annealing.*

OS-R8810 A. SCHRIJVER. *The Klein bottle and multicommodity flows.*

OS-R8811 A. SCHRIJVER. *Homotopy and crossings of systems of curves on a surface.*

OS-R8812 A. SCHRIJVER. *Disjoint circuits of prescribed homotopies in a graph on a compact surface.*

OS-R8813 O.J. BOXMA, W.P. GROENENDIJK, J.A. WESTSTRATE. *A pseudoconservation law for service systems with a polling table.*

OS-R8814 S.L. VAN DE VELDE. *A simpler and faster algorithm for optimal total-work-content-power due date determination.*

OS-R8815 F.A. VAN DER DUYN SCHOUTEN, T. RONNER. *Calculation of the availability of a two-unit parallel system with cold standby: An illustration of the embedding technique.*

OS-R8816 W.P. GROENENDIJK. *A conservation-law based approximation algorithm for waiting times in polling systems.*

OS-R8817 S.A. SMULDERS. *Control of freeway traffic flow.*

OS-R8818 J.W. VAN DER WOUDE. *A note on pole placement by static output feedback for single-input systems.*

OS-R8819 J.W. VAN DER WOUDE. *A graph theoretic characterization for the rank of a transfer matrix of a structured system.*

OS-R8820 R.K. BOEL, J.H. VAN SCHUPPEN. *Distributed routing for load balancing.*

OS-N8801 J.K. LENSTRA. *Algorithmics and heuristics in combinatorial optimization.*

Publications in Journals, proceedings, etc.

B1 J.M. ANTHONISSE, K.M. VAN HEE, J.K. LENSTRA (1988). Resource-constrained project scheduling: an international exercise in DSS development. *Decision Support Systems 4*, 249-257.

B2 J.L. VAN DEN BERG, O.J. BOXMA (1988). Sojourn times in feedback and processor sharing queues. (=OS-R8801). M. BONATTI (ed.). *Proceedings ITC-12*, North-Holland, Amsterdam.

B3 R.K. BOEL, J.H. VAN SCHUPPEN (1988). Distributed load balancing. *Proceedings 27th IEEE Conference on Decision and Control*, IEEE Press, 1486.

B4 J. BONTSEMA, R.F. CURTAIN, J.M. SCHUMACHER (1988). Robust control of flexible structures: a case study. *Automatica J. IFAC 24*, 177-186.

B5 O.J. BOXMA (1988). Sojourn times in cyclic-queues - the influence of the slowest server. *Computer Performance and Reliability,* North-Holland, Amsterdam, 13-24.

B6 O.J. BOXMA, R. SYSKI (1988). J.W. Cohen: his scientific career. *CWI Quarterly 1*, 73-80.

B7 O.J. BOXMA, W.P. GROENENDIJK (1988). Waiting times in discrete-time cyclic-service systems. *IEEE Trans. Comm. 36*, 164-170.

B8 O.J. BOXMA, W.P. GROENENDIJK (1988). Two queues with alternating service and switching times. *Queueing Theory and its Applications - Liber Amicorum for J.W. Cohen,* North-Holland, Amsterdam, 261-282.

B9 M. DESROCHERS, J.K. LENSTRA, M.W.P. SAVELSBERGH, F. SOUMIS (1988). Vehicle routing with time windows: optimization and approximation. B.L. GOLDEN, A.A. ASSAD (eds.). *Vehicle Routing: Methods and Studies*, North-Holland, Amsterdam, 65-84.

B10 W.P. GROENENDIJK (1988). Waiting-time approximation for cyclic-service systems with mixed service strategies. (=OS-R8802). M. BONATTI (ed.). *Proceedings ITC-12*, North-Holland, Amsterdam.

B11 C.A.J. HURKENS, L. LOVÁSZ, A. SCHRIJVER, É TARDOS (1988). How to tidy up your set-system? A. HAJNAL, L. LOVÁSZ, V.T. SÓS (eds.). *Combinatorics,* North-Holland, Amsterdam, 309-314.

B12 C.A.J. HURKENS, A. SCHRIJVER, E. TARDOS (1988). On fractional multicommodity flows and distance functions. *Discrete Mathematics 73,* 99-109.

B13 G.A.P. KINDERVATER, J.K. LENSTRA (1988). Parallel computing in combinatorial optimization. *Ann. Oper. Res. 14*, 245-289.

B14 B.J. LAGEWEG, J.K. LENSTRA, A.H.G. RINNOOY KAN, L. STOUGIE (1988). Stochastic integer programming by dynamic programming. YU. ERMOLIEV, R.J-B. WETS (eds.). *Numerical Techniques for Stochastic Optimization*, Springer-Verlag, Berlijn, 403-412.

B15 J.K. LENSTRA (1988). Interfaces between operations research and computer science. M. HAZEWINKEL, R.M.M. MATTHEIJ, E.W.C. VAN GROESEN (eds.). *Proceedings of the First European Symposium on Mathematics in Industry*, Teubner/Kluwer, Stuttgart, 79-94.

B16 J.K. LENSTRA (1988). Algorithmics and heuristics in combinatorial optimization. H. SCHELLHAAS, P. VAN BEEK, H. ISERMANN, R. SCHMIDT, M. ZIJLSTRA (eds.). *Operations Research Proceedings 1987*, Springer-Verlag, Berlijn, 56-65.

B17 J.M. SCHUMACHER (1988). Transformations of linear systems under external equivalence. *Linear Algebra and its Applications 102*, 1-34.

B18 J.M. SCHUMACHER (1988). Analytic methods for the modeling of flexible structures. A. BENSOUSSAN, J.L. LIONS (eds.). *Analysis and Optimization of Systems* (Proceedings 8th International Conference, Antibes, June 1988), Lecture Notes in Control and Information Sciences III, Springer-Verlag, Berlijn, 461-471.

B19 H.L. TRENTELMAN, J.W. VAN DER WOUDE (1988). Almost invariance and noninteracting control: a frequency domain analysis. *Linear Algebra and its Applications 101*, 221-254.

B20 S.L. VAN DE VELDE (1988). Surrogate duality in integer linear min-max programming. *Proceedings EURO Workshop on Production Planning & Scheduling*, Parijs.

B21 P.R. DE WAAL (1988). Stochastic control of a processor sharing queue with partial state information. *Proceedings 27th IEEE Conference on Decision and Control*, IEEE Press, 1135-1136.

B22 J.W. VAN DER WOUDE (1988). Disturbance decoupling and output stabilization by measurement feedback: a combined approach. *Int. J. Control 47*, 393-412.

B23 J.W. VAN DER WOUDE (1988). A note on pole placement by static output feedback for single input systems. *Systems & Control Letters 11*, 285-287.

Other publications

B24 O.J. BOXMA, D.J. DER KINDEREN, J.W. KOTEN, W. DEN OTTER (1988).

Stochastic Theory of Oncogenesis. Report Pathologisch Instituut, RU Utrecht.

B25 O.J. BOXMA, A.H.G. RINNOOY KAN, M. VAN VLIET (1988). *Machine Allocation Problems in Manufacturing Networks*. Report EU Rotterdam.

B26 O.J. BOXMA, R. SYSKI (eds.) (1988). *Queueing Theory and its Applications-Liber Amicorum for J.W. Cohen*, North-Holland, Amsterdam.

B27 M. GRÖTSCHEL, L. LOVÁSZ, A. SCHRIJVER (1988). *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, Berlijn.

B28 G. IAZEOLLA, P.-J. COURTOIS, O.J. BOXMA (eds.) (1988). *Computer Performance and Reliability*, North-Holland, Amsterdam.

B29 H. LEVY, M. SIDI, O.J. BOXMA (1988). *Dominance Relations in Polling Systems*. Report Tel-Aviv University.

B30 M.W.P. SAVELSBERGH (1988). *Computer Aided Routing*. Thesis, CWI, Amsterdam.

B31 A. SCHRIJVER (1988). *Homotopic Routing Methods*. Rapport 88522-OR, Institut für Ökonometrie und Operations Research, Universität Bonn, Bonn (to appear in 'Paths, Flows, and VLSI-layout' (Springer-Verlag)).

B32 J.M. SCHUMACHER (1988). *Discrete Events: Perspectives from System Theory*. Research memorandum 354, Faculteit der Economische Wetenschappen, KU Brabant, Tilburg.

Department of Numerical Mathematics

Report series

NM-R8801 P.M. DE ZEEUW. *Matrixdependent prolongations and restrictions in a blackbox multigrid solver.*

NM-R8802 P.J. VAN DER HOUWEN, B.P. SOMMEIJER. *The use of smoothing techniques in the method of lines.*

NM-R8803 B. KOREN. *Multigrid and defect correction for the steady Navier-Stokes equations.*

NM-R8804 J.G. VERWER, J.G. BLOM, J.M. SANZ-SERNA. *An adaptive moving grid method for one-dimensional systems of partial differential equations.*

NM-R8805 H.J.J. TE RIELE, W.M. LIOEN, D.T. WINTER. *Factoring with the quadratic sieve on large vector computers.*

NM-R8806 R.M. FURZELAND, J.G. VERWER, P.A. ZEGELING. *A numerical study of three moving grid methods for one-dimensional partial differential equations which are based on the method of lines.*

NM-R8807 W.M. LIOEN, H.J.J. TE RIELE, D.T. WINTER. *Optimization of the MPQS-factoring algorithm on the Cyber 205 and on the NEC SX-2.*

NM-R8808 P.J. VAN DER HOUWEN, B.P. SOMMEIJER. *Smoothed predictor-corrector methods for solving partial differential equations.*

NM-R8809 P.J. VAN DER HOUWEN, B.P. SOMMEIJER. *Iterated 'theta'-method for hyperbolic equations.*

NM-R8810 B. KOREN. *Upwind discretization of the steady Navier-Stokes equations.*

NM-R8811 M. LOUTER-NOOL. *LINPACK routines based on the level 2 BLAS.*

NM-R8812 A. GRANVILLE, J. VAN DE LUNE, H.J.J. TE RIELE. *Checking the Goldbach conjecture on a vector computer.*

NM-R8813 E.D. DE GOEDE. *Finite difference methods for the three-dimensional hydrodynamic equations.*

NM-R8814 P.J. VAN DER HOUWEN, B.P. SOMMEIJER, P.A. VAN MOURIK. *Note on explicit parallel multistep Runge-Kutta methods.*

NM-R8815 W.H. HUNDSDORFER, J. SCHNEID. *On the equivalence of BS-stability and B-consistency.*

NM-R8816 J.H.M. TEN THIJE BOONKKAMP. *Pressure correction splitting methods for the computation of oscillatory free convection in low Pr fluids.*

NM-R8817 P.J. VAN DER HOUWEN, B.P. SOMMEIJER. *Variable step iteration of high-order Runge-Kutta methods on parallel computers.*

NM-R8818 J.G. VERWER, J.G. BLOM, R.M. FURZELAND, P.A. ZEGELING. *A moving-grid method for one-dimensional PDEs based on the method of lines.*

NM-R8819 J.J.F.M. SCHLICHTING, H.A. VAN DER VORST. *Solving 3D block bidiagonal linear systems on vector computers.*

NM-N8801 P.W. HEMKER, B. KOREN. *Defect correction and nonlinear multigrid for the steady Euler equations.*

NM-N8802 P.W. HEMKER, B. KOREN. *Multigrid defect correction and upwind schemes for the steady Navier-Stokes equations.*

NM-N8803 B. KOREN, P.M. DE ZEEUW, P.W. HEMKER. *Line Gauss-Seidel relaxation and multigrid for steady, two-dimensional flow computations.*

NM-N8804 H.J.J. TE RIELE. *Factoriseren en Primaliteitstesten, een Inleiding.*

NM-N8805 B. KOREN. *Robustness improvement of point Gauss-Seidel relaxation for steady, hypersonic flow computations.*

Publications in Journals, proceedings, etc.

N1 J.G. BLOM, J.M. SANZ-SERNA, J.G. VERWER (1988). On simple moving grid methods for one-dimensional evolutionary partial differential equations. *J. Comput. Phys. 74*, 191-213.

N2 J.G. BLOM, J.M. SANZ-SERNA, J.G. VERWER (1988). A Lagrangian moving grid scheme for one-dimensional evolutionary partial differential equations. *Proceedings 12-th IMACS World Congress on Scientific Computation, Vol. 3.* (IMACS Publication Office), 585-587.

N3 E.D. DE GOEDE (1988). Stabilization of the Lax-Wendroff method and a generalized one-step Runge-Kutta method for hyperbolic initial-value problems. *Appl. Numer. Math. 4,* 439-453.

N4 P.W. Hemker (1988). A multigrid approach for one-dimensional semiconductor device simulation. W. Joppich, U. Trottenberg (eds.). *Device Simulation-Numerische problemfelder-,* GMD-Studien Nr. 144, GMD, Bonn, 157-164.

N5 P.W. Hemker, B. Koren (1988). Multigrid, defect correction and upwind schemes for the steady Navier-Stokes equations. K.W. Morton, M.J. Baines (eds.). *Numerical Methods for Fuid Dynamics III,* Clarendon Press, Oxford, 153-170.

N6 P.W. Hemker, B. Koren (1988). Defect correction and nonlinear multigrid for the steady Euler equations. *Lecture Series on Computational Fluid Dynamics at the Von Karman Institute,* March 7-11, Rhode Saint Genese, Belgium.

N7 P.J. van der Houwen (1988). Stabilization of explicit difference schemes by smoothing techniques. K. Strehmel (ed.). *Numerical Treatment of Differential Equations* (Proc. Fourth Seminar Halle 1987), NUMDIFF-4), Teubner-Texte zur Mathematik 104, BSB B.G. Teubner Verlaggesellschaft, Leipzig, 205-215.

N8 P.J. van der Houwen, C. Boon, F.W. Wubs (1988). Analysis of smoothing matrices for the preconditioning of elliptic difference equations. *Z. Angew. Math. Mech. 68,* 3-10.

N9 P.J. van der Houwen, B.P. Sommeijer (1988). Smoothed Predictor-Corrector methods for solving partial differential equations. *Intern. Series of Numer. Math. 86,* 201-224.

N10 P.J. van der Houwen, B.P. Sommeijer (1988). The use of smoothing techniques in the method of lines. *IMACS Proceedings of the 12th World Congress on Scientific Computing, Vol. I,* Paris, 608-610.

N11 B. Koren (1988). Defect correction and multigrid for an efficient and accurate computation of airfoil flows. *J. Comput. Phys., 77,* 183.

N12 B. Koren (1988). Multigrid and defect correction for the steady Navier-Stokes equations. W. Hackbusch (ed.). *Notes on Numerical Fluid Mechanics Vol. 23,* Vieweg Verlag, Braunschweig.

N13 B. Koren (1988). *Upwind Discretization of the Steady Navier-Stokes Equations,* CWI Report NM-R8810, to appear in Proceedings of the Second International Conference on Hyperbolic Problems, Aachen, Vieweg Verlag, Braunschweig.

N14 B. Koren, S.P. Spekreijse (1988). Solution of the steady Euler equations by a multigrid method. S.F. McCormick (ed.). *Lecture Notes in Pure and Applied Mathematics,* Dekker, New York.

N15 W.M. Lioen, H.J.J. te Riele, D.T. Winter (1988). Optimization of the MPQS-factoring algorithm on the Cyber 205 and the NEC SX-2. *Supercomputer 26,* 42-50.

N16 M. Louter-Nool (1988). ALGORITHM 663, Translation of Algorithm 539: Basic Linear Algebra Subprograms for FORTRAN Usage in FORTRAN 200 for the Cyber 205. *ACM Trans. Math. Software 14,* 177-195.

N17 J.H.M. ten Thije Boonkkamp (1988). Residual smoothing for accelerating the ADI iteration method for elliptic difference equations. *ZAMM 68,* 445-453.

N18 J.G. Verwer (1988). Some stability results for the hopschotch difference method when applied to convection-diffusion equations. K. Strehmel (ed.). *Numerical Treatment of Differential Equations* (Proc. Fourth Seminar Halle 1987: NUMDIFF-4), Teubner-Texte zür Mathematik No. 104, BSG B.G. Teubner Verlaggesellschaft, Leipzig, 243-252.

Other publications

N19 W.M. Lioen, H.J.J. te Riele, D.T. Winter (1988). *Optimization of the MPQS-factoring Algorithm on the CYBER 205 and the NEC SX-2.* Symposiumverslag 'Rekenen op de SX-2', NLR/SARA/WGS, 3 juni.

N20 H.J.J. te Riele (1988). *Factoriseren en Primaliteitstesten, een Inleiding.* Symposiumverslag 'Priemgetallen en Privacy - Toepassingen van getaltheorie en cryptografie', Studievereniging A-Eskwadraat, Utrecht, 27 October.

N21 J.H.M. ten Thije Boonkkamp (1988). *The Numerical Computation of Time-Dependent, Incompressible Flow.* Thesis, CWI, Amsterdam.

Department of Software Technology

Report series

CS-R8801 N.W.P. van Diepen. *Implementation of modular algebraic specifications.*

CS-R8803 J.W. de Bakker, J.-J.Ch. Meyer. *Metric semantics for concurrency.*

CS-R8807 W.P. Weijland. *The algebra of synchronous processes.*

CS-R8809 J.N. Kok. *A compositional semantics for Concurrent Prolog.*

CS-R8810 K.R. Apt, H.A. Blair. *Arithmetic classification of perfect models of stratified programs.*

CS-R8811 K.R. Apt, N. Francez, S. Katz. *Appraising fairness in languages for distributed programming.*

CS-R8812 F.W. Vaandrager. *Some observations on redundancy in a context.*

CS-R8814 J. Heering, P. Klint. *Towards shorter algebraic specifications: a simple language definition and its compilation to Prolog.*

CS-R8815 J.C.M. Baeten, J.A. Bergstra, J.W. Klop, W.P. Weijland. *Term* *rewriting systems with rule priorities.*

CS-R8816 L.C. VAN DER GAAG. *The certainty factor model and its basis in probability theory.*

CS-R8820 M.H. LOGGER. *An integrated text and syntax-directed editor.*

CS-R8821 R.J. VAN GLABBEEK, F.W. VAANDRAGER. *Modular specifications in process algebra - with curious queues.*

CS-R8822 J. HEERING, P. KLINT, J.G. REKERS. *Incremental generation of parsers.*

CS-R8823 P.R.H. HENDRIKS. *ASF system user's guide.*

CS-R8824 M. BEZEM *Semantics and consistency of rule-based expert systems.*

CS-R8825 A. ELIËNS. *Expert systems as deductive systems.*

CS-R8826 K.R. APT. *Introduction to logic programming (revised and extended version).*

CS-R8827 J.C. MULDER. *On the Amoeba protocol.*

CS-R8830 K.R. APT. *Efficient computing of least fixpoints.*

CS-R8831 J.J.M.M. RUTTEN. *Correctness and full abstraction of metric semantics for concurrency.*

CS-R8832 W.P. WEIJLAND. *Synchrony with empty process.*

CS-R8833 C. PALAMIDESSI. *A fixpoint semantics for Guarded Horn Clauses.*

CS-R8834 J.W. DE BAKKER, J.N. KOK. *Uniform abstraction, atomicity and contractions in the comparative semantics of Concurrent Prolog.*

CS-R8835 J.N. KOK. *Data flow semantics.*

CS-R8837 M. BEZEM. *Completeness of resolution by transfinite induction.*

CS-R8838 P.H. RODENBURG, R.J. VAN GLABBEEK. *An interpolation theorem in equational logic.*

CS-R8839 F.W. VAANDRAGER. *Determinism → (Event structure isomorphism = Step sequence equivalence).*

CS-R8840 J.W. DE BAKKER. *Comparative semantics for flow of control in logic programming without logic.*

CS-R8842 L.C. VAN DER GAAG. *Partially specified probability measures in expert systems.*

CS-R8843 J.J.M.M. RUTTEN. *Semantic correctness for a parallel object-oriented language.*

CS-R8844 J.A. BERGSTRA, J. HEERING, P. KLINT. *Module algebra (revised version).*

CS-R8845 J.F. GROOTE, F.W. VAANDRAGER. *Structured operational semantics and bisimulation as a congruence.*

CS-R8846 A. ELIËNS. *Parallel inference based on Delta Processing.*

CS-R8847 L.C. VAN DER GAAG. *Different notions of uncertainty in quasi probabilistic models.*

CS-R8848 E.A. VAN DER MEULEN. *Algebraic specification of a compiler for a language with pointers.*

CS-N8801 M. DE ROOY. *Concurrent evaluation of side-effects.*

CS-N8802 A. PONSE. *Process algebra and Hoare's logic.*

Publications in Journals, proceedings, etc.

P1 P. AMERICA, J.W. DE BAKKER (1988). Designing equivalent semantic models for process creation. *Theoretical Computer Science, 60,* 109-176.

P2 P. AMERICA, J.J.M.M. RUTTEN (1988). Solving reflexive domain equations in a category of complete metric spaces. M. MAIN, A. MELTON, M. MISLOVE, D. SCHMIDT (eds.). *Proc. of the Third Workshop on Mathematical Foundations of Programming Language Semantics,* LNCS 298, 254-288.

P3 K.R. APT (1988). Proving correctness of concurrent programs - a quick introduction. E. BORGER (ed.). *Current Trends in Theoretical Computer Science,* Computer Science Press, 305-346.

P4 K.R. APT, H. BLAIR (1988). Arithmetic classification of perfect models of stratified programs. *Proc. 5th Int. Conference Symposium on Logic Programming,* The MIT Press, 765-779.

P5 K.R. APT, H. BLAIR, A. WALKER (1988). Towards a theory of declarative knowledge. J. MINKER (ed.). *Foundations of Deductive Databases and Logic Programming,* Kaufman and Morgan, 89-148.

P6 K.R. APT, N. FRANCEZ, S. KATZ (1988). Appraising fairness in languages for distributed programming. *Distributed Computing,* Vol. 2, 226-241.

P7 K.R. APT, E.-R. OLDEROG (1988). Fairness in parallel programs, the transformational approach. *ACM TOPLAS,* Vol. 10, 420-455.

P8 J.C.M. BAETEN, W.P. WEIJLAND (1988). Semantics for Prolog via term rewrite systems. S. KAPLAN, J.P. JOUANNAUD (eds.). *Proc. 1st Int'l Workshop on Conditional Term Rewriting, Orsay, 1987,* LNCS 308, 3-14.

P9 J.W. DE BAKKER, J.N. KOK (1988). Uniform abstraction, atomicity and contractions in the comparative semantics of Concurrent Prolog. *Proc. Int. Conference on Fifth Generation Computer Systems 1988, Institute for New Generation Computer Technology,* 347-355.

P10 J.W. DE BAKKER, J.-J.CH. MEYER (1988). Metric semantics for concurrency. *BIT, 28,* 504-529.

P11 J.W. DE BAKKER, J.-J.CH. MEYER, E.-R. OLDEROG, J.I. ZUCKER (1988). Transition systems, metric spaces and ready sets in the semantics of uniform concurrency. *Journal of Comp. and System Sciences, 36,* 158-224.

P12 J.A. BERGSTRA, J.W. KLOP (1988). A complete inference system for regular processes with silent moves. F.R. DRAKE, J.K. TRUS (eds.). *Proc. Logic Colloquium '86,* Elsevier Science Publishers B.V. (North-Holland), 21-81.

P13 M. BEZEM (1988). Consistency of rule-based expert systems. *Proc. of 9th*

Int. Conference on Automated Reasoning, Argonne, 1988, Springer Lecture Notes in Computer Science, Vol. 310, Springer-Verlag, 151-161.
P14 M. Bezem, J. van Leeuwen (1988). On the complexity of logarithmic decompositions. *Information Processing Letters 26,* nr. 6, 321-324.
P15 M. Bezem (1988). Equivalence of bar recursions in the theory of functionals of finite type. *Archive for Mathematical Logic 27,* 149-160.
P16 M. Bezem (1988). Logic programming and PROLOG. *CWI Quarterly,* Vol. 1, nr. 3, 15-29.
P17 N.W.P. van Diepen (1988). Implementation of modular algebraic specifications. H. Ganzinger (ed.). *Proc. of ESOP '88,* LNCS 300, 64-78.
P18 L.C. van der Gaag, P.J.F. Lucas (1988). HEPAR: an expert system in PROLOG. *AI Expert,* juni.
P19 J. Heering, P. Klint (1988). Towards shorter algebraic specifications: a simple language definition and its compilation to Prolog. *ESPRIT '88: Putting the Technology to Use,* North-Holland, 365-379.
P20 P.R.H. Hendriks (1988). Automatic implementation of algebraic specification. *Conference Proceedings of Computing Science in the Netherlands CSN88,* SION 1988, 83-94.
P21 J.W. Klop, A. Middeldorp (1988). An introduction to Knuth-Bendix completion. *CWI Quarterly,* Vol. 1, nr. 3, 31-52.
P22 J.N. Kok (1988). A compositional semantics for concurrent Prolog. R. Cori, M. Wirsing (eds.). *Proc. of the 5th Annual Symposium on Theoretical Aspects of Computer Science,* Bordeaux, February 1988, LNCS 294, 373-388.
P23 J.N. Kok, J.J.M.M. Rutten (1988). Contractions in comparing concurrency semantics. T. Lepisto, A. Salomaa (eds.). *Proc. 15th ICALP,* Tampere, Finland, LNCS 317, 317-332.
P24 P.J.F. Lucas, R.W. Segaar, A.R. Janssens (1988). Hepar, een expertsysteem voor de diagnostiek van aandoeningen van lever en galwegen. *NTVG 132,* nr. 16, 730-733.
P25 W.P. Weijland (1988). Semantics for logic programs without occur check. T. Lepisto, A. Salomaa (eds.). *Proc. 15th ICALP,* Tampere, Finland, LNCS 317, 710-726.

Other publications

P26 J.C.M. Baeten, F.W. Vaandrager (1988). *Specification and Verification of a Circuit in ACP.* Programmatuur rapport P8803, Universiteit van Amsterdam, januari.
P27 J.W. de Bakker (ed.) (1988). *Deliverable ESPRIT Project 415 Working Group on Semantics and Proof Techniques, Year 1987-1988,* November.
P28 J.A. Bergstra, J. Heering, P. Klint (1988). *Module Algebra, (revised version).* Programmatuur rapport P8823, Universiteit van Amsterdam, November.
P29 J.A. Bergstra, J.W. Klop (1988). *Process Theory Based on Bisimulation Semantics.* Programmatuur rapport P8824, Universiteit van Amsterdam, November.
P30 P. Borras, D. Clement, J. Despeyroux, F. Dupont, M.H.H. van Dijk, L. Hascoet, J. Heering, P.R.H. Hendriks, J. Incerpi, G. Kahn, P. Klint, J.W.C. Koorn, B. Lang, E.A. van der Meulen, V. Pascual, J. Rekers, L. Rideau (1988). *Fourth Annual Review Report of Esprit Project 348 (GIPE),* December.
P31 J.W. Klop, A. Middeldorp (1988). *An Introduction to Knuth-Bendix Completion.* Report IR-162, VU Amsterdam, September.
P32 P.J.F. Lucas, L.C. van der Gaag (1988). *Principes van Expertsystemen.* Academic Service, Schoonhoven.

Department of Algorithmics and Architecture

Report series

CS-R8804 A. Siebes, M.L. Kersten. *A functional approach to database semantics.*
CS-R8805 M.L. Kersten, A.P.J.M. Siebes, C.A. van den Berg. *Using a graph rewriting system for databases.*
CS-R8806 M.L. Kersten. *A time and space efficient implementation of a dynamic index in a main-memory DBS.*
CS-R8808 E. Kranakis. *Functional dependencies of variables in wait-free programs.*
CS-R8813 M. Li, P.M.B. Vitányi. *Two decades of applied Kolmogorov complexity in memoriam Andrei Nikolaevich Kolmogorov 1903-1987.*
CS-R8817 G. van Rossum. *STDWIN - A standard window system interface.*
CS-R8828 I.J.P. Elshoff. *A distributed debugger for Amoeba.*
CS-R8836 P. Clote, E. Kranakis. *Boolean functions, invariance groups and parallel complexity.*

Publications in Journals, proceedings, etc.

A1 P.M.G. Apers, M.L. Kersten, H.C.M. Oerlemans (1988). PRISMA Database Machine: A Distributed, Main-Memory Approach; Research Issues and a Preliminary Architecture. *Proc. Extending Database Technology Conference,* Venice, Italy.
A2 B. Awerbuch, L. Kirousis, E. Kranakis P.M.B. Vitányi (1988). A proof

technique for register atomicity. *Proc. 8th Conf. Found. Software Techn. & Theoret. Comp. Sci.*, Lecture Notes in Computer Science, vol. 338, 286-303.

A3 J.M. BACON, C. HORN, A. LANGSFORD, S.J. MULLENDER, W. ZIMMER (1988). MANDIS: Architectural Basis for Management. R. SPETH (ed.). *Proc. of the EUTECO 88 Conf., Vienna, Austria, April 1988*, North-Holland, 795-809.

A4 H. BALSTERS, M.M. FOKKINGA (1988). Subtyping can have simple semantics. *Proceedings van SION conferentie CSN 88, Vol. 1*, 181-195.

A5 M. CARRASQUER, D. DRAPER, L. MEERTENS, S. PEMBERTON (1988). *Euromath Functional Specification*. Euromath Deliverable, Task 5.

A6 J.T. JEURING. Finding palindromes. *Proceedings van SION conferentie CSN 88, Vol. 1*, 123-140.

A7 J.T. JEURING (1988). On classes of run-time functions. *Proceedings van SION conferentie CSN 88, Vol. 2*, 335-351.

A8 M.L. KERSTEN, F.H. SCHIPPERS (1988). Using the Guardian Programming Paradigm to Support Database Evolution. R.A. MEERSMAN, A.C. SERNADAS (eds.). *Data and Knowledge (DS-2)*, North-Holland, 189-201.

A9 L. KIROUSIS, E. KRANAKIS, P.M.B. VITÁNYI (1988). Atomic multireader register. *Proceedings 2nd International Workshop on Distributed Algorithms*, Lecture Notes in Computer Science, Vol 312, Springer-Verlag, Berlin, 278-296.

A10 E. KRANAKIS, P.M.B. VITÁNYI (1988). Weighted distributed Match-Making. *Proceedings 3rd Agean Workshop on Computing: VLSI Algorithms and Architectures*, Lecture Notes in Computer Science, vol. 319, Springer-Verlag, Berlin, 361-368.

A11 M. LI, P.M.B. VITÁNYI (1988). Tape versus stacks and queue: the lower bounds. *Information and Computation, 78*, 56-85.

A12 M. LI, P.M.B. VITÁNYI (1988). Two Decades of applied Kolmogorov Complexity: In memoriam Andrei Nikolaevich Kolmogorov 1903 - 1987. *Proc. 3rd IEEE Structure in Complexity Theory Conference*, Washington D.C., 80-101.

A13 M. LI, P.M.B. VITÁNYI (1988). Kolmogorovskaya slozhnost': dvadsat' let spustia. *Uspekhi Mat. Nauk*, 43:6, 129-166 (= *Russian Mathematical Surveys*).

A14 S.J. MULLENDER, P.M.B. VITÁNYI (1988). Distributed Match-Making. *Algorithmica, vol. 3*, 367-391 (Special 'Distributed Computing' issue).

A15 S. PEMBERTON (1988). Progress towards ABC. *ABC Newsletter nr. 6*, 2-3.

A16 S. PEMBERTON (1988). Approximate numbers. *ABC Newsletter nr. 6*, 7-11.

A17 R. VAN RENESSE, J.M. VAN STAVEREN, J. HALL, M. TURNBULL, B. JANSSEN, J. JANSEN, S.J. MULLENDER, D. HOLDEN, A. BASTABLE, T. FALLMYR, D. JOHANSEN, K.S. MULLENDER, W. ZIMMER (1988). MANDIS/Amoeba: A Widely Dispersed Object-Oriented Operating System. R. SPETH (ed.). *Proc. of the EUTECO 88 Conf., Vienna, Austria, April 1988*, North-Holland, 823-831.

A18 J. SEIFERAS, P.M.B. VITÁNYI (1988). Counting is easy. *Journal Ass. Comp. Mach. 35*, 985-1000.

A19 K. SIKKEL, N. VERBRUGGE (1988). Belofte en rede ter toelichting op de belofte. *Informatie vol. 30, nr. 6*, 422-425.

A20 M.P.M. VAN DE VEN, P.M.B. VITÁNYI (1988). Een marktgerichte aanpak van de structurele werkeloosheid. *Economisch Statistische Berichten 73*, 1001-1004, 1010.

A21 P.M.B. VITÁNYI (1988). Locality, communication and interconnect length in multicomputers. *SIAM J. on Computing, 17*, 659-672.

A22 P.M.B. VITÁNYI (1988). A modest proposal for communication costs in multicomputers. S.K. TEWKSBURY, B.W. DICKINSON, S.C. SCHWARTZ (eds.). *Concurrent Computations, Algorithms, Architecture, and Technology*, Plenum Press, New York, 203-216.

A23 P.M.B. VITÁNYI (1988). Andrei Nikolaevich Kolmogorov. *CWI Quarterly, 1*, 3-18.

Other publications

A24 P.M.G. APERS, M.L. KERSTEN, C.A. VAN DE BERG, P. GREFEN, M. HOUTSMA, E. VAN KUIJK, R. VAN DE WEG, A. WILSCHUT (1988). *Design Deliverable of PRISMA/DB*. PRISMA Report P0294.

A25 H.E. BAL, J.G. STEINER, A.S. TANENBAUM (1988). *Programming Languages for Distributed Systems*. Vrije Universiteit, Faculteit Wiskunde en Informatica, Report IR-147, February.

A26 C.A. VAN DE BERG (1988). *The OFM-OFM Interface: Design Document*. PRISMA Report P0248.

A27 C.A. VAN DE BERG (1988). *The OFM-OFM Interface*. PRISMA Report P0249.

A28 C.A. VAN DE BERG, P. GREFEN (1988). *The TM-OFM Interface*. PRISMA Report P0250.

A29 C.A. VAN DE BERG, M.L. KERSTEN, P.M.G. APERS, P. AMERICA (1988). *Language Support for Implementing a Distributed Main Memory Database System*. PRISMA Report P0376.

A30 M.A.W. HOUTSMA, H.J.A. VAN KUYK, J. FLOKSTRA, P.M.G. APERS, M.L. KERSTEN (1988). *A Logic Query Language and its Algebraic Optimization for a Multiprocessor Database Machine*. Memorandum INF-88-52, Universiteit Twente.

A31 JACK JANSEN, PETER BOSCH, JAN-HEIN BÜHRMAN. *The Coffee Server*. Internal paper, April.

A32 A.P.J.M. SIEBES, M.L. KERSTEN (1988). *PRISMA & Statistical Databases.* PRISMA Report P0312.

Department of Interactive Systems

Report series

CS-R8802 V. AKMAN, P.J.W. TEN HAGEN, A.A.M. KUIJK. *A vector-like architecture for raster graphics.*

CS-R8818 A.A.M. KUIJK, P.J.W. TEN HAGEN, V. AKMAN. *An exact incremental hidden surface removal algorithm.*

CS-R8819 V. AKMAN, P.J.W. TEN HAGEN. *The power of physical representations.*

CS-R8829 J. VAN DER VEGT, H.F.J.M. BUFFART, C.C. VAN LEEUWEN. *The 'Structural Memory'; a network model for human perception of serial objects.*

CS-R8841 H.J. SCHOUTEN, P.J.W. TEN HAGEN. *Dialogue cell resource model and basic dialogue cells.*

Publications in Journals, proceedings, etc.

I1 V. AKMAN (1988). Geometry and Graphics aplied to Robotics. R.A. EARNSHAW (ed.). *Theoretical Foundations of CAD and Computer Graphics,* Springer-Verlag, 619-638.

I2 V. AKMAN (1988). Geometric Computing and Robotics. R.A. EARNSHAW (ed.). *Techniques in Computer Graphics and CAD,* Springer-Verlag.

I3 V. AKMAN, P.J.W. TEN HAGEN (1988). R.A. EARNSHAW (ed.). The Power of Physical Representations. *Preprints of the Second Eurographics Workshop on Intelligent CAD Systems, April 1988, Veldhoven,* 175-198.

I4 V. AKMAN, P.J.W. TEN HAGEN (1988). The Power of Physical Representations. V. AKMAN, P.J.W. TEN HAGEN, P.J. VEERKAMP (eds.). *Intelligent CAD Systems 2: Implementational Issues, Proceedings of the Second Eurographics Workshop on Intelligent CAD Systems, EurographicSeminars Series,* Springer-Verlag.

I5 V. AKMAN, P.J.W. TEN HAGEN, A.A.M. KUIJK (1988). A Vector-like Architecture for Raster Graphics. A.A.M. KUIJK W. STRASSER (eds.). *Advances in Computer Graphics Hardware II,* EurographicSeminars Series, Springer-Verlag, 137-154.

I6 V. AKMAN, P.J.W. TEN HAGEN, J.L.H. ROGIER, P. VEERKAMP (1988). Knowledge engineering in design. *Knowledge-based Systems, vol. 1, no. 2,* March.

I7 M. BAKKER (1988). Adding Name Sets and Workstation Filters to GKS: a Future Extension. *Computer Graphics Forum, 7,* 3-7.

I8 P. BERNUS, P.J.W. TEN HAGEN, P.J. VEERKAMP, V. AKMAN (1988). IDDL: The Language of a Family of Intelligent, Integrated, and Interactive CAD Systems (IIICAD). *Preprints of the Second Eurographics Workshop on Intelligent CAD Systems, April 1988, Veldhoven,* 35-65.

I9 E.H. BLAKE (1988). Report on the Third Eurographics Workshop on Graphics Hardware. *Computer Graphics Forum, vol. 7, nr. 4,* 361-362.

I10 W.R. FRANKLIN, V. AKMAN (1988). Adaptive grid for polyhedral visibility in object space: An implementation. *The Computer Journal, Vol. 31, No. 1.*

I11 W.R. FRANKLIN, N. CHANDRASEKHAR, M. KANKANHALLI, M. SESHAN, V. AKMAN (1988). Efficiency of uniform grids for intersection detection on serial and parallel machines. *Proceedings Computer Graphics International '88, Geneva, May 1988.*

I12 W.R. FRANKLIN, N. CHANDRASEKHAR, M. KANKANHALLI, M. SESHAN, V. AKMAN (1988). Efficiency of uniform grids for intersection detection on serial and parallel machines. N. MAGNENAT-THALMANN, D. THALMANN (eds.). *New Trends in Computer Graphics,* Springer-Verlag.

I13 I. HERMAN, J. REVICZKY (1988). Some Remarks on the Modelling Clip Problem. *Computer Graphics Forum, vol. 7, nr. 4,* 265-271.

I14 A.A.M. KUIJK, P.J.W. TEN HAGEN, V. AKMAN (1988). An Exact Incremental Hidden Surface Removal Algorithm. A.A.M. KUIJK, W. STRASSER (eds.). *Advances in Computer Graphics Hardware II, EurographicSeminars,* Springer-Verlag, 21-37.

I15 C.C. VAN LEEUWEN, H.F.J.M. BUFFART, J. VAN DER VEGT (1988). Sequence influence on the organisation of meaningless serial stimuli: economy after all. *Journal of Experimental Psychology: Human Perception and Performance, 14,* 481-502.

I16 R. VAN LIERE (1988). User Interface Management System. M.M. DE RUITER (ed.). *Advances in Computer Graphics III, EurographicSeminars Series,* Springer-Verlag, 99-133.

I17 R. VAN LIERE (1988). A model for interaction. R.A. EARNSHAW (ed.). *Fundamental Algorithms for Computer Graphics, NATO ASI Series,* Springer-Verlag, 517-543.

I18 D.B.M. OTTEN (1988). Knowledge base aspects for the IIICAD-system. *Proceedings of the 2nd IFIP WG 5.2 Workshop on Intelligent CAD,* UK.

I19 H.J. SCHOUTEN, P.J.W. TEN HAGEN (1988). Dialogue Cell Resource Model and Basic Dialogue Cells. *Computer Graphics Forum, vol. 7, nr. 4,* 311-322.

I20 P.J. VEERKAMP, V. AKMAN, P. BERNUS, P.J.W. TEN HAGEN (1988). IDDL: A Language for Intelligent Interactive Integrated CAD Systems. V. AKMAN, P.J.W. TEN HAGEN, P.J. VEERKAMP (eds.). *Intelligent CAD Systems 2: Implementational Issues, Proceedings of the Second Eurographics Workshop on Intel-*

ligent CAD Systems, EurographicSeminars Series, Springer-Verlag.
I21 P.J. VEERKAMP (1988). Multiple Worlds in an Intelligent CAD System. H. YOSHIKAWA, D. GOSSARD (eds.). *Intelligent CAD: Record of the first IFIP WG 5.2 Workshop on Intelligent CAD,* North-Holland.
I22 P.J. VEERKAMP (1988). The Multi-world mechanism in IDDL (Integrated Data Description Language). *Proceedings of the Second IFIP WG 5.2 Workshop on Intelligent CAD, UK.*
I23 J. VAN DER VEGT, H.F.J.M. BUFFART, C.C. VAN LEEUWEN (1988). The 'Structural Memory'; a network model for human perception of serial objects. *Psychological Research, vol. 50 nr. 4.*

Other publications

I24 V. AKMAN, P.J.W. TEN HAGEN, P.J. VEERKAMP (eds.) (1988). *Intelligent CAD Systems 2: Implementational Issues, Proceedings of the Second Eurographics Workshop on Intelligent CAD Systems, Eurographic Seminars Series,* Springer-Verlag.
I25 M. BAKKER (1988). *GKS-3D, The Graphical Kernel System for Three Dimensions,* ISO 8805.
I26 M. BAKKER (1988). *GKS-3D/C, The Graphical Kernel System for Three Dimensions Language Bindings, Part 4: C,* ISO/IEC Initial Draft 8806-4; ISO/IEC Working Draft 8806-4.
I27 M.M. DE RUITER (ed.) (1988). *Advances in Computer Graphics III,* EurographicSeminars Series, Springer-Verlag.