Euler Institute for Discrete Mathematics and its Applications
ANNUAL REPORT 1999

Preface

To the outside world, EIDMA's activities and achievements in 1999 may have looked very similar to those in 1998. Nevertheless, these activities and achievements are worth to be mentioned here. In this annual report one can find a complete overview.

Prof.dr. K.A. Schouhamer Immink was awarded the Edison Medal by the IEEE for a career of creative contributions to the technologies of digital video, audio and data recording. He also received the AES Gold Medal from the Audio Engineering Society for significant contributions to the advancement of consumer audio technology.

Nine of EIDMA's graduate students received a Ph.D. degree in 1999. In the past they have profited from EIDMA's graduate curriculum consisting of regular courses, minicourses, and seminars. EIDMA was fortunate to have found Prof.dr. N. Alon from Tel-Aviv University willing to give a minicourse on "The probabilistic method". Similarly, Prof.dr. P.V. Kumar from USC lectured on "Quaternary codes and designs" and Prof.dr. R. Kannan from Yale University on "Low rank approximations of matrices and applications".

To celebrate EIDMA's first lustrum, a two-day symposium was organized in Mierlo on October 7 and 8. Many young members used the opportunity to present their work to the other participants. Invited speakers were Prof.dr. R. Ahlswede from the University of Bielefeld, Prof.dr. J.L. Massey, emeritus professor from the ETH Zürich, and Prof.dr. K. Mehlhorn from Max-Plank Institute in Saarbrücken. They gave overviews that inspired many attendees.

In 1999, EIDMA started the preparations of the renewal procedure of her recognition by the Royal Netherlands Academy of Arts and Sciences. The peer reviews that came as part of this procedure were very favorable. That should serve as encouragement to us to continue with our efforts.

Prof.dr.ir. H.C.A. van Tilborg
Scientific Director EIDMA

Contents

1 Structure and Composition of EIDMA

1.1 Organizational Structure

- Board of Governors:
  - Prof.dr. A.M. Cohen, Technische Universiteit Eindhoven, Department of Mathematics and Computing Science (chairman).
  - Prof.dr. C. Hoede, Universiteit Twente, Faculty of Applied Mathematics.
  - Prof.dr. A. Schrijver, Centrum voor Wiskunde en Informatica.
  - Dr. J. Simonis, Technische Universiteit Delft, Faculty of Information Technology and Systems.
  - Dr. F.M.J. Willems, Technische Universiteit Eindhoven, Department of Electrical Engineering.
- Scientific Director: Prof.dr.ir. H.C.A. van Tilborg, Technische Universiteit Eindhoven, Department of Mathematics and Computing Science.
- Secretary: Ir. H.J.M. Wijers, Technische Universiteit Eindhoven, Department of Mathematics and Computing Science.
- Management assistant: H.A.M. Houben-Verhees, Technische Universiteit Eindhoven, Department of Mathematics and Computing Science.
- Scientific Board:
  - Prof.dr. E.H.L. Aarts, Philips Research, Eindhoven (chairman).
  - Prof.dr.ir. J.P.L. Vandewalle, Katholieke Universiteit Leuven, Department of Electrical Engineering, Belgium.
  - Prof.dr. J.A. Thas, Universiteit Gent, Department of Pure Mathematics and Computer Algebra, Belgium.
  - Prof.dr.ir. A.J. Vinck, Institut für Experimentelle Mathematik, Essen, Germany.
  - Prof.dr. F. Buekenhout, Université Libre de Bruxelles, Department of Mathematics, Belgium.
  - Prof.dr. J.K. Lenstra, Technische Universiteit Eindhoven, Department of Mathematics and Computer Algebra.
  - Prof.dr. A.E. Brouwer, Technische Universiteit Eindhoven, Department of Mathematics and Computer Algebra.
  - Dr. G. Sierksma, Rijksuniversiteit Groningen, Quantitative Logistics Research Group.

1.2 Participating Groups

In 1999, EIDMA consisted of the following groups and persons:

- Technische Universiteit Eindhoven, Department of Mathematics and Computing Science, Discrete Mathematics Group:
  - dr. A.G. van Asch, dr. S.M. Ball, prof.dr. A. Blokhuis, prof.dr. A.E. Brouwer, dr. O. Caprotti, prof.dr. A.M. Cohen, dr. F.G.M.T. Cuypers, dr. G. Ivanyos, prof.dr.ir. C.J.A. Jansen, prof.dr. J.H. van Lint (emeritus), dr. G.R. Pellikaan, dr.ir. L.A.M. Schoenmakers, prof.dr. J.J. Seidel (emeritus), prof.dr. J. Simonis, dr. H.J.M. Sterk, prof.dr.ir. H.C.A. van Tilborg, dr. R. Ushirobira, dr. E.R. Verheul, dr.ir. H.A. Wilbrink, S.-B. Xu.
  - PhD students: P.H.T. Beelen, J. Doumen, J. Draisma, R. Gramlich, J. Keuning, M. Lavrauw, A.J. de Man, S.M. van Rijnswou, M. Smeets.

- Technische Universiteit Eindhoven, Department of Mathematics and Computing Science, Combinatorial Optimization Group:
  - prof.dr.ir. A.M.H. Gerards, dr.ir. C.A.J. Hurkens, prof.dr. J.K. Lenstra, dr. R.A. Pendavingh, dr. L. Stougie.
  - PhD students: R.M.F. Schilham, P. Schuurman, S.R. Tiourine, T. Vredeveld.
- Technische Universiteit Eindhoven, Department of Electrical Engineering, Information and Communication Theory Group:
  - dr. V. Balakirsky, H.M.C. Creemers, prof.dr. J.P.M. Schalkwijk (emeritus), dr.ir. Tj.J. Tjalkens, dr.ir. F.M.J. Willems.
  - PhD students: M.S. Bargh, Y. Guo, H.B. Meeuwissen, A. Nowbakth-Irani, P.A.J. Volf.
- Technische Universiteit Delft, Faculty of Information Technology and Systems, Department of Technical Mathematics and Informatics:
  - dr.ir. R.W. Goldbach , dr. A.G.M. Maks, prof. dr. J. Simonis, prof.dr.ir. T.H.M. Smits, dr. A.J. van Zanten.
  - PhD students: S. Guritman P.S. Kazakov, A. Lukito,.
- Universiteit Twente, Faculty of Applied Mathematics, Group Algebra and Discrete Mathematics:
  - dr.ir. H.J. Broersma, dr. T.S.H. Driessen, prof.dr. C. Hoede, drs. A.A. Jagers, dr. J.C.M. Keijsper.
  - PhD students: S. Uttunggadewa.
- Center for Mathematics and Computer Science (CWI), Amsterdam,
  Research group "Networks and Logic - Optimization and Programming":
  - prof.dr.ir. A.M.H. Gerards, dr. J.H. Koolen, dr. A.V. Kotlov, dr. M. Laurent, prof.dr. J.K. Lenstra, dr. R. Rizzi, prof.dr. A. Schrijver.
  - PhD students: H. Elbers, T. Fleiner.
- Universiteit Gent, Department of Pure Mathematics and Computer Algebra:
  - prof.dr. F. De Clerck, dr. G. Cornelissen, prof.dr. J. Van Geel, prof.dr. H. Van Maldeghem, prof.dr. W. Mielants, prof.dr.
    R. Puystjens, prof.dr. L. Storme, prof.dr. J.A. Thas.
  - PhD students: L. Brouns, B. De Bruyn, M. Delanote, F. Gardeyn, E. Govaert, E. Kuijken, L. Kuijken, L. Luyckx, V. Vermeulen, C. De Volder, K. Zahidi.
- Katholieke Universiteit Leuven, Department Electrical Engineering-ESAT, Group Computer Security and Industrial Cryptography (COSIC):
  - dr. K. Martin, dr. S. Nikova, prof.dr.ir. B. Preneel, dr.ir. V. Rijmen, dr.ir. M. Vandenwauver, prof.dr.ir. J. Vandewalle.
  - PhD students: J. Borst, A. Bosselaers, J. Claessens, D. De Cock, W. Moreau, J. Nakahara, B. Van Rompay, F. Vercauteren, E. De Win, K. Wouters.
- Katholieke Universiteit Brabant, Department of Econometrics:
  - dr. E.R. van Dam, dr.ir. W.H. Haemers, dr.ir. M.J.P. Peeters.
- Université Libre de Bruxelles, Département de Mathématique:
  - Service de Géometrie: prof.dr. F. Buekenhout, dr. C. Cerf, prof.dr. J. Doyen, dr. M.J. Dehon, dr. C. Huybrechts, D. Leemans.

– Faculté des Sciences Appliqueés: Dr. D. Buset, prof.dr. A. Delandtsheer.
– Mathématiques Générales: prof.dr. J.P. Doignon.
– Calcul Symbolique sur Ordinateur: Dr. J. Sengier.
– Laboratoire d'Informatique Th/'eorique: prof.dr. Y. Roggeman.
– Mathématiques de la Gestion: dr. St. Chrétien, D. De Wolf, dr. B. Fortz, dr. Ph. Fr. Geurts, dr. Ph. Grégoire, prof.dr. M. Labbé, dr. N. Mladenovic, dr. J.L. Ottinger, dr. M. Pinar.

  PhD students:
– Service de Géometrie: P. Cara, A. Devillers, M. Sebille, M. Salazar.
– Faculté des Sciences Appliqueés: C. Archer.
– Mathématiques Générales: S. Fiorini.
– Calcul Symbolique sur Ordinateur: Y. Delhaye, St. Louies.
– Mathématique de la Gestion: S. Dewez, G. Fasbender, C. Feremans, H. M'elot, Ch. Nocq, I. Rodriguez-Martin, Chr. Wynants, H. Yaman. M. Salazar.

- Universität Gesamthochschule Essen, Institut for Experimental Mathematics, Digital Communication Group:
  – prof.dr. H. Stichtenoth, dr. V.T. Tran, prof.dr.ir. A.J. Vinck. prof.dr.ir. K.A. Schouhamer Immink.
  – PhD students: V. Canda, P. Gober, O. Harmjanz, C. Haslach, J. Häring.
- Rijksuniversiteit Groningen, Quantitative Logistics Research Group:
  – dr. D.P. van Donk, prof.dr.ir. G.J.C. Gaalman, dr. D. Ghosh, prof.dr. B. Goldengorin, prof.dr. R.J.J.M. Jorna, prof.dr. W.K. Klein Haneveld, drs. M.J. Land, drs. J. Riezebos, prof.dr.ir. C. Schweigman, prof.dr. G. Sierksma, prof.dr.ir. J.L. Simons, dr.ir. J. Slomp, prof.dr. J.A.A. van der Veen, dr. V. Venugopel, dr. M.H. van der Vlerk, prof.dr. J. Wijngaard.
  – PhD students: A. Budihardjo, S. Drijver, H.C. Heesen, G.A. Tijssen, W. van Wezel, H.T.L. Wanders, G. Xiang.
- Philips Research Laboratories, Eindhoven:
  – prof.dr. E.H.L. Aarts, dr.ir. C.P.M.J. Baggen, dr.ir. M.E. van Dijk, dr. S. Egner, A. Gorokorov, dr.ir. E.B. Hekstra, dr.ir. H.D.L. Hollmann, ir. F.L.A.J. Kamperman, ir. A.G.C. Koppelaar, dr.ir. J.H.M. Korst, ir. J.P. Lenoir, dr.ir. J.P.M.G. Linnartz, ir. W.P.A.J. Michiels, J. Talstra, dr.ir. L.M.G.M. Tolhuizen, dr.ir. W.F.J. Verhaegh, dr.ir. A. van der Werf.
- Philips Crypto B.V., Eindhoven:
  – drs. J. Brands, ir. G. Damen, ir. E.J. Eichhorn, prof.dr.ir. C.J.A. Jansen, dr.ir. C.L.M. van Pul, dr.ir. P. Roelse, ir. M. Sas, dr.ir. M. Struik, ir. M. van Weert.
- KPN Research, Leidschendam & Groningen.
  – dr.ir. A.P. Hekstra, dr. H.J.M. Joosten, F. Muller, ir. S.C.L. Prins, ir. S.J. Vlaar.

2 EIDMA courses, seminars and meetings in 1999

In 1999, EIDMA organized the following courses, seminars and meetings:

- Regular Courses:
  - Advanced Graph Theory (in cooperation with the Thomas Stieltjes Institute for Mathematics), spring 1999.
  - Combinatorial Optimization 1 (in cooperation with the Dutch Network on the Mathematics of Operations Research (LNMB)), autumn 1999.
  - Discrete Algebra and Geometry 2, winter 1999/2000.
  - Coding Theory, Information Theory and Cryptology 3, winter 1999.
- Minicourses:
  - Prof. N. Alon, Tel-Aviv University, Israel, *The Probabilistic Method*, Eindhoven, February 8-12, 1999.
  - Prof. P.V. Kumar, USC, California, USA, *Quaternary Codes and Sequences*, Eindhoven, June 7-11, 1999.
  - Prof. R. Kannan, Yale University, USA, *Low-Rank Approximation of Matrices and Applications*, May 31-June 4, 1999.
- Seminars:
  - Combinatorial Theory Seminar, Technische Universiteit Eindhoven, every Wednesday afternoon.
  - bi-monthly seminar Coding, Crypto and Information Theory, Technische Universiteit Eindhoven.
  - bi-monthly Cryptography Working Group, Utrecht.
  - bi-weekly Optimization Seminar, Technische Universiteit Eindhoven.
- EIDMA was (co)-organizor of the following meetings:
  - EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 7 and 8, 1999.
  - Geometric and Algebraic Combinatorics, An international conference in honour of J.J. Seidel on the occasion of his 80th birthday, SBI-Conferentiecentrum Boschoord, Oisterwijk, August 15-20, 1999, organized by Departement Econometrie KUB, EIDMA, KNAW, NWO, Vakgroep Wiskunde TUE.
  - 4th Workshop on Models and Algorithms for Planning and Scheduling Problems (MAPSP99), Renesse, June 14-18, 1999.

3 Research Activities

The research activities of EIDMA concentrate on three main topics:

- Discrete algebra and geometry,
- Coding theory, information theory and cryptology,
- Combinatorial optimization, combinatorial algorithms and graph theory.

We first give a short description of these three areas of research and then, in the subsequent sections, list the contributions of the various research groups in these areas.

Discrete algebra and geometry

Design theory
Existence results, constructions and possible unicity of finite discrete structures with a given specification (often by means of some parameters). The structures can be classical block designs, but also association schemes, mutually orthogonal Latin squares, etc.

Geometry
The study of the geometry of groups of Lie type, buildings (introduced by Tits) and the diagram geometries of Buekenhout. Constructions, characterizations and classification problems of incidence geometries such as generalized polygons, near polygons, (semi)partial geometries are part of the research activities. Also included are combinatorial problems concerning point sets in finite projective planes and spaces, especially blocking sets and arcs as well as characterizations of quadric and Hermitian Veronese varieties.

Algebra
The classical relation between algebra and geometry enables the use of algebra to solve geometric problems. In particular need to be mentioned linear algebra, group theory, Clifford algebras and, to a lesser degree, number theory and topology.

Computer-algebraic methods
Algebra viewed as the study of operations on sets can, when the computer is able to perform these operations, be supported by expert systems, formula-manipulation, searching software, as well as classical computations. The study of the methods to realize this is the focus of this project.

Coding theory, information theory and cryptology

Source coding
Determining the most efficient (shortest) way to represent a certain amount of information. Designing algorithms that realize such a representation.

Channel coding
Representing an amount of information, that makes reliable transmission possible. Designing algorithms, that realize reliable transmission.

Coding methods for communication networks
The study of source and channel coding, encoding and addressing (protocols) in networks.

Cryptology
Protecting information against unauthorized access (privacy), determining if a message has been altered by a third party (integrity), adding a signature to an electronic document and verifying the identity, all by mathematical means.

Combinatorial optimization, combinatorial algorithms and graph theory

Algorithms for NP-hard problems
The development and analysis of optimal and suboptimal algorithms for NP-hard problems.

Polynomial algorithms, combinatorics and graph theory
The design and analysis of optimization algorithms that have a polynomial-bounded complexity. The application of these algorithms.

Graph-theoretic problems
Graph theory deals with a variety of different problems. We mention functions that transform graphs into graphs like line graphs, topics like perfect graphs, cycle coverings of graphs and homomorphisms of graphs, the relation between graphs and cooperative games, and graph theoretic applications in knowledge-technology and social sciences.
A different area concerns the representation of graphs, metric graph theory (with emphasis on shortest paths), the relation between geometric and algebraic structures, applications in discrete location theory and the theory of (dynamic) searching in graphs.

Cycles and paths in graphs
The existence of Hamilton cycles in graphs and, more general, of cycles and paths with particular properties.

3.1 Discrete Algebra and Geometry

3.1.1 Technische Universiteit Eindhoven, Faculteit Wiskunde en Informatica, Sectie Discrete Wiskunde

- **A.M. Cohen**
  Some progress has been made with the book 'Diagram Geometry' (joint with Buekenhout).

  Work on Distance-transitive graphs with various collaborators has led to an almost complete classification of the affine case.

  Joint work with Cuypers and Sterk has resulted in a classification of linear groups generated by reflection tori.

  Joint work with O. Caprotti and H. Elbers has led to a standard for OpenMath, a survey of existing technology and a draft typing mechanism of OpenMath objects.

  In joint work with A. Steinbach, R. Ushirobira and D. Wales, more insight is obtained into Lie algebras generated by extremal elements. In joint work with G. Ivanyos, a connection of these Lie algebras with geometric recognition theorems is studied.

  With R. Ushirobira, a Buchberger algorithm for non-commutative Gröbner bases has been implemented in GAP4. It was used to explore the universal enveloping algebra of a Lie algebra generated by 5 extremal elements.

- **F.G.M.T. Cuypers**
  The joint work with A. Steinbach (University of Giessen, Germany) on linear groups generated by transvections has been continued. An almost complete classification of linear groups generated by an abstract class of root-subgroups whose elements are transvections has been obtained.

  Weak embeddings of Fischer spaces and Delta spaces have been studied.

  The geometric hyperplane of the $M_2 4$-near hexagon have been classified. This is joint work with Andries Brouwer and Ernst Lambeck.

  A β-version of an interactive 'Voorkennistoets' has been produced.

  Work on a new version of the book 'Algebra Interactive' in cooperation with Arjeh Cohen, Hans Sterk, Olga Caprotti, Michael Kohlhase (Universität Saarbrücken).

3.1.2 Technische Universiteit Delft, Faculteit Technische Wiskunde en Informatica

The research of geometries related to buildings has been completed with the PhD-thesis of Blok. The thesis deals with two subjects, namely, the spanning of shadow spaces of buildings by small sets of points and the subgeometry of a building consisting of flags far away from a given flag. Among other things, using a computation in the Coxeter group it is shown that for the shadow space belonging to a node of the diagram that corresponds to a so-called minimal weight the set of points on a apartment forms a minimal set. It is also shown that in almost all cases the subgeometry far from a flag is connected.

3.1.3 Katholieke Universiteit Brabant, Faculteit der Economische Wetenschappen

- E.R. van Dam
  - construction of uniformly packed codes, association schemes and distance-regular graphs from highly non-linear functions.
  - construction of association schemes, in particular fissions of the triangular scheme.
- W.H. Haemers
  - Bicliques.
  - Spectral characterization of graphs.
  - Constructions of combinatorial designs.
- M.J.P. Peeters
  - p-ranks and binary codes of distance regular graphs

3.1.4 Université Libre de Bruxelles, Département de Mathématique

- Service de mathématiques:
  - F. Buekenhout: The flag-transitive geometries of small simple groups and primitive groups (joint with M. Dehon, Ph. Cara, D. Leemans, M. Salazar). Polyhedra with various degree of regularity (with E. Dony). History of Incidence Geometry, Polar spaces, Generalized Polygons, Polyhedra. Book project "Diagram Geometry" (with A.M. Cohen).
  - Ph. Cara: Study of residually weakly primitive flag-transitive geometries of the alternating and symmetric groups as well as groups PSL(2,q) for q=11,13 and 17. Study of inductively minimal and Petersen geometries.
  - C. Cerf: Knot theory: pure and applied to chemistry and molecular biology. Development of invariants for knots. Fullerenes. Chirality.
  - M. Dehon: Study of the residually weakly primitive flag-transitive geometries of various primitive permutation groups (joint with F. Buekenhout, Ph. Cara and D. Leemans). Study of reaction graphs (with F. Buekenhout and J. Brocas).
  - A. Devillers: Classification of d-homogeneous and d-ultrahomogeneous relational structures such as linear spaces, semilinear spaces and designs.
  - J. Doyen: Automorphism groups of t-designs. Homogeneous structures. History of Mathematics.
  - C. Huybrechts: Reduction of diagram geometries over Coxeter diagams extended by linear spaces. Constructions of diagram geometries and embeddings in projective spaces. Dimensional dual hyperovals. Gated graphs.
  - D. Leemans: Study of the residually weakly primitive flag-transitive geometries of the Suzuki groups and various other groups. Study of regular thin geometries. Diagram geometries. Implementation of a module on Incidence Geometry in MAGMA.

- M. Salazar: Construction of bipartite graphs with prescribed girth and diameter. Classification of RWPRI rank two geometries for the simple groups PSL(2,q)(joint with D. Leemans and F. Buekenhout).
- M. Sebille: Study of t-designs and their automorphism groups. Study of polynomial Kramer-Mesner matrices. Designs invariant under a given primitive permutation group.

- Service de mathématiques et d'informatique générales:
  - J.P. Doignon: Finding facets of convex polytopes associated to families of orders.
  - S. Fiorini: Polyhedral combinatorics of order polytopes: facets, graph and automorphisms of the linear ordering polytopes, the linear signed order polytopes, the weak order polytopes, the partial order polytopes, and related families of polytopes. General methods for the interpretation and generation of valid inequalities for 0/1-polytopes: Chvatal-Gomory cuts, lift-and-project, sum & strengthen.

- Computer Algebra:
  We are interested in systems of first order ODE's that belong to the so called quasi-monomial (QM hereafter) class. These systems read:

$$\dot{x}_i = \lambda_i x_i + x_i \sum_{j=1}^{M} A_{ij} \prod_{k=1}^{N} x_k^{B_{jk}}$$

where λ_i, A_{ij} and B_{jk} are complex numbers, and M denotes the number of quasi-monomials $\prod_{k=1}^{N} x_k^{B_{jk}}$ that appear in the system (eventually, M can go to infinity). This class of systems is thus quite general(it contains notably polynomial and analytical systems).

The attractive fact about the notation used here-above is that, the adding of the following variables to the system:

$$x_{N+j} = \prod_{k=1}^{N} x_k^{B_{jk}},$$

(doing so, we increase the dimension by M), leads to the following system:

$$\begin{aligned} \dot{x}_i &= \lambda_i x_i + x_i \sum_{j=1}^{M} A_{ij} x_{N+j} & (i = 1...N) \\ \dot{x}_{N+j} &= (B \circ \lambda)_j x_i + x_{N+J} \sum_{p=1}^{M} (B \circ A)_{jp} x_{N+p} & (j = 1...M) \end{aligned}$$

which is of the well known Lotka-Volterra (LV hereafter) form.

We can now perform several operations on this last system without loosing any information on the original system, since the first N variables of the LV system are precisely the variables of the QM system

Let us now list a few results that have been obtained recently with the use of the QM formalism:

  - The Taylor series: In most cases, the nonlinearity of the system is such that the recursion relations defining the Taylor series coefficients of the solutions, induce an amount of operations growing as the exponential of the order. In the case of the LV system, it has been shown that this number of operations behaves as the order to the power two. Moreover, the general coefficient of the Taylor series can be explicitly written.
  - Perturbation series: The situation is quite the same as for the Taylor series (which can be seen as a particular case of perturbation series): one is able to write the explicit coefficient and quadratic recursion relations for the series obtained by considering the nonlinearity of the LV system as a perturbation.

– Normal forms: The normal form approach is one of the most powerful tools for local analysis of fixed point. It consists in finding a diffeomorphism that maps the system onto its linear part. Of course, this objective cannot always be reached: when a resonance condition is satisfied on the linear part, no diffeomorphism will linearize the system. The objective is then to remove as much nonlinearity as we can. Doing so, we build what is called the normal form of the system. The transformation that maps the system onto its normal form is obtained as a multi-variables Taylor series, called the Poincaré series.

  Again, the simple form of the LV system allows the explicit writing of the Poincaré series (in the non resonant case). Moreover particular changes of time parameterization allow to study fixed points at infinity.

– Invariants: Formal invariants can be explicitly constructed around fixed points. They are obtained as Taylor series of the variables. It can also be shown that a resonance for the fixed point will in general make several invariants disappear.

– Resummations: Resummation process have been obtained for all the series given above. These resummations often accelerate the convergence of the series, and can sometimes be used to simplify the structure of the series.

  An important class of resummed forms of the Taylor series can be obtained: the Padé approximants which are usually denoted $[0/M]$ (they are of the form $c/P^M(x)$, where c is a constant, and $P^M(x)$ is a polynomial of degree M). With the use of those, it is possible to obtain a good approximation of the radius of convergence, either of the Taylor series, or of the Padé approximants themselves.

Reference:

S.Louies, "General properties and resummations of series expansions for nonlinear dynamical systems", PhD thesis, Université Libre de Bruxelles, September 2000. (and references therein).

- Faculté des Sciences Appliquées:

  – A. Delandtsheer: Line-transitive finite linear spaces with a point-imprimitive automorphism group.

  – C. Archer: Study of group extensions for elaborating effective methods for constructing nonsolvable groups.

3.1.5 Universiteit Gent, Vakgroep Zuivere Wiskunde en Computeralgebra

- L. Brouns:
  Characterization of finite Moufang hexagons. Interesting pointsets in generalized quadrangles and hexagons.

- G. Cornelissen:
  Arithmetic geometry: global function fields, moduli-problems, automorphic forms, non-archimedean uniformization, diophantine sets.

- B. De Bruyn:
  Near polygons: constructions, characterisations, projective and affine embeddings. Distance regular graphs.

- F. De Clerck:
  Constructions and characterizations of finite incidence structures and their adjacency graphs, with the emphasis on (semi)partial geometries, generalized quadrangles, and near polygons. Spreads of (semi)partial geometries. Distance regular graphs. Conical flocks.

- M. Delanote:
  Constructions and characterisations of (semi)partial geometries.

- C. De Volder:
  Very Ampleness and Gauss Maps of Linear Systems on Blowings-up of Projective Varieties.

- F. Gardeyn:
  Galois representations associated to Drinfeld modules.

- E. Govaert:
  Characterizations of generalized hexagons using regularity properties; characterizations of the Hermitian Spread in the split Cayley Hexagon $H(q)$.

- E. Kuijken:
  Regular two-graphs: geometric constructions, connection with partial geometries and with codes.

- L. Kuijken:
  Fuzzy projective spaces from fuzzy groups. Fibred projective planes, fibred generalized polygons.

- D. Luyckx:
  m-systems of finite classical polar spaces: connection with generalized polygons, SPG-reguli and the BLT-property, constructions and characterizations.

- W. Mielants:
  Countable relational structures whose age satisfies the strong ammalgamation property. Countable discrete random linear orders.

- R. Puystjens:
  Linear algebra. Drazin invertibility of products.

- L. Storme:
  Study of substructures in finite projective spaces. The research was focussed on: Partial s-spreads in $PG(N, q)$, Codes meeting the Griesmer bound, Multiple blocking sets in $PG(2, q)$, Caps in finite projective spaces, Covers of quadrics and of classical generalized quadrangles, Rédei-type k-blocking sets in $PG(N, q)$, $N \geq 3$, MDS codes over finite rings, Packing and covering groups with subgroups.

- J.A. Thas:
  Generalized quadrangles of order (s, s^2). Ovoids and spreads of generalized quadrangles and generalized hexagons. Embeddings of polar spaces and generalized polygons. Extensions of generalized quadrangles. Arcs and caps in $PG(n, q)$. Partial m-systems and m-systems of polar spaces. Constructions of (semi)partial geometries.

- J. Van Geel:
  Quadratic forms and division algebras over function fields.

- H. Van Maldeghem:
  Classification of embeddings of generalized hexagons of order $(q, 1)$ in $\mathrm{PG}(d, q)$; classification of embeddings of the dual split Cayley generalized hexagons $\mathrm{H}(q)^{dual}$ in $\mathrm{PG}(13, q)$. Combinatorial and group related characterizations of the Hermitian spreads in the generalized hexagon $\mathrm{H}(q)$. Elementary constructions of small generalized polygons. Epimorphisms between generalized n-gons and generalized m-gons with $n \neq m$. The Cherlin-Zil'ber conjecture for BN-pairs with panels of Morley rank 1.

- V. Vermeulen:
  Twin buildings.

- K. Zahidi:
  Undecidability in number theory.

3.1.6 Universität Gesamthochschule Essen, Institut für experimentelle Mathematik

Prof. Dr. Trung van Tran

- **Discrete Algebra:**
  General construction methods for combinatorial structures are topics of investigation. New bounds for t-directed Steiner systems and the existence of t-packings and t-directed Steiner systems are our main interests. Directed Steiner systems are considered as perfect deletion correcting codes.

  Generic recursive construction methods for 3-designs have been proposed. This general approach appears to be very powerful. An interesting fact of the methods is that infinitely many families of non-trivial simple 3-designs can be derived from the trivial designs.

- **Cryptography:**
  One of our interests in this research field is the designing of block ciphers with a mathematical foundation. The aim is to develop a class of scalable symmetric cryptosystems using binary permutation groups. The system utilizes the profilic existence of certain bases with respect to which such groups can be factorized. The idea on which the encryption is based is a mapping of group elements between two random bases. Security investigation and experimental implementation of the system are important parts of this undertaking.

Prof. Dr. Henning Stichtenoth
Several constructions of algebraic-geometric codes, construction of codes meeting the Tsfasman-Vladut-Zink bound. Explicit equations for asymptotatically good towers of algebraic function fields.

3.2 Coding Theory, Information Theory and Cryptology

3.2.1 Technische Universiteit Eindhoven, Faculteit Wiskunde en Informatica, Sectie Discrete Wiskunde

Algebraic graph theory
Locally Paley graphs were investigated, and for a large number of orders all locally Paley graphs were determined. All hyperplanes of the M24 near polygon were determined. Antidesigns in the classical association schemes were studied. Work on two books (distance-regular graphs and strongly regular graphs) was continued.

Cryptography
A variant of the Diffie-Hellman scheme in a field extension of degree 6 is given in which the number of bits exchanged is one third of what is used in the classical DH scheme, while the offered security against attacks known today is equal to the one offered by the standard DH scheme.

A new class of systematic authentication codes was constructed. It is based on sets of affine transformations applied to the coordinates of the words in error-correcting codes.

A new authentication protocol for portable communication systems was devised.

A new textbook on cryptography has been completed. Its electronic version is a Mathematica notebook, which makes it possible for students to run and change all examples.

Existing algorithms to count the number of points on an elliptic curve (Schoof, Elkies and Atkin) have been implemented.

A study has been made of NCount. This is a method for value transfer, based on one-way chaining. A concrete application (called content metering) has been worked in greater detail.

Toggling has been introduced as a new concept in electronic voting. It gives the voter the possibility to change his vote as long as the voting process continues. A connection has been made between the underlying technique and group signatures, a special class of digital signatures.

A novel approach to digital certificates has led to a PhD thesis. Implementation will have significant and attractive (in terms of privacy) consequences for public key infrastructures.

A prototype for electronic voting has been refined and extended with methods resulting from research into publicly verifiable secret sharing schemes. The prototype is also used for in-class demonstrations of internet elections.

Advanced protocols for secure time-stamp servers have been developed. An example application of secure time-stamp servers is to handle priority of patent filings in a fair and secure way.

An efficient two-party protocol for testing equality of bit strings (socialist millionaires' problem) has been developed.

The Differential Power Analysis attack has been performed for a specific smart card.

Coding theory
A new (minimum distance) decoding algorithm for linear codes has been described. The complexity of this algorithm for long linear codes is exponentially smaller than of all other known methods.

Small quaternary codes were investigated.

Necessary and sufficient conditions were found for a collection of 2-spaces over $GF(2)$ to be 1-spaces over $GF(4)$.

Tables and data bases of small codes, linear or not, were constructed, extended and maintained.

A PhD thesis on codes has been completed. Major topics are quasicyclic codes (constructions, their decoding), optimal cyclic burst correcting codes and Reed-Muller codes (generalized Hamming weights).

A formula for the redundancy of improved geometric Goppa codes is derived for a certain class of curves in terms of the Weierstrass semigroup.

Baker's formula for the genus of plane curves in terms of the Newton-polygon of the defining polynomial is generalized, and many examples of curves with many rational points with low genus are given.

The structure of order domains is investigated.

3.2.2 Philips Crypto B.V.

Research activities:

- J. Brands:
  Key management and protocols.
- G. Damen:
  Network security mechanisms and architectures.
- E. Eichhorn:
  Design, analysis and implementation aspects of cryptographic algorithms.
- C. Jansen:
  Design and analysis of efficient symmetric cryptographic algorithms, mechanisms and crypto ASICs.

- P. Roelse:
  Design, analysis and implementation of blockcipher algorithms and implementation of public key routines.
- M. Sas:
  Cryptographic applications of elliptic curves over finite fields.
- M. van Weert:
  Key management and authentication protocols; X.509 certificate structures.

3.2.3 Philips Research Labs., Eindhoven

- C.P.M.J. Baggen:
  Coding theory, communication and information theory.
- M.E. van Dijk:
  Coding theory and cryptology.
- E.B. Hekstra-Nowacka:
  Coding theory.
- H.D.L. Hollmann:
  Discrete mathematics, information theory.
- F.L.A.J. Kamperman:
  Cryptography, security.
- A.G.C. Koppelaar:
  Coding theory.
- J.P. Lenoir:
  Cryptography, security.
- J.P.M.G. Linnartz:
  Research on the appliaction of cryptography and electronic watermarking.
- J. Talstra:
  Research in application of cryptology—and to a lesser extent coding—for content protection in consumer electronics.
- L.M.G.M. Tolhuizen:
  Coding theory, information theory.

3.2.4 KPN research Lab., Leidschendam

- A.P. Hekstra:
  Development of an objective distortion measure that agrees with human perception for speech signal transported over the Internet or mobile networks, that is speech signals possibly affected by time varying transmission delay.
- J.H. Hoepman:
  Cryptographic protocols for smart cards and security of networks.
- H.J.M. Joosten:
  Refinement and design of new smartcard systems.
- F. Muller:
  Design of smart card systems.

- S.C.L. Prins:
  Electronic commerce, security aspects.

- S. Vlaar:
  Design of topologics for ATM and IP networks.

3.2.5 Technische Universiteit Eindhoven, Faculteit Electrotechniek

Source and Channel Coding
Programme members : dr.ir. F.M.J. Willems, Associate Professor
dr.ir.Tj.J. Tjalkens, Assistant Professor
prof.dr.ir. P. Schalkwijk, Guest
ir. P.A.J. Volf, PhD student
ir. M. Shoae Bargh, PhD student
A. Nowbakht, PhD student
Y. Guo, MSc., MTD student
dr. V.B. Balakirsky , Post Doc
ing. H. Creemers, Technical Research Assistant

Programme design in brief
The mission of the research programme is the study of the fundamental limitations in communications and the techniques (coding methods) that aim at achieving these limits.

In a communication system information is either transmitted or stored. Information and communication theory is concerned with fundamental limits in transmission and storage. The first objective of the sub-programme "Source and Channel Coding" is to establish such limits, the second is to develop efficient methods that approach these limits as closely as possible. Source coding is concerned with removing redundancy from data such that the original data can be exactly reproduced from the encoded data (noiseless source coding, compaction), or with removing irrelevancy from the original in which case some distortion between the reproduction and the original data is introduced (lossy coding, compression). In both the noiseless and the lossy case the research objective is to find techniques (codes) that are universal, i.e. achieve a high compaction or compression without knowing the source statistics in advance, and that have a low implementation cost.
Channel coding is adding redundancy to data that are to be transmitted over a channel. This is done in such a way that possible channel errors can be corrected. While in the past researchers concentrated on finding the best error-correcting codes for the simplest channels, the objective is now to find codes that allow efficient decoding procedures, often for channels with a more complex structure.

Overview of scientific results
Source Coding
During the period April 1 till July 31 Dr. Tj. Tjalkens visited the Information Technology Department of the University of Lund, Sweden. There he worked on several problems in the field of noiseless (universal) source coding. Topics of discussion were the behaviour of various estimators in context algorithms, in particular the redundancy introduced by the "escape mechanism", the modelling of video-generating sources, and the complexity redundancy behaviour of optimal codes (Huffman, Tunstall) for memoryless sources.
In particular the work on the complexity of Huffman codes was successful and gave surprising results. In this work the relation between the redundancy, defined as the difference in bits between the expected codeword length of a code and the source entropy, and the storage and computation cost was studied. The Huffman codes are the best possible codes among all codes with a fixed number of variable-length code words.
This combined very well with results obtained in 1998 for the Tunstall codes, which are the best possible codes when variable length source sequences are coded by fixed-length code words.
Both codes, Huffman and Tunstall, are originally described in terms of rooted complete trees and

implementations based on trees have similar redundancy/memory cost relations, under the condition that the computational cost is constant per source letter. Applying enumerative, i.e. exact computation, techniques one derives from Huffman codes the so called "Minimal Redundancy Codes" and from Tunstall codes the "Petry Codes". The redundancy/memory cost relation now improves exponentially. By relaxing the precision of the computations an even better trade-off is achieved, again almost exponentially better. Surprising is that for the enumerative approach the behaviour of the Minimal Redundancy Codes and the Petry Codes are dissimilar. For Petry codes the redundancy drops proportional to the square root of the storage cost, while the redundancy of the Minimal Redundancy Codes only decreases with the cubic root. Moreover the part of the code implementation responsible for this cost is precisely the part mainly ignored in the literature, namely the ordering of the source sequences.

We have addressed the problem of estimating the maximal cumulative redundancy of universal coding. This has lead to a non-asymptotic lower bound for Bernoulli sources with an unknown parameter. The bound can be used in the fixed-to-variable and variable-to-variable case. The approach can be directly generalised to the other source models.

Channel Coding
Research on the additive white Gaussian noise channel with Shannon-type of side-information was started again. A new technique which may be called 'quantisation coding' was developed. This method results in considerable improvements over the bounds that we obtained in 1988. Parallel research, motivated by our 1988 paper, has been initiated in Israel (Technion). Moreover it became clear in 1999 that these results are relevant for embedding information in host signals (watermarking, data hiding).

We have developed a maximum-likelihood decoding algorithm for messages transmitted over a binary symmetric channel by means of low-density parity-check code. The sequential decoding algorithm is based on a tree structure consisting of possible noise vectors. It determines a maximum-likelihood path in this tree using a special metric function. An upper bound on the exponent of the expected number of computations in the ensemble of low-density codes has been given. It was shown that it is much less than the exponent related to exhaustive search.

A study was started of the problem of joint source-channel coding when variable length codes are used for information transmission over a discrete memoryless channel. The data transmitted over the channel are interpreted as pairs (m(k),t(k)) where m(k) is the message generated by the source and t(k) is the time instant when the transmission of the k-th code word begins. The decoder constructs the estimate of the transmitted sequence of pairs, and the k-th decoding error is introduced as the event that the pair (m(k),t(k)) does not belong to this sequence. We describe the maximum-likelihood decoding algorithm and prove a lower bound on the exponent of decoding error probability. For a subclass of discrete memoryless sources and discrete memoryless channels this bound is tight.

Multi-user information theory
A code was constructed for the two-user binary-adder multiple-access channel that gives results that are very close to the known theoretical limits.

In another study results were obtained that can serve as tools for constructing a theory of searching with lies.

Cryptology aspects of data transmission over the binary multiplying channel were addressed. The combinatorial problem was solved of computing the conditional entropy of a common key that can be constructed by the communicating participants when an eavesdropper knows the channel output sequence.

A coding procedure was developed that allows one to represent integers by binary vectors (code words) in such a way that addition is replaced with the OR operation. The code word of the sum was constructed using the decoding algorithm. As a result, many of the transformations may be realised using parallel processing. The method can be considered as a competitor to existing computer arithmetic.

The PhD project "Coding Strategies for channels with feedback" was completed with a dissertation. The thesis describes transmission methods that can de used for communication over additive white Gaussian noise channels with feedback. These methods could be applied for transmitting data over telephone lines.

Programme development

Source Coding
In the coming year the difference of behaviour of the enumerative codes will be studied in more detail.

The PhD project on the development of a text-compression system based on the context-tree weighting method will be completed with a thesis. This will be a so-called "promotie op proefontwerp".

A PhD study on model-estimation techniques was started at the end of 1999. In 2000 the Ph.D. student will study the literature in this field and in the field of universal noiseless source coding. The objective of this project is to apply source coding methods to estimate the model corresponding to a data-set.

Channel Coding
We will continue our research on low-density parity-check codes and joint source-channel coding. A post-doctoral fellow and an AIO-2 will be working on this project in 2000.
Research on side-information channels and embedding of information in data-streams will be continued in 2000. The emphasis is not only on obtaining capacity-results but also on finding codes for practical situations.

Co-operation with external organisations:

- K.U. Leuven, I.P.P.I Moscow, Council for Cybernetics Moscow, and I.P.I.A. Erevan: INTAS project "Mathematical and Statistical Research in Information Theory and Telecommunications".
- University of Lund (prof. Smeets) and University of Electro-Communications in Tokyo (prof. Kawabata): universal source coding problems.
- KPN research: context-tree weighting algorithm.
- Philips Research and Philips Semiconductors: efficient decoding algorithms for convolutional codes.

3.2.6 Technische Universiteit Delft, Faculteit Technische Wiskunde en Informatica

Many polynomials haven been found for which the corresponding CRC codes perform better in comparison with existing standards, like IEEE and ATM. For spherical codes Boyvalenkov's method has been implemented in the program SCOD. This yielded quite a few upper bounds on the size of spherical codes. New methods have been found for the construction of self-dual codes over fields of size 2^r and 3. As for optimal linear codes the non-existence of several binary linear codes of dimension nine and of ternary and quaternary codes has been established. A new set of constraints for the weight distribution of general linear codes has been found. This promises to produce a major breakthrough in solving the problem of optimal linear codes over larger alphabets. A very general technique, based on the standard Gray code and on some simple tools from linear algebra, was developed for the construction of certain distance preserving $< m, n >$-codes (circuit codes). An iterative solution was found for the ranking and unranking problem for the construction of these codes. For snake-in-the-box-codes ($< 2, n > -codes$) new upper bounds were derived for their maximal length. First a new upper bound was established by refining Snevily's method counting edges not in the snake. Later this bound was improved by combining the methods of Soloveva and of Zemor, estimating the number of 4-cycles and the number of 3-claws outside the snake. The standard Towers-of-Hanoi problem with 3 pegs can be solved with elementary combinatorics. If there are more than 3 pegs the optimal strategy for the solution of the problem is unknown. Sarkar's recursive algorithm for solving the generalised Tower-of-Hanoi problem with 4 pegs was proved to be optimal. A method was developed for constructing all non-equivalent optimal algorithms solving this problem. Iterative versions of these algorithms were derived as well.

3.2.7 Katholieke Universiteit Leuven, Departement Elektrotechniek–ESAT

The goal of COSIC's research activities is to create an electronic equivalent for primitives in the physical world such as confidentiality, signatures, identification, anonymity, notarization, and payments. To achieve this goal, the research concentrates on the design, evaluation, and implementation of cryptographic algorithms and protocols, and on the development of security architectures for computer systems and telecommunications networks. COSIC's *theoretical work* on cryptographic algorithms and protocols is mainly based on discrete mathematics (a.o. number theory, finite fields, Boolean functions, finite geometry, and coding theory); other fields of mathematics relevant to our research include statistics and optimization. The goal is to achieve efficient and (provably) secure solutions. COSIC intends to integrate these solutions into different *applications* including computer systems, telecommunications systems (Internet security, mobile communications), and payment systems. Important aspect here are the efficient implementation (in both software and hardware) of cryptographic primitives and the security evaluation of components and systems including smart cards. COSIC provides *consultancy* in the area of computer security and cryptography.

COSIC organized its two-yearly international summer course on Computer Security and Industrial Cryptography on June 1–4, 1999.

COSIC collaborates closely with the company Utimaco Belgium. COSIC also cooperates with the University of California at Los Angeles, the University of Bergen, Queensland University of Technology, University of Klagenfurt, Entrust Technologies, RSA Laboratories, the Dutch organization for Applied Scientific Research (TNO), University of Wollongong, University of Adelaide, Université Catholique de Louvain, Vodafone Ltd, Siemens-ATEA, Giesecke & Devrient, Panafon SA, Royal Holloway University of London, Siemens AG, Banksys, Europay International, ICRI, Imec, Proton World International, Roularta N.V., S.W.I.F.T., SmartMove, PriceWaterhouseCoopers, Philips, and Ubizen. Some important projects are:

- EC—ACTS: Advanced Security for Personal Communications Technologies (1995-1999)
- OSTC–TIMESEC: Digital Time-Stamping and the Evaluation of Security Primitives (1996–1999)
- OSTC–EPV: Electronic PV (1998–2000)
- OSTC–FATIMA: Federal Action on Telematics withIn Modern Administrations (FATIMA) (1998–1999)
- IWT–IT MOL: Information-Technology - Media On-line (1996–1999)
- FWO–OSABA: Open Security Systems for agent-based applications (1999–2002).

COSIC's current research and project information, publication list, and recent papers are available at `http://www.esat.kuleuven.ac.be/cosic/`.

3.2.8 Universität Gesamthochschule Essen, Institut für experimentelle Mathematik

Prof.dr.ir. K.A. Schouhamer Immink
Research is mainly done in codes for mass data storage.
Prof. Dr.ir. Han Vinck

- **Random Access Communications:** We investigated a particular method of random access communications for asynchronous multiple access. We compared the classical synchronous capacity with the respective asynchronous capacities for three different types of multi-user channels: the OR, the OR with intensity information and the XOR. We assume that the number of active users (inputs) T is large. In particular, we show that for instance, for M-ary input asynchronous access, multiple user interference reduces the capacity for the OR channel, from $(M-1)$ to $(ln2)(M-1)$ bits per transmission. However, for the OR with intensity information the channel capacity reduces from $\log_2(T+1)$ to 0.82 bits per transmission. For the binary input XOR, the capacity reduces from 1 to 0.32 bits per transmission. We derive the capacity achieving transmission method for the M-ary input OR channel and compare the presented method with earlier results.

- **Power Line Communications:** We investigated the question: At what rates can we use the 220 V power-lines for communications? We estimated the capacity to be about 1 Mbit/sec for the CENELEC band 9-94 kHz. The power-line communication channel is one of the practical channels where Shannon theory partly gives an answer to the question about channel capacity. From measurements it followed that the logarithm of the noise power spectral density is a linear decreasing function of the frequency. We could apply the "water-filling" arguments to show that the channel can be used at a data rate of about 1 Mbit/sec. on a bandwidth of 100 kHz. In practice it means that most of the power should go to the higher frequency region. We presented these results on the "2nd International Symposium on Power-Line Communications and its Applications" in Japan. Another question that needs to be answered is the art of modulation that is suited for the 220 V channel. The answer is that modulation schemes with a constant envelope signal modulation such as binary-FSK and M-ary FSK are in agreement with the CENELEC norms, EN 50065.1, part 6.3.2. In our research at the moment we focus on the low frequency range below 150 kHz. In this region, there are several channel characteristics like attenuation, permanent frequency disturbances and impulsive noise that need special attention. The main goal is to show that a combination of M-ary FSK modulation and coding can provide for a constant envelope modulation signal, frequency spreading to avoid bad parts of the frequency spectrum, and time spreading to facilitate correction of frequency disturbances and impulse noise simultaneously. A transmission scheme combining 4-FSK modulation with diversity and coding can make the transmission over power lines robust against permanent frequency disturbances and impulse noise. We suggest simple non-coherent detection and derive the corresponding error correcting capabilities of the scheme. Since we use 4-FSK, the scheme is in agreement with the existing CENELEC norms. The scheme can be considered as a form of coded Frequency Hopping and is easy extendable to any frequency range.

3.3 Combinatorial Optimization, Combinatorial Algorithms and Graph Theory

3.3.1 Technische Universiteit Eindhoven, Faculteit Wiskunde en Informatica, Sectie Besliskunde en Stochastiek

Combinatorial Optimization

a. Polyhedral Combinatorics.
A thesis entitled 'Decision Support by Combinatorial Optimization' has been completed by S.R. Tiourine. Several chapters deal with algorithms based on approximately solving combinatorial problems, such as packing (for cutting stock problems), and graph coloring (frequency assignment). Algorithms for cutting stock, and for statistical disclosure protection, were partly based

on polyhedral models.

b. Alternatives for polyhedral methods.
Progress has been made in the study of the advantages of using reformulated models based on basis reduction. In particular for the so-called Market Split problem, we have been able to accurately predict the number of feasible solutions to problem instances drawn from a reasonable probability distribution. We now try to understand the connections between the growth of the binary branch-and-bound search trees and the determinants of the lattices generated.

Within the research project with Delft, Rotterdam and Utrecht, performance of approximation algorithms for a scheduling problem based on a semi definite relaxation has been tested empirically against various local search methods.

c. Local search.
Commonality-based restarts for local search heuristics. A common way to enhance a local search heuristic is performing multiple independent runs, each started in different solution. Instead of starting a new run from scratch, we construct an initial solution by perturbing the best solution found so far. Building elements that are common to many solutions found by preceding runs are preserved with high probability. For the TSP and the JSSP, existing local search heuristics are improved by the commonality-based restart mechanism.

First results were obtained in performance guarantees for local search methods for some scheduling problems. Research into the complexity of the local search strategies mentioned is continued.

d. New models and methods for routing problems.
Together with the research school BETA, a project on routing problems is executed. A classification of the problems has been made. The map of computational complexity is still under construction, but a lot of questions have been solved by now. On the field of on-line routing some alternative models have been proposed to oppose the usual adversary models used in this field for performance quality measures.

Together with Feuerstein from Buenos Aires first results on competitive analysis for on-line dial-a-ride problems have been derived.

e. New models and methods for scheduling problems.
For several scheduling problems the approximability status has been determined by either constructing polynomial time approximation schemes or proving in-approximability by means of the gap-technique. This was joined work with Woeginger from Graz.

Together with Feuerstein from Buenos Aires and Mydlarz from Rutgers University the competitiveness of multi-threaded on-line scheduling problems has been established.

f. Graph theory and network optimization
We showed the polynomial-time solvability of the capacitated version of a path-packing problem of Mader using the ellipsoid method for linear programming. Further research will be directed at finding a combinatorial algorithm for this problem. We investigated the class of graphs that can be embedded in 3-space without knotted circuits. In particular, we found forbidden minors for this class.

3.3.2 Université Libre de Bruxelles

Service de Mathématiques de la Gestion

- *Park and Ride Integrated System: Région de Bruxelles-Capitale / Stratec / G.R.T. (FUNDP Namur)/S.M.G. (March 1997 / February 1999).*
  The idea is to combine the Park and Ride with a demand-responsive urban shuttles system. The potential user of such a system is the motorist wishing to go to a town-centre for which

the private transport accessibility is - spontaneously or intentionally - restricted. The system to be created should offer the user the following services:

- a guidance towards a peri-urban parking and the disposability of a parking space,
- the access to seat(s) in a shuttle within a low amount of time,
- the arrival at a (bus-)stop not too far from the user's destination,
- at the requested time, and in the same conditions as those of the journey there, the access to a shuttle which will bring the user back to the parking.
- the system is intended to be implemented in the so-called middle size cities which population is comprised between 50.000 and 500.000 habitants.

- *Stockplanner: Inventory management and scheduling in push/pull production systems: A.I. Systems (March 1998 / February 2000)*
  Most steel companies use a variety of sub-processes like continuous casting, hot/cold rolling mill, pickling, painting, etc. Betwen these elemens of the process chain, several inventories typically serve as buffers. The global planning of the chain not only involves the respect of due date and technical constraints but also the "smooth" inventory management, that is, each partial inventory never falls below/grow above predefined thresholds. On the other hand, the global planning does not necessarily require the finest-grain scheduling of orders: an intermediate precision level can be used, and only involve groups of orders or product types. A general strategy is experimented that can reuse local schedulers and establish negotiations between them through time ranges during which events can/have to happen. Apparantly, the same strategy could also be used to first solve the material flow problem which could then be used as a set of constraints for the more precise order scheduling.

- *Bin Packer: 3 dimensional general purpose bin packing software: Steria/Région Bruxelles Capitale/SMG (July 1998 / June 2000).*
  Bin packer will be a software able to handle general 3 dimensional bin packing problems. The first part of the software is devoted to orthogonal problems and is based on the use of 2 different heuristics addressing different sub-problems: a greedy algorithm for managing problems with very few different types of pieces and a tree search algorithm for problems with many different types of pieces. The second part of the software would be devoted to problems involving irregular pieces and thus rely on the use of a geometrical library.

- *Conception and implementation of algorithms for solving routing problems of oil and gas industry (bulk deliveries): BLUEGATE Optimisation Technologies (Second Phase: October 1998 / January 2000).*
  We inspired ourselves from the academical literature on VRP and VRPTW to develop an algorithm to solve routing problems with many difficult paricularities such as: multi-shifts routing, frequent reloads, more than one product planning, prices of products in depots, multi-compartment vehicles, and more. The most important part of the work was to adapt standard procedures known to be good on academical problems, to handle the mentioned particularities. The whole algorithm has been integrated as a black box into a software named DARWIN being sold to the oil and gas industry by BLUEGATE. The first phase of the project has been successful, and a follow-on project has begun in October. This phase is concerned with improvement of the efficiency of used algorithms and adding new functionalities such as on-line modifications, multi-day planning and truck stock feedback regulation.

- *Reliable Telecom network design*
  One group of the Service de Mathématiques de la Gestion is specialized in the application of combinatorial optimization methods to telecommunication network optimization. Several projects were aimed to the formulation of real applications as combinatorial optimization problems, and the resolution of these problems using state-of-the-art techniques such as branch-and-bound, branch-and-cut, Lagrangean relaxation or tabu search methods.

  Problems studies include:

- Design and routing in backbone telecommunication networks.
- Ring protection design problem in zonal networks.
- Multiplexing and dimensioning of concentrators in backbone networks.

- *Generalized minimum spanning tree problem.*
  Given an undirected graph whose nodes are partitioned into mutually exclusive and exhaustive node sets, the Generalized Minimum Spanning Tree Problem (GMSTP) is to find a minimum-cost tree which includes exactly one node from each node set. We consider several linear formulations of the GMSTP and their related linear relaxations with the aim of finding a "good" formulation for the development of a Branch and Cut solving method. It is well known that the classical Minimum Spanning Tree Problem (MSTP) is polynomial however its generalized version is NP-hard. A Branch and Bound algorithm is developed using one of the best formulations and a greedy heuristic is implemented yielding an upper bound. This method is implemented in C++ and uses the class library ABACUS. We analyse the facial structure of the polytope associated to the GMSTP with the aim of finding "good" inequalities to strengthen our previous linear formulations. Several families of inequalities which are facet-inducing for the polytope of the GMSTP are investigated.

- *Network synthesis problem.*
  Given a set of requirements, which correspond to single or multicommodity flows, the network synthesis problem consists in determining minimum cost edge capacities in order to satisfy the routing of these requirements. Mathematical formulations of network synthesis problems result in large size integer linear models. We are interested in different aspects of these problems that have been little, if not at all studied in the literature. We analyse the complexity of network synthesis problems with non simultaneous single commodity flow requirements, study the particular case with uniform costs and requirements. For the network synthesis problem with non-simultaneous multicommodity flow requirements, we study different bounds and build integer feasible solutions with a tabu search heuristic. Finally, a practical application is studied, that is, the restoration problem in a partially equipped network.

- *Bilevel bilinear programming.*
  In collaboration with the CRT (Montréal), we consider bilevel bilinear optimization problems where the leader wants to maximize revenues from a taxation scheme, while the follower rationally reacts to those tax levels. In particular, we address complexity issues and study the links of such problems with bilevel linear problems. Special attention is given to the special case of toll-setting.

3.3.3 Centrum voor Wiskunde en Informatica, Amsterdam

Submodular function minimization.
A. Schrijver designed a new, combinatorial algorithm to find the minimum value of a submodular function.

Touching number of convex bodies and equilateral sets.
The following is joined work of J. Koolen, M. Laurent and A. Schrijver. The touching number of a convex body K is defined as the maximum number of translates of K that are pairwise touching; two convex bodies being touching if they meet but their relative interiors are disjoint. For K centrally symmetric, the touching number is equal to the maximum number of equidistant points in the associated normed space having K as unit ball. Kusner (1983) conjectured that the touching number of the k-dimensional cross-polytope (the unit ball of ℓ_1-space)is equal to $2k$. Bandelt, Chepoi and Laurent (1998) have shown that the conjecture holds for $k \leq 3$ and we now settle the case $k = 4$. This conjecture is also related to determining the touching number of the simplex and to finding large antichains in designs.

l_1-embeddibility.

T. Fleiner provided new insights on the l_1-embeddibility problem based on a relation with Fleiner's theorem on symmetric chain covers.

Branch width of graphs and matroids.
Broadly speaking, a graph or matroid has "small width" if it decomposes across noncrossing separations into small parts. Together with J. Geelen (University of Waterloo) and G. Whittle (Victoria University, Wellington), A.M.H. Gerards proved that a class of matroids representable over a fixed finite field and with bounded branch width is well-quasi-ordered under taking minors. This generalizes Robertson and Seymour's result that graphs with bounded tree width (or equivalently, bounded branch width) are well-quasi-ordered under taking minors.

Stability.
T. Fleiner extended the stable matching theorem of Gale and Shapley to partially orders and matroids. It turns out that these results, including Gale and Shapley's, follow from a fixed point theorem of Tarski. It also turned out that a theorem of Sands et al. on monochromatic paths and Pym's linking theorem can easily be derived from Tarski's theorem. Fleiner also extended the linear description of the stable matching polytope as given by Vande Vate and by Rothblum to the matroid-kernel case. T. Fleiner and R. Aharoni observed a connection between a lemma of Scarf and the topological fixed point theorem of Brouwer.

Stable sets.
With M. Conforti (University of Padova), A.M.H. Gerards derived a polynomial time algorithm for the stable set problem in cap-free graphs without even holes. The algorithm is based on a decomposition theorem for these graphs by Conforti, Cornuéjols, Kapoor, and Vušković and uses novel decompositions techniques.

Hypercubes.
A. Kotlov proved that every collection of $2^{d-1}+1$ nodes in the d-dimensional hypercube contains a subcollection that meets every facet of the hypercube and induces a connected subgraph in the skeleton of the hypercube. This was conjectured by Alon, Seymour, and Thomas in 1990. Further, such a subcollection can be chosen of size $O(1.5^d)$.

Using a simple construction, A. Kotlov proves that for every bipartite G the strong product of G and K_2 is a minor of the Cartesian product of G and K_2. In particular, the d-dimensional hypercube has a complete minor on $2^{(d+1)/2}$ vertices if d is odd, and on $3\cdot 2^{(d-2)/2}$ vertices if d is even.

It was conjectured by I. Havel in 1984 and proved by L. Nebeský in 1988 that a subdivision of a star, i.e. a tree with exactly one vertex of degree greater than two, is a spanning tree of the d-dimensional hypercube if and only if some trivially-necessary conditions are satisfied. Recently, Kobeissi and Mollard made a similar conjecture for more complicated trees. A. Kotlov settled their conjecture.

Graph colouring.
Kotlov proved that the complement of minimal counterexample to Hadwiger's conjecture has a matching of size $\lfloor n/2 \rfloor$ (with n the number of vertices). This implies the result of T. Gallai (1963), that the chromatic number of such a counterexample is at most $\lceil n/2 \rceil$. Further, the forementioned complement is homeomorphic to a three-connected graph and has tree width at least four. The same holds for minimal counterexamples to Colin de Verdière's conjecture. The proofs of these results use the Gallai-Edmonds structure theorem. A. Kotlov also provided a short proof of that result.

Triangulations of spheres and balls.
A. Kotlov proved the conjecture of Aharoni and Chudnovsky that every triangulation of the $(d-1)$-sphere can be extended to a triangulation of the d-dimensional ball by a (possibly empty) sequence of adding a vertex of degree at most $2d$. (The special case $d=3$ was settled by A. Kotlov and Aharoni.) Kotlov also proved that a triangulation T of the $(d-1)$-sphere is can be extended to a

triangulation of the d-dimensional ball by adding vertices of degree at most $2d-1$ if and only if it is contained in a triangulation of d-dimensional ball whose one-skeleton is equal to that of T.

Random walks.
Using a mixture of linear algebra and statics, A. Kotlov derives for the context of mechanical systems a generalization of the Coppersmith-Tetali-Winkler identity $H(i,j)+H(j,k)+H(k,i) = H(j,i)+H(k,j)+H(i,k)$ for hitting times of a random walk.

Cuts in graphs.
R. Rizzi strengthened and generalized results of Nagamochi, Ono and Ibaraki concerning the efficient implementation of legal ordering algorithms for minimum cut problem based on multiple node-identifications in legal order computations.

3.3.4 Universiteit Twente, Faculteit der Toegepaste Wiskunde

Graph theoretic problems
Graph theory deals with a variety of different problems. Topics studied in Twente at the moment are: cycle coverings of graphs, independence trees, flows in graphs, edge-colored graphs, cyclic graphs etc., graph-theoretic applications in information technology, telematics, knowledge technology, intelligent networks and social sciences.

Hamiltonian graph theory
The search for conditions for the existence of Hamilton cycles, long cycles and cycles through prescribed vertex and/or edge sets in graphs, sometimes within special classes of graphs such as regular, claw-free or triangle-free graphs, graphs with a certain toughness.

Graph Theory
The results yet obtained can be found in Chapter 4. The group is under reconstruction.

Game Theory
T.S.H. Driessen continued his study of several problems in cooperative game theory.

Application of Graph Theory
The group intends to focus more on applications in Information Technology and Telematics in the direct future.

3.3.5 Philips Research Labs., Eindhoven

- E.H.L. Aarts:
  Title: Design and analysis of combinatorial algorithms for planning and design. Key words: mathematical modeling, computational complexity, combinatorial optimization, scheduling, real-time computing, on-line algorithms.

- S. Egner:
  Research in computer algebra, disk scheduling and coding theory.

- J.H.M. Korst:
  Optimization.

- W.P.A.J. Michiels :
  Study of the problem of ordering a sequence of numbers, such that the maximum sum of k successive numbers is minimized.

- W.F.J. Verhaegh:
  In 1999, the main topic of research has been on scheduling data services over video networks.

Due to the explosive growth of Internet, there is a strong demand for high-bandwidth data connections to the homes. One very interesting option is to use video broadcast networks for that purpose, as they are converted from analog networks into digital ones. By encapsulating IP traffic into DVB/MPEG packets one gets in this way a high downstream bandwidth that can be used for a multitude of digital services. In the Data Broadcast Chain (DBC) project at the Nat.Lab. (group Software Architectures) such a system has been developed, in which IP traffic can be broadcasted over satellite channels.

Since bandwidth is nevertheless a scarce resource (even over video networks) and since the amount of applications and data services is enormous, in contrast to standard broadcasting, it is essential to optimally use the available bandwidth, in order to give an as good as possible service to consumers at home. This induces a scheduling problem, in which one (i.e. a service provider) has to determine when and how to play out data services, within bounds given by the available resources.

So, more specifically, one has to determine for each data service a transmission profile, indicating when it starts, when it ends, and the bit rate that is used during that time interval. This bit rate need not be constant, but it may vary. Secondly, one has to determine for each data service which resources are used for it. As the setup is a chain of resources, not only containing the transmission channel as a resource but also resources such as playout devices, IP encryptors, IP-DVB gateways, etc., playing out a data service occupies several resources at the same time, which all have to be checked for feasibility with respect to their allowed total bit rate and number of simultaneous services.

In the past year we have been working on several parts of the scheduling problem.

– First, we have developed a mathematical model of the scheduling problem, clearly identifying the decision variables and the constraints that have to be obeyed.
– Secondly, we have shown that the problem is formally hard to solve, so we have to opt for a heuristic approach.
– Thirdly, we have been working on a solution approach. The solution approach is roughly as follows. On a top level we are going to use a local search technique to determine the order in which data services are played out, or more specifically, the relative order of the start and end points of the data services. Furthermore, the resource assignment is determined by the local search technique.

On a second level, we determine the absolute times for the start and end points of the data services, and we determine the absolute bit rates that are used during playout, for the given relative time ordering and resource assignment. To this end, we developed a linear programming (LP) approach, using column generation, which determines an optimal absolute time and bit rate assignment. This LP approach has been implemented and tested, and it runs in a reasonable amount of time. It finds a feasible time and bit rate assignment if one exists, and otherwise it finds a time and bit rate assignment that results in a minimal violation of the constraints.

Using this LP subroutine, we next plan to work out the local search technique on the top level, in which iteratively small modifications are made in the relative time order or in the resource assignment, after which we use the LP subroutine to determine whether the minimal associated constraint violation decreases or increases. In this way we try to find a solution without violations.

- A. van der Werf:
  Optimization.

3.3.6 Rijksuniversiteit Groningen, Quantitative Logistics Research Group

Goldengorin has proved the following theorem for a general submodular set function. For any pair of embedded subsets, the difference of their function values is a lower bound for the difference between the unknown optimal values of the corresponding partition defined by these subsets. He has successfully applied a special case of this theorem for a justification of the correctness of the so called dichotomy algorithm and for constructing a data-correcting algorithm for more efficient solving some well known instances of the quadratic cost partition problem on dense graphs.

Sierksma continued his research on the relationships between Markov chains and polytops, the sensitivity analysis of combinatorial optimization problems (with Libura, van der Port, van der Veen). The field with applications concerned packaging in the process industry, and cardboard manufacturing. He started a project on applying OR models for team formation and the development of training programs.

Slomp continued research in the field of cellular manufacturing and flexible systems. He also did some research in the area of process planning. He started a project on human factors in cellular manufacturing and in planning and control of flexible manufacturing systems.

Tijssen continued research in the field of linear optimization (degeneracy degrees, duality between multiplicity and degeneracy, Balinski-Tucker tableaus and their applications) and data-correcting algorithms in combinatorial optimization.

Venugopal continued research in the field of cellular manufacturing and supply chain management. His research in cellular manufacturing resulted in a publication in International Journal of production research Vol.37 and No.14; Besides this he is also in the process of Guest Editing a special issue on Manufacturing Cells to be published in Integrated Manufacturing Systems Journal. He (with Prof.J.A.A. van der Veen) also started researching the area of contract theory and supply chain management.

Van der Vlerk continued research in the field of stochastic integer programming awarded from Dutch Royal Academy of Sciences.

Wanders continued research in the field of production planning and scheduling. He did his research in a solid board production plant. Two main approaches known from literature have been combined: cognitive science and operations research. The final product, a prototype, showed the developed conceptual framework with respect to the fine planning stage. In this project also Gerard J.C. Gaalman, Gerard Sierksma and René J.J. Jorna were involved.

4 Publications in 1999

4.1 Books

- K. Aardal, J.K. Lenstra, F. Maffioli and D.B. Shmoys, *Selected papers of Eugene L. Lawler*, CWI Tract, 126, Amsterdam: CWI, p. 318.
- P. Ashley and M. Vandenwauver, *Practical Intranet Security - Overview of the State of the Art and Available Technologies,* Kluwer Academic Publishers, 1999, ISBN 0-7923-8354-0, p. 244.
- A.M. Cohen, F.G.M.T. Cuypers and H. Sterk (eds.), *Some tapas of computer algebra*, Springer-Verlag, Berlin, Heidelberg, New York, 1999, p. 352.
- A.M. Cohen, F.G.M.T. Cuypers and H. Sterk, *Algebra Interactive*, book and CD-rom, Springer-Verlag, Berlin, Heidelberg, New York, 1999, p. 159.
- G.J.C. Gaalman, J. Slomp and N. Suresh (eds.), *Special issue on integration of process planning with production planning and control of flexible manufacturing systems*, Design, analysis, and operation of manufacturing and assembly systems, vol. II, Kluwer Academic Publishers, Dordrecht/Boston/London, 1999, p. 213.
- K.A.S. Immink, *Codes for Mass Data Storage Systems*, Shannon Foundation Publishers, The Netherlands, 1999, ISBN 90-74249-23-X, p. 350.
- B. Preneel (Ed.), *Secure Information Networks. Communications and Multimedia Security,* Kluwer Academic Publishers, 1999, ISBN 0-7923-8600-0, p. 322.

4.2 Research Articles

- P. Abramenko and H. Van Maldeghem, *Connectedness of opposite-flag geometries in Moufang polygons*, European J. Combin. 20, 1999, 461-468.
- R. Ahlswede nd V.B. Balakirsky, *Construction of uniquely decodable codes for the two-used binary adder channel*, IEEE Transations on Information Theory 45, nr. 1, 1999, 326-330.
- P. Ashley, B. Broom and M. Vandenwauver, *An implementation of secure version of NFS including RBAC*, The Australian Computer Journal, Vol. 31, No. 2, May 1999, 54-62.
- P. Ashley, A. Clark, G. Gaskell and M. Vandenwauver, *Experiences auditing IT security systems*, AUUGN, The journal of AUUG Inc., Vol. 20, No. 4, November 1999, 11-15.
- A. Barg, E. Krouk and H.C.A. van Tilborg, *On the complexity of minimum distance decoding of long linear codes*, IEEE Transactions on Information Theory, 45, 1392-1405.
- B. Baudelet and M. Sebille, *A generalization of a result of Tran van Trung on t-designs*, Jour. Comb. Designs, 7, 1999, 1-6.
- Juergen Bierbrauer, Yves Edel and Ludo Tolhuizen, *New codes via the lengthening of BCH codes with UEP codes*, Finite Fields and Their Applications, Vol. 5, No. 4, October 1999, 345-353.
- A. Blokhuis, S.M. Ball, A.E. Brouwer, L. Storme and T. Szönyi, *On the number of slopes of the graph of a function defined on a finite*, Journal of Combinatorial Theory, Series A, 86, 1999, 187-196.
- A. Blokhuis and A. E. Brouwer, *The universal embedding dimension of the near polygon on the 1-factors of a complete graph*, Designs, Codes and Cryptography, 17, 1999, 299-303.
- A. Blokhuis, L. Storme and T. Szőnyi, *Lacunary polynomials, Multiple blocking sets and Baer subplanes*, J. London Math. Soc., 2, 60, 1999, 321-332.
- T. Böhme, H.J. Broersma and H. Tuinstra, *A note on a conjecture concerning tree-partitioning 3-regular graphs*, Tatra mountains mathematical publications, 18, ISSN 1210-3195, 15-21.

- H.J. Broersma, N. Bruin, J.L. Hurink, L.E. Meester, S.S. op de Beek and J.H. Westhuis, *Throughput of ADSL modems*, CWI quarterly, 46, ISSN 0922-5366, 11-26.
- H.J. Broersma, E.A. Engbers and H. Trommel, *Various results on the toughness of graphs*, Networks, 33, ISSN 0028-3045, 233-238.
- H.J. Broersma and C. Hoede, *Another equivalent of the graceful tree conjecture*, Ars combinatoria, 51, 1999, ISSN 0381-7032, 183-192.
- H.J. Broersma, T. Kloks, D. Kratsch, and H. Müller, *Independent sets in asteroidal triple-free graphs*, SIAM journal on discrete mathematics, 12, 1999, ISSN 0895-4801, 276-287.
- A.E. Brouwer, *An associative block design* $ABD(8,5)$, SIAM Journal on Computing, 28, 1999, 1970-1971.
- A.E. Brouwer and J.H. Koolen, *The distance-regular graphs of valency four*, Journal of Algebraic Combinatorics, 10, 1999, 5-24.
- A.E. Brouwer, R.M. Wilson and Qing Xiang, *Cyclotomy and strongly regular graphs*, Journal of Algebraic Combinatorics, 10, 1999, 25-28.
- B. De Bruyn, *Generalized quadrangles with a spread of symmetry*, European J. Comb. 20, 1999, 759-771.
- B. De Bruyn and F. De Clerck, *On linear representations of near hexagons*, European J. Comb. 20, 1999, 45-60.
- B. De Bruyn and F. De Clerck, *Near polygons from partial linear spaces* Geom. Dedicata 75, 1999, 287-300.
- N.G. de Bruijn, *A model for associative memory, a basis for thinking and consciouness*, In: J. Wiedermann, P. van Emde Boas, and M. Nielsen (Eds.), Automata, Languages and Programming, Springer, Lecture Notes in Computer Science, 1644, 74-89.
- F. Buekenhout, *Les démonstrations: une vision génétique et en spirale*, Mathématique et Pédagogie, no. 124, 1999, 15-43.
- F. Buekenhout and B. Baumeister, *On the classification of flag-transitive* $c.c^*$*-geometries*, Geom. Dedicata 75, 1999, 1-18.
- F. Buekenhout, M. Dehon and D. Leemans, *An atlas of residually weakly primitive geometries for small groups*, Mm. Acad. R. Belg. Cl. Sciences, Coll. 8, Ser.3, Tome XIV, 1999, p. 175.
- F. Buekenhout and D. Leemans, *On a geometry of Ivanov and Shpectorov for the O'Nan sporadic simple group.*, Jour. Comb. Th. (A). 85, 1999, 148-164.
- D. de Caen and E.R. van Dam, *Association schemes related to Kasami codes and Kerdock sets*, Designs, Codes and Cryptography 18, 1999, 89-102.
- D. de Caen and E.R. van Dam, *Fissions of classical self-dual association schemes*, J. Comb. Th. A 88. 1999, 167-175.
- D. de Caen, E.R. van Dam and E. Spence, *A nonregular analogue of conference graphs*, J. Comb. Th. A 88, 1999, 194-204.
- C. Cerf, *Topological chirality of knots and links*, In Chemical Topology, Mathematical Chemistry Vol. 6, D. Bonchev and D.H. Rouvray (eds.), Gordon and Breach Publishers, 1999, 1-33.
- C. Cerf and J. Sengier, *Taxi-choses et taxi-trucs*, Math-jeunes, 91 S, 1999, 10-14 and 33-34.
- A.M. Cohen, *Gröbner bases, an introduction*, In: A.M. Cohen, H. Cuypers and H. Sterk (Eds.), Some Tapas of Computer Algebra, Springer Verlag, Berlin, 1-33.

- A.M. Cohen, F.G.M.T. Cuypers and R.J. Riebeek, *Project: Explorations with the icosahedral group*, In: A.M. Cohen, F.G.M.T. Cuypers and H.J.M. Sterk (Eds.), Some tapas of computer algebra, Springer Verlag, Berlin, 1999, 315-322.
- A.M. Cohen, F.G.M.T. Cuypers and H.J.M. Sterk, *Groups generated by reflection tori*, Canadian Journal of Mathematics, 51, 1999, 1149-1174.
- A.M. Cohen, K. Magaard and S. Shpectorov, *Affine distance-transitive graphs: The cross characteristics case*, European Journal of Combinatorics, 20, 1999, 351-373.
- G. Cornelissen, *Zeros of Eisenstein series, quadratic class numbers and supersingularity for rational function fields*, Math. Ann. 314, nr. 1, 1999, 175-196.
- G. Cornelissen, *Deligne's congruence and supersingular reduction of Drinfeld modules*, Arch. der Math. 72, 1999, 346-353.
- G. Cornelissen, *Stockage diophantien et hypothèse abc généralisée*, C. R. Acad. Sci. Paris, 328, Ser. I, 1999, 3-8.
- I.J. Cox, M. Miller, J.P.M.G. Linnartz and A.C.C. Kalker, *A review of watermarking principles and practices*, Chapter 17 of "Digital Signal Processing for Multimedia Systems", K.K. Parhi and T. Nishitani (eds.), Marcel Dekker, Inc., New York, March 1999, 461-486.
- J. Csirik, J.B.G. Frenk, M. Labbé and S. Zhang, *Two simple algorithms for bin covering*, Acta Cybernetica, vol. 14, 1999, 13-25.
- F.G.M.T. Cuypers, *Voorkennistoets, beta-version*, software product.
- F.G.M.T. Cuypers and A. Steinbach, *Linear transvection groups and embedded polar spaces*, Inventiones Mathematicae, 137, 169-198.
- F.G.M.T. Cuypers, L.H. Soicher and H.J.M. Sterk, *Working with finite groups*, In: A.M. Cohen, H. Cuypers and H. Sterk (ed.), Some Tapas of computer algebra, Berlin, Heidelberg, New York: Springer Verlag, 184-207.
- F.G.M.T. Cuypers, L.H. Soicher and H.J.M. Sterk, *Project: The small Mathieu groups*, In: A.M. Cohen, F.G.M.T. Cuypers and H.J.M. Sterk (Eds.), Some tapas of computer algebra, Springer Verlag, 323-337.
- E.R van Dam, *Three-class association schemes*, J. Alg. Combinatorics 10, 1999, 69-107.
- P. van Dam, G.J.C. Gaalman and G. Sierksma, *Production scheduling across multi-machine packaging lines for the pre-scheduling level*, In: International Journal of Production Research, 1999, 37, nr. 16, 3619-3641.
- M. Dell'Amico, M. Labbé and F. Maffioli, *Exact solution for the SONET ring loading problem*, Operations Research Letters, vol. 25, 1999, 119-129.
- M. Desrochers, C.V. Jones, J.K. Lenstra, M.W.P. Savelsbergh and L. Stougie, *Towards a model and algortihm management system for vehicle routing and scheduling problems*, Decision Support Systems, 25, 1999, 109-133.
- S. Dodunekov, S, Guritman and J. Simonis, *Some new results on the minimum length of binary linear codes of dimension nine*, IEEE Transactions on Information Theory, 45, 1999, 2543-2547.
- T.S.H. Driessen, *Pairwise-bargained consistency and game theory: the case of a two-sided firm*, Topics in Mathematical Economics and Game Theory: Essays in honor of Robert. J. Aumann, Providence, Rhode Island: American Mathematical Society, ISBN 0-8218-0525-8, 65-82.
- T.S.H. Driessen and C. Rafels, *Characterizations of k-convex games*, Optimization, 46, 1999, ISSN 0233-1934, 403-431.

- T.S.H. Driessen, *Membership of values to the core for average-convex TU-games*, Operations Research Proceedings 1998, Berlin: Springer-Verlag, ISBN 3-540-65381-3, 303-311.
- M. van Dijk and L. Tolhuizen, "Efficient encoding for a class of subspace subcodes", IEEE Trans. on Inform. Theory, Vol. 45, No. 6, 1999, 2142-2146.
- Sebastian Egner and Thomas Beth, *How to play* M_{13} (English), J. Designs Codes Cryptography 16, 1999, No. 3, 243-247.
- T. Fleiner, W. Hochstättler, M. Laurent and M. Loebl, *Cycle bases for lattices of binary matroids with no Fano dual minor and their one-element extensions*, Journal of Combinatorial Theory B, 25-38.
- T. Fleiner and T. Jordan, *Coverings and structure of crossing families*, Connectivity augmentation of networks: structures and algorithms, Budapest, 1994, Mathematical Programming Series B, 84, 505-518.
- E.M. Gabidulin and J. Simonis, *Metrics generated by primitive 2-error-correcting binary BCH codes*, Problems of Information Transmission, 35, 1999, 224-230.
- J. Van Geel and V.I. Yanchevski, *Indices of double coverings of genus 1 over p-adic fields*, Annales de la faculté des Sciences de Toulouse, Vol. VIII, nr 1, 1999, 155-172.
- F. Göbel and C. Hoede, *Magic labellings of graphs*, Ars Combinatoria, 51, ISSN 0381-7032, 3-19.
- B. Goldengorin, G. Sierksma, G.A. Tijssen and M. Tso, *The data-correcting algorithm for minimization of supermodular functions*, In: Management Science, 1999, 45, 11, 1539-1551.
- A. Gorokhov, M. Kristensson and B. Ottersten, *Robust blind second order deconvolution*, IEEE Signal Processing Letters, Jan. 1999, 13-16.
- A. Gorokhov and P. Loubaton, *Blind identification of MIMO-FIR systems: a generalized linear prediction approach*, Signal Processing (Elsevier), vol. 73, 1999, 105-124.
- W.H. Haemers, *Minimum resolvable coverings with small parallel classes*, Discrete Mathematics 197/198, 1999, 393-396.
- Dr. W.H. Haemers, M. Erickson, S. Fernando, D. Hardy and J. Hemmeter, *Deza graphs: A generalization of strongly regular graphs*, Journal of Combinatorial Designs 7, 1999, 395-405.
- W.H. Haemers, R. Peeters and J.M. van Rijckevorsel, *Binary codes of strongly regular graphs*, Designs, Codes and Cryptography 17, 1999, 187-209.
- S.L. Hakimi, M. Labbé and E.F. Schmeichel, *Locations on time-varying networks*, Networks, vol. 34, 1999, 250-257.
- C. D'Halluin, G. Bijnens, V. Rijmen and B. Preneel, *Attack on six rounds of crypton*, Fast Software Encryption, LNCS 1636, L.R. Knudsen (Ed.), Springer-Verlag, 46-59.
- C. D'Halluin, G. Bijnens, B. Preneel and V. Rijmen, *Equivalent keys of HPC, Advances in Cryptology*, LNCS 1716, K.Y. Lam, E. Okamoto, C. Xing (eds.), Springer-Verlag, 29-42.
- H.W. Hamacher, M. Labbé and S. Nickel, *Multicriteria network location problems with sum objectives*, Networks, vol. 33, 1999, 79-92.
- H. Handschuh and B. Preneel, *On the security of double and 2-key triple modes of operation*, Fast Software Encryption, LNCS 1636, L.R. Knudsen (ed.), Springer-Verlag, 1999, 215-230.
- B.P. van Heusden and R.J.J.M. Jorna, *Towards a semiotic theory of cognitive dynamics in organizations*, In: Kecheng Liu (ed.), Organizational Semiotics, Kluwer Academic Publishers, Dordrecht/Boston/London, 1999, 142-156.
- B.P. van Heusden and R.J.J.M. Jorna, *Organizational semiotics or: (how) do organizations know?*, In: The Semiotic Review of Books, 10, nr. 1, 1999, 2-5.

- C. Hoede, *A comparison of some conditions for non-hamiltonicity of graphs*, Ars Combinatoria, 51, ISSN 0381-7032, 149-159.
- H. van der Holst, L. Lovász and A. Schrijver, *The Colin de Verdière graph parameter*, Graph Theory and Combinatorial Biology, L. Lovász, A. Gyárfás, G. Katona, A. Recksi, L. Székely (eds.), János Bolyai Mathematical Society, Budapest, 29-85.
- C. Huybrechts, *$L.L^*$-geometries and Dn-buildings*, Discrete Math. 197-198, 1999, 431-451.
- C. Huybrechts and A. Pasini, *Flag-transitive extensions of dual affine spaces*, Contrib. Algebra Geom. 40, 1999, 503-532.
- K.A.S. Immink, *The future of digital audio recording*, Journal AES, vol. 47, 171-172,
- K.A.S. Immink and A.J.E.M. Janssen, *Error propagation effects of enumerative coding schemes*, IEEE Trans on Inform. Theory, vol. 45, no. 7, 2591-2594.
- W.-A. Jackson and K.M. Martin, *An algorithm for efficient geometric secret sharing*, Utilitas Mathematica, Vol. 54, 1998, 127-150.
- D.B. Jaffe and J. Simonis, *New binary linear codes which are dual transforms of good codes*, IEEE Transactions on Information Theory, 45, 1999, 2136-2137.
- A. De Jongh, M. Gendreau and M. Labb'e, *Finding disjoint routes in telecommunications networks with two technologies*, Operations Research, vol. 47, 1999, 81-92.
- R.J.J.M. Jorna, *New opportunities for psychology: signs and information*, In: W. Maiers, B. Bayer, B. Duarte Esgalhado, R. Jorna, E. Schraube (eds.), Challenges to theoretical psychology, Captus Press, North York, Ontario, 1999, 120-128.
- G. Khachatrian and K.A.S. Immink, *Construction of simple runlength-limited codes*, Electronics Letters, vol. 35, no 2, 1999, 140.
- S. Klavzar, J. Koolen and H. Mulder, *Graphs which locally mirror the hypercube structure*, Inform. Process. Lett., 71, 87-90.
- W.K. Klein Haneveld and M.H. van der Vlerk, *Stochastic integer programming: general models and algorithms*, In: Annals of Operations Research, 1999, 85, 39-57.
- L.R. Knudsen and K.M. Martin, *In search of multiple domain key recovery*, Journal of Computer Security, Vol. 6, No. 4, 1998, 219-236.
- L.R. Knudsen and V. Rijmen, *On the decorrelated fast cipher (DFC) and its theory*, Fast Software Encryption, LNCS 1636, L.R. Knudsen (ed.), Springer-Verlag, 81-94.
- L. Kramer and H. Van Maldeghem, *Compact ovoids in quadrangles, I. Geometric constructions*, Geom. Dedicata 78, 1999, 279-300.
- L. Kramer, K. Tent and H. Van Maldeghem, *Simple groups of finite Morley rank and Tits buildings*, Israel J. Math. 109, 1999, 189-224.
- L. Kuijken, H. Van Maldeghem and E. Kerre, *Fuzzy projective geometries from fuzzy groups*, Tatra Mt. Math. Publ. 16, 1999, 95-108.
- D. Leemans, *Some applications of Magma to Finite Geometry and Group Theory*, In: The Magma System for Algebra, Number Theory and Geometry, http://www.maths.usyd.edu.au:8000/u/magma/AboutMagma/node198.html.
- D. Leemans, *The residually weakly primitive geometries of the Suzuki simple group Sz(8)*, In C.M. Campbell e.a. (editors), Groups St Andrews 1997, London Math. Soc. Lect. Notes, 261, 1999, 517-526.
- D. Leemans, *An atlas of regular thin geometries for small groups*, Math. Comp. 68, 1999, 1631-1647.

- D. Leemans, *The rank 2 geometries of the simple Suzuki groups Sz(q)*, Contributions to Algebra and Geometry, 39, 1998, 97-120.
- J.H. van Lint, *The Stan Ackermans Institute*, 1999, SEFI News, 79.
- Jack van Lint and Ludo Tolhuizen, *On perfect ternary constant weight codes*, Designs, Codes and Cryptography, 18, December 1999, 231-234.
- L. Lovász and A. Schrijver, *On the null space of a Colin de Verdière matrix*, Annales de l'Institut Fourier, 49, 1017-1026.
- A.R. Mahjoub and C. Nocq, *On the linear relaxation of the 2-node connected subgraph polytope*, Discrete Applied Mathematics, vol. 95, 1999, 389-416.
- H. Van Maldeghem, *Finite generalized quadrangles as the union of few large subquadrangles*, Discrete Math. 208/209, 1999, 589-605.
- H. Van Maldeghem and K. Van Steen, *Characterizations by automorphism groups of some rank 3 buildings – II: A half strongly-transitive locally finite triangle building is a Bruhat-Tits building*, Geom. Dedicata 74, 1999, 113-133.
- H. Van Maldeghem and K. Van Steen, *Characterizations by automorphism groups of some rank 3 buildings – IV. Hyperbolic p-adic Moufang buildings of rank 3*, Geom. Dedicata 75, 1999, 115-122.
- K.M. Martin and C.J. Mitchell, *Comments on an optimized protocol for mobile network authentication and security*, Mobile Computing and Communications Review, Volume 3, Number 2, 1999, p. 37.
- K.M. Martin, J. Pieprzyk, R. Safavi-Naini and H. Wang, *Changing thresholds in the absence of secure channels*, Australian Computer Journal, Vol. 31, No. 2, 1999, 34-43.
- K.M. Martin, R. Safavi-Naini and H. Wang, *Bounds and techniques for efficient redistribution of secret shares to new access structures*, The Computer Journal, Vol. 42, No. 8, 1999, 638-649.
- K. Metsch and L. Storme, *Partial t-spreads in* $PG(2t+1, q)$, Des. Codes Cryptogr., 18, 1999, 199-216.
- B. Mühlherr and H. Van Maldeghem, *Exceptional Moufang quadrangles of type* $ßF_4$, Canad. J. Math. 51, 1999, 347-371.
- W. Nevelsteen and B. Preneel, *Software performance of universal hash functions*, Advances in Cryptology, LNCS 1592, J. Stern (ed.), Springer-Verlag, 1999, 24-41.
- T. Namekata and T.S.H. Driessen, *The egalitarian non-k-averaged contribution value for TU-games*, International game theory review, 1, ISSN 0219-1989, 45-61.
- G.R. Pellikaan and F. Torres, *On Weierstrass semigroups and the redundancy of improved geometric Goppa codes*, IEEE Transactions on Information Theory, 45, November 1999, 2512-2519.
- B. Preneel, *The state of cryptographic hash functions*, Lectures on Data Security, LNCS 1561, I. Damgård (Ed.), Springer-Verlag, 1999, ISBN 3-540-65757-6, 158-182.
- B. Preneel, *State-of-the-art ciphers for commercial applications*, Computers & Security, Vol. 18, No. 1, 1999, 76-74.
- B. Preneel and P.C. van Oorschot, *On the security of iterated message authentication codes*, IEEE Transactions on Information Theory, Vol. 45, No. 1, January 1999, 188-199.
- T. Recio, H. Sterk and M. Pilar Vélez, *Automatic geometry theorem proving*, In: A.M. Cohen, F.G.M.T. Cuypers and H.J.M. Sterk (Eds.), Some tapas of computer algebra, Springer Verlag, 276-296.

- R. Rizzi, *Indecomposable r-graphs and some other counterexamples*, Journal of Graph Theory, 32, 1-15.
- P.L.A. Roelse, *Factoring high-degree polynomials over F_2 with Niederreiter's algorithm on the IBM SP2*, Math. Comp. 68, no. 226, 1999, 869-880.
- P.L.A. Roelse, *Cryptanalysis of the Wu-Dawson public key cryptosystem*, Finite Fields Appl. 5, no. 4, 386-392.
- K.A. Schouhamer Immink, *The future of digital audio recording*, Journal AES, vol. 47, March 1999, 171-172.
- K.A. Schouhamer Immink and A.J.E.M. Janssen, *Error propagation effects of enumerative coding schemes*, IEEE Transactions on Information Theory, vol. 45, no. 7, Nov. 1999, 2591-2594.
- K.A. Schouhamer Immink and G. Khachatrian, *Construction of simple runlength-limited codes*, Electronics Letters, vol. 35, no 2, 1999, p. 140.
- A. Schrijver, *Bipartite edge-colouring in $O(\Delta m)$ time*, SIAM Journal on Computing, 28, 841-846.
- A. Schrijver, P. Seymour and P. Winkler, *The ring loading problem*, SIAM Review, 41, 777-791.
- G. Sierksma, *Limiting polytopes and periodic Markov chains*, In: Linear and Multilinear Algebra, 46, 1999, 281-298.
- G. Sierksma, *E.S. van der Poort, M. Libura and J.A.A. van der Veen*, *Solving the k-best traveling salesman problem*, In: Computers & OR, 1999, 26, 409-425.
- *G. Sierksma and W. Sierksma*, *The great leap to infinitely small. Johann Bernouilli: mathematician and philosopher*, In: Annals of Science, 1999, 56, 433-449.
- J. Simonis and E.M. Gabidulin, *Perfect codes for metrics generated by primitive 2-error-correcting binary BCH codes (Soversennye kody dla metrik, porozdaemyh primitivnymi dvoicnymi BCH-kodami, ispravlausimi dvojnye osibki)*, in: Problemy peredachi informatsii, vol. 35, 3, 1999, 40-47.
- J. Slomp and N. Suresh, *Formation of teams in a multi-shift situation*, In: J. Ashayeri, W.G. Sullivan and M.M. Ahmad (eds.), Flexible Automation and Intelligent Manufacturing, Begell House Inc., 1999, 525-538.
- P. Soriano, C. Wynants, R. Séguin, M. Labbé, M. Gendreau and B. Fortz, *Design and dimensioning of survivable SDH networks*, Telecommunications network planning, B. Sanso and P. Soriano (eds.), Kluwer Academic Press, 147-167.
- B. Steinbach and H. Van Maldeghem, *Generalized quadrangles weakly embedded of degree > 2 in projective space*, Forum Math. 11, 1999, 139-176.
- L. Storme, *On the largest caps contained in the Klein quadric of $PG(5, q)$, q odd*, J. Combin. Theory, Ser. A, 87, 1999, 357-378.
- L. Storme, A. De Vos and G. Jacobs, *Group theoretical aspects of reversible logic gates*, J. Univ. Computer Science, 5, 1999, 307-321.
- N. Suresh, J. Slomp and S. Kaparthi, *Sequence-dependent clustering of parts and machines: a fuzzy ART neural network approach*, In: International Journal of Production Research, 1999, 37, No. 12, 2793-2816.
- R. Teunter and L. Fortuin, *End-of-Life Service*, International Journal of Production Economics, 1999, 59, 487-497.

- J.A. Thas, *Generalized quadrangles of order (s, s^2): Recent results*, Discrete Math. 208/209, 1999, 577-587.

- J.A. Thas, *Generalized quadrangles of order (s, s^2),III*, J. Combin. Theory (A) 87, 1999, 247-272.

- J.A. Thas and H. Van Maldeghem, *Lax embeddings of polar spaces in finite projective spaces*, Forum Math. 11, 1999, 349-367.

- J.A. Thas and H. Van Maldeghem, *On embeddings of the flag geometries of projective planes in finite projective spaces*, Des. Codes Cryptogr. 17, 1999, 97-104.

- M. Vandenwauver, R. Maier, J. Claessens and C. Vaduva, *Mobile code: friend or enemy?* PriceWaterhouseCoopers Cryptographic Centre of Excellence, Quarterly Journal, Issue 3, 1999, 13-16.

- M. Vandenwauver, P. Ashley and G. Gaskell, *The intranet authorization paradigm*, Information Security Management & Small Systems Security, Kluwer Academic Publishers, J.P. Eloff, L. Labuschagne, R. von Solms and J. Verschuren (eds.), 1999, 145-160.

- V. Venugopal, *Soft-computing-based approaches to group technology problem: a state-of-the-art review*, In: International Journal of Production Research, 1999, 37, No. 14, 3335-3357.

- A.J. Han Vinck, *Power line communication*, Encyclopedia of Electrical and Electronics Engineering, Wiley, New York, John Webster (ed.), 1999, 706-716.

- A.J. Han Vinck and Fangwei Fu, *On the capacity of generalized write-once memory with state transitions described by an arbitrary directed acyclic graph*, IEEE Transactions on Information Theory, Vol. 45, no.1, January 1999, 308-312.

- A.J. Han Vinck and Ch. Haslach, *A decoding algorithm with restrictions for array codes*, IEEE Transactions on Information Theory, November 1999, 2339-2345.

- S. van Vlijmen, S. Klusener and A. Schrijver, *The compact dynamic bus station*, Electronic Notes in Theoretical Computer Science, 21, 7, Elsevier, Amsterdam, 1999.

- W.M.C. van Wezel and R.J.J.M. Jorna, *The SEC-system: reuse support for scheduling system development*, In: Decision Support Systems, 26, nr. 1, 1999, 67-87.

- A.J. van Zanten, *Binomial systems and the ranking problem of certain combinatorial objects in lexicographic order and in gray order* (russian text), in: Diskretn'j analiz i issledovanie operacij, vol. 6, 1, 1999, 12-18.

- A.J. van Zanten, *The golden ratio in the arts of painting, building and mathematics*, in: Nieuw archief voor wiskunde (serie 4), vol. 17, 2, 1999, ISSN: 0028-9825, 229-245.

- A.J. van Zanten, *Rekenend denken*, inaugural speech, Maastricht, 1999, p. 26.

- A.J. van Zanten and A. Lukito, *Construction of certain cyclic distance-preserving codes having linear-algebraic characteristics*, in: Designs, codes and cryptography, vol. 16, 1999, 185-199.

4.3 Conference Proceedings

- K. Aardal, R.E. Bixby, C.A.J. Hurkens, A.K. Lenstra and J.W. Smeltink, *Market split and basis reduction: Towards a solution of the Cornuéjols-Dawande instances*, In: Integer Programming and Combinatorial Optimization, 7th International IPCO Conference, Berlin: Springer, 1999, 1-16.

- Y. Abramovich, N. Spencer and A.Gorokhov, *Identifiability and manifold ambiguity in DOA estimation for nonuniform linear antenna arrays*, Proc. ICASSP'99, Phoenix, AZ, March 1999.

- J.J.D. Aerts, J.H.M. Korst and W.F.J. Verhaegh, *Load balancing for redundant storage strategies: Retrieval problems*, proceedings Philips Workshop on Scheduling and Resource Management (SCHARM), Eindhoven, The Netherlands, December 1999, 51-58.

- P. Ashley, B. Broom and M. Vandenwauver, *An implementation of a secure version of NFS including RBAC*, Fourth Australian Conference on Information Security and Privacy (ACISP99), LNCS 1587, Springer-Verlag, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), 1999, 213-227.

- P. Ashley, A. Clark, G. Gaskell and M. Vandenwauver, *Experiences auditing IT security systems*, Proceedings of Open Source – AUUG'99, D. Purdue (ed.), AUUG Inc., 1999, 195-201.

- P. Ashley and M. Vandenwauver, *Using SESAME to implement role based access control in Unix file systems*, Proceedings of the Eighth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'99) / 4th International Workshop on Enterprise Security, 1999, 141-146.

- P. Ashley, M. Vandenwauver and J. Claessens, *Using SESAME to secure web based applications on an intranet*, Secure Information Networks, Proceedings of the IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99), 1999, 303-317.

- V.B. Balakirsky, *Characterization of the secrecy of a common key constructed via data transmission over the two-way AND channel*, Proc. 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, May 1999, (ed. A. Barb, E. van der Meulen, P. Vanroose), ISBN 90-71048-14-4; Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, Netherlands, 1999, 87-94.

- V.B. Balakirsky, *Addition of integers in a computer memory: information theory approach*, Proc. 22nd Symposium on Information Theory and Its Applications (SITA99), Vol 1, Yuzawa, Niigata, Japan, 30 November-3 December 1999, 415-418.

- V.B. Balakirsky, *Possibilities of increasing the speed of computations via a "component-wise" computer arithmetic*, Proc. 26th Intern. Conf. and Scientific Discussion Club, Ukraine, March 1999, 58-59.

- V.B. Balakirsky and F.M.J. Willems, *Nonasymptotic lower bound on the maximal cumulative redundancy of universal coding*, Proc. 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, May 1999, ISBN 90-71048-14-4, (ed. A. Barb, E. van der Meulen, P. Vanroose); Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, Netherlands, 1999, 17-24.

- M.S. Bargh and J.P.M. Schalkwijk, *On error correction in information feedback schemes*, Proc. 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, 27-28 May 1999, ISBN 90-71048-14-4, (ed. A. Barb, E. van der Meulen, P. Vanroose); Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, Netherlands, 1999, 173-180.

- J. Bloom, I.J. Cox, A.A.C. Kalker, J.P.M.G. Linnartz, M. Miller and B. Traw, *Copy Protection for DVD*, Proceedings of the IEEE, Special issue on Identification and Protection of Multimedia Information, July 1999, Vol. 87, No. 7, 1267-1276.

- J. Borst, B. Preneel and J. Vandewalle, *Linear cryptanalysis of RC5 and RC6*, Fast Software Encryption, LNCS 1636, L.R. Knudsen, (Ed.), Springer-Verlag, 16-30.

- H.J. Broersma, U. Faigle, C. Hoede and J.L. Hurink (eds.), Proc. 6th Twente Workshop on graphs and combinatorial optimization, Amsterdam: Electronic Notes in Discrete Mathematics, vol.3, Elsevier Science, p. 272.

- A.E. Brouwer, G.R. Pellikaan and E.R. Verheul, *Doing more with fewer bits*, In: K.Y. Lam, E. Okamoto, C-P Xing (Eds.), Advances in Cryptology Asiacrypt '99, LNCS, Springer Verlag, Berlin, 1716, 321-332.

- V. Buchoux, E. Moulines, O. Cappe and A.Gorokhov, *Semi blind subspace techniques for digital communications systems*, Proc. Signal Processing Advances in Wireless Communications, Annapolis, MD, May 1999.
- F. Buekenhout, *The O'Nan-Scott theorem*, Seminar Bingen-Cara-Van Maldeghem on Permutation Groups, Vrije Universiteit Brussel, 1999, p. 27.
- F. Buekenhout, *Le programme d'Erlangen de Félix Klein (1872), La relation entre les géométries et les groupes*, Séminaire CREM-GEPEMA-UREM, 1999, p. 49.
- J. Claessens, B. Preneel and J. Vandewalle, *Solutions for anonymous communication on the internet*, Proceedings of the IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology (ICCST'99), 1999, 298-303.
- J. Claessens, B. Preneel and J. Vandewalle, *Enabling a lightweight software agent framework for secure agent-based electronic commerce applications*, Proceedings of the Workshop on Agents in Electronic Commerce (WAEC'99), First Asia-Pacific Conference on Intelligent Agent Technology (IAT'99), 1999, 151-158.
- J. Claessens, B. Preneel and J. Vandewalle, *Anonymity controlled electronic payment systems*, 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, May 27-28, 1999, 109-116.
- A.M. Cohen and O. Caprotti, *Integrating computational and proof systems using OpenMath*, In: Y. Bertot, G. Dowek, A. Hirschowitz, C. Paulin, and L. Théry (Eds.), Theorem Proving in High Order Logics, Proceedings of the 12th International conference, TPHOLs'99. LNCS, 1690, Springer.
- A.M. Cohen and R. de Man, *Some indications that the exceptional groups form a series*, In Computational Methods for Representations of groups and algebras, P. Dräxler, G.O. Michler and C.M. Ringel (eds.), Proceedings Euroconference, Birkhäuser, Basel, vol. 173, 121-138.
- A. Cossidente and L. Storme, *Cyclic and elementary abelian caps in projective spaces*, Proceedings of Combinatorics '96, Assisi, Italy, September 9-15, 1996, Discrete Math., 208/209, 1999, 139-156.
- J. Daemen and V. Rijmen, *Resistance against implementation attacks: a comparative study of the AES proposals*, Proceedings of the 2nd AES Candidate Conference, 1999, 122-132.
- J. Daemen and V. Rijmen, *Efficient block ciphers for Smartcards*, USENIX Workshop on Smartcard technology '99, Conference proceedings, 29-35.
- C. Feremans, M. Labbé and G. Laporte, *The generalized minimum spanning tree: Polyhedra and Branch-and-Cut*, Proceedings of the 6th Twente Workshop on graphs and combinatorial optimization, Enschede, the Netherlands, May 1999, 48-53.
- P. Flocchini, F. Geurts and N. Santoro, *Optimal irreversible dynamos in chordal rings*, Proceedings of WG 99, 25th International Workshop on Graph-Theoretic Concepts in Computer Science, Ascona, Switzerland, June 1999, LNCS 1665, Springer Verlag, 202-214.
- B. Goldengorin, G.A. Tijssen and M. Tso, *A Non-Greedy algorithm for supermodular function minimization with applications*, In: Proceedings of International Conference on Industrial Logistics, ICIL'99, University of Southampton, United Kingdom, 1999, 318-325.
- A. Gorokhov, *On the performance of the Viterbi decoder with trained and semi-blind channel estimators*, Proc. ICASSP'99, Phoenix, AZ, March 1999.
- Gorokhov, *Blind equalization and channel coding in SIMO multicarrier systems*, Proc. Signal Processing Advances in Wireless Communications, Annapolis, MD, May 1999.
- K.A.S. Immink, *A survey of high-rate codes*, Proc. Asian Symposium on Information Storage Technology, January 1999, Singapore, 133-139.

- C.J.A. Jansen, H.C.A. van Tilborg and S.-B. Xu, *A New authentication protocol for portable communication systems*, Proceedings of CMS'99 - IFIP Conference on Communications & Multimedia Security, Leuven, Belgium, September 1999, 216-230.

- R.J.J.M. Jorna and B.P. van Heusden, *Cognitive dynamics: a framework to handle types of knowledge*, In: J. Schreinemakers (ed.), Knowledge Management: the 7th ISMICK Conference, Rotterdam: EUR, 1999, 128-145.

- M.H. Klompstra, W.F.J. Verhaegh, R.J. Bril and E.F.M. Steffens, *QoS resource management challenges for consumer devices*, proceedings Philips Workshop on Scheduling and Resource Management (SCHARM), Eindhoven, The Netherlands, December 1999, 93-99.

- L.R. Knudsen and B. Preneel, *Error correcting codes and collision-resistant hashing*, Proc. 1999 IEEE Information Theory and Communications Workshop, 55-57.

- L.R. Knudsen and V. Rijmen, *Weaknesses in LOKI97*, Proceedings of the 2nd AES Candidate Conference, Rome, March 22-23, 1999, 168-174.

- A.G.C. Koppelaar and M. van Dijk, *Symbol by symbol APP decoding with a generalized Viterbi decoder*, Proc. of the ITW'99, Kruger National Park, South Africa, June 20-25, p. 95.

- J.P.M.G. Linnartz, *Partial correlations and cyclic prefixes in Direct Sequence Spread Spectrum*, IEEE Veh. Tech. Conf, Fall 1999, Amsterdam, September 19-23, 1999.

- J.P.M.G. Linnartz, A.A.C. Kalker and J. Haitsma, *Detecting electronic watermarks in digital video?*, Paper 3010, Invited paper for special session at ICCASP ?99, Phoenix, AR, March 1999.

- J.P.M.G. Linnartz, A.A.C. Kalker and G. Depovere, *On the design of a watermarking system: considerations and rationales*, Information Hiding Workshop, Dresden, September 1999. Preliminary Proc. and Springer Verlag, LNCS 1768, 254-269.

- J.P.M.G. Linnartz and J.C. Talstra, *MPEG PTY-Marks: cheap detection of embedded copyright data in DVD-video*, Computer Security - ESORICS 98, Proceedings 5th European Symposium on Research in Computer Security, Louvain-la-Neuve, Belgium, 16-18 Sept. 1998. Edited by J.J. Quisquater et al., 1998, 221-40.

- B. Lukito *An upper bound for snake-in-the-box codes*, in: Proceedings, Algebraic and combinatorial coding theory: 6th International Workshop Pskov, September 1998, 183-186.

- P. Magniez and A. Gorokhov, *Space-time equalization for DVB-T in single frequency networks*, Proc. Asilomar'99 Conference, Pacific Grove, CA, October 1999.

- K.M. Martin, J. Pieprzyk, R. Safavi-Naini and H. Wang, *Changing thresholds in the absence of secure channels*, Information Security and Privacy, 4th Australasian Conference, ACISP99, LNCS 1587, J. Pieprzyk, R. Safavi-Naini and J. Seberry (eds), 1999, 177-191.

- J. Nakahara Jr., J. Vandewalle and B. Preneel, *Diffusion analysis of Feistel networks*, 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, May 27-28, 1999, 101-108.

- S. Nikova and V. Nikov, *Some applications of bounds for designs to the cryptography*, Proc. Seventh IMA Conference on Cryptography & Coding, LNCS 1746, Springer-Verlag, 25-34.

- Van Rompay, B. Preneel and J. Vandewalle, *the digital timestamping problem*, 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, May 27-28, 1999, 71-78.

- L.A.M. Schoenmakers, *A simple publicly verifiable secret sharing scheme and its application to electronic voting*, In – (Ed.), Advances in Cryptology – CRYPTO'99, Springer-Verlag, Berlin, 148-164.

- K.A. Schouhamer Immink, *A survey of high-rate codes*, Proc. Asian Symposium on Information Storage Technology, Singapore, Jan. 25-26, 1999, 133-139.
- H.C.A. van Tilborg and S.B. Xu, *A construction of systematic authentication codes based on error-correcting codes*, Proceedings of the 1999 Workshop on Coding and Cryptography (ed. D. Augot and C. Corlet), IRRIA, Paris, 1999, 279-289.
- Tj.J. Tjalkens and F.M.J. Willems, *Variable-to-fixed length source codes: a geometrical approach to low complexity codes*, proceedings 1999 IEEE International Symposium on Information Theory, Metsovo, Greece, June 27 - July 1, 1999, (ed. the IEEE Information Theory Society), 33-33.
- Ludo Tolhuizen, *The binary multiplying channel without feedback: new rate pairs in the zero-error capacity region*, Proc. 20th Symp. on Information Theory in the Benlux, Haasrode, Belgium, May 27 and 28, 1999, 215-217.
- M. Vandenwauver and P. Ashley, *The importance of security in modern communication networks*, Proceedings World Multiconference on Systemics, Cybernetics and Informatics, Volume 4, Communication Systems, Internet and Mobile/Wireless Computing, M. Torres, B. Sanchez, S. Radhakrishnan and R. Osers (eds.), 1999, 443-450.
- M. Vandenwauver, J. Claessens, W. Moreau, C. Vaduva and R. Maier, *Why enterprises need more than firewalls and intrusion detection systems*, Proceedings of the Eighth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'99) / 4th International Workshop on Enterprise Security, 1999, 152-157.
- W.F.J. Verhaegh, *Capacity scheduling for data services over digital networks*, proceedings Philips Workshop on Scheduling and Resource Management (SCHARM), Eindhoven, The Netherllands, December 1999, 147-156
- A.J. Han Vinck, *Coding for random access communications*, WIC Benelux, May 28-29, 1999, Leuven, Belgium, ISBN 90-71048-14-4, p. 227.
- A.J. Han Vinck and J. Häring, *Coding and modulation for power line communications*, 1999 International Symposium on Power-Line Communications and its Applications, Lancaster University, March 1999, ISBN 90-74249-22-1, 102-106.
- A.J. Han Vinck and Bahram Honary, *Proceedings 3rd International Symposium on Power-Line Communications and its Applications,* University of Lancaster, March 1999, ISBN 90-74249-22-1, p. 175.
- A.J. Han Vinck, J. Häring and T. Wadayama, *Proceedings of SITA 99*, Yuzawa, Niigata, Japan, 1999, 661-664.
- A.J. Han Vinck and T. Wadayama, *DC-free binary convolutional codes*, Proceedings of SITA 99, Yuzawa, Niigata, Japan, 1999, 809-812.
- P.A.J. Volf, F.M.J. Willems and Tj.J. Tjalkens, *Complexity reducing techniques for the CTW algorithm*, Proc. 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, May 27-28, 1999, ISBN 90-71048-14-4, (ed. A.Barb, E. van der Meulen, P. Vanroose); Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, Netherlands, 1999, 25-32.
- H.L.T. Wanders, G.J.C. Gaalman, R.J.J. Jorna and G. Sierksma, *Integrating cognitive science and operations research techniques for building a better planning support system for a solid board factory*, In: HCP'99, Human Centered Processes, 10th Mini Euro Conference, Brest, France, September 22-24, 1999, 99-107.

4.4 Preprints and Internal Reports

- K. Aardal, C.A.J. Hurkens, J.K. Lenstra and S.R. Tiourine, *Algorithms for the radio link frequency assignment problem*, Memorandum COSOR (Int. r. no. 99-17). Capaciteitsgroep Wiskunde, 1999, p. 19.

- K. Aardal, J.K. Lenstra, F. Maffioli and D.B. Shmoys, *Selected papers of Eugene L. Lawler*, CWI Tract (Ext. r. no. 126). Amsterdam: CWI, 1999.

- P. Abramenko and H. Van Maldeghem, *On opposition in spherical buildings and twin buildings*, to appear in Annals of Combinatorics.

- P. Abramenko and H. Van Maldeghem, 1-*twinnings of buildings*, to appear in Math. Z.

- G. Ausiello, E. Feuerstein, S. Leonardi, L. Stougie and M. Talamo, *Algorithms for the on-line travelling salesman problem*, COSOR Memorandum 99-09, TU Eindhoven, p. 33, Accepted for Algoritmica.

- J. Barát and L. Storme, *Multiple blocking sets in* $PG(n,q)$*, q square,* $n \geq 3$, Des. Codes Cryptogr., submitted.

- S.G. Barwick, Christine M. O'Keefe and L. Storme, *Unitals which meet Baer subplanes in 1 modulo q points*, J. Geom., to appear.

- Y. Bartal, S. Leonardi, A. Marchetti Spaccamela, J. Sgall and L. Stougie, *Multiprocessor scheduling with rejection*, COSOR Memorandum 99-06, TU Eindhoven, p. 18, accepted for SIAM Journal on Discrete Mathematics.

- L. Batten, M. Davidson and L. Storme, *An analysis of Chen's construction of distance five codes*, IEEE Trans. Inform. Theory, to appear.

- D. Bauer, H.J. Broersma, A. Morgana and E. Schmeichel, *Polynomial algorithms that prove an NP-hard hypothesis implies an NP-hard conclusion*, Memorandum Faculteit TW no. 1499, Enschede: Universiteit Twente, ISBN 0169-2690, p. 15.

- P. Beelen and G.R. Pellikaan, *The Newton-polygon of plane curves with many rational points*, to appear in Designs, Codes and Cryptography.

- J.M. Bilbao, A. Jimenez-Losada, E. Lebron and T.S.H. Driessen, *The Shapley value for games on matroids: the static model*, External report, Working Paper, Sevilla, Spain: Universidad de Sevilla, p. 16.

- M. Blom, S.O. Krumke, W.E. de Paepe and L. Stougie, *The on-line TSP against fair adversaries (extended abstract)*, COSOR-Memorandum 99-24, TU Eindhoven, accepted for presentation at CIAC 2000, Rome, Italy.

- J. Bokowski Ph. Cara and S. Mock, *On a self dual 3-sphere of Peter McMullen*, preprint. p. 14.

- J. van Bon and A.M. Cohen, *Affine distance-transitive graphs and exceptional Chevally groups*, submitted to Proc. LMS.

- D. Bonheure, F. Buekenhout, D. Leemans, *On the Petrials of thin rank three geometries*, Jour. Geom., to appear, p. 8.

- F. Boudot, B. Schoenmakers and J. Traoré, *A fair and efficient solution to the socialist millionaires' problem*, to appear in Discrete Applied Mathematics.

- A.L.A. Broersma, G. Sierksma and J. Wijngaard, *Decomposed versus integrated control of a one-stage production system*, OM Research Report, 99A18, University of Groningen, 1999.

- H.J. Broersma, *On some intriguing problems in Hamiltonian graph theory – A survey*, Memorandum Faculteit TW no 1508, Enschede: Universiteit Twente, ISBN 0169-2690, p. 26.

- H.J. Broersma, N. Bruin, J.L. Hurink, L.E. Meester, S.S. op de Beek and J.H. Westhuis, *Throughput of ADSL modems*, Memorandum Faculteit TW no 1482, Enschede: Universiteit Twente, ISBN 0169-2690, p. 18.
- H.J. Broersma, R.J. Faudree, A. Huck, H. Trommel and H.J. Veldman, *Forbidden subgraphs that imply Hamiltonian-connectedness*, Memorandum Faculteit TW, no. 1481, Enschede: Universiteit Twente, ISBN 0169-2690, p. 20.
- H.J. Broersma, M. Kriesell and Z. Ryjácek, *On factors of 4-connected claw-free graphs*, Memorandum Faculteit TW no. 1491, Enschede: Universiteit Twente, ISBN 0169-2690, p.13.
- H.J. Broersma and Liming Xiong, *On minimum degree conditions for supereulerian graphs*, Memorandum Faculteit TW no 1507, Enschede: Universiteit Twente,, ISBN 0169-2690., p. 10.
- L. Brotcorne, M. Labbé, P. Marcotte and G. Savard, *A bilevel model and solution algorithm for a freight tariff setting problem.*
- L. Brouns, J. A. Thas and H. Van Maldeghem, *m-Clouds in generalized hexagons*, to appear in Discrete Math.
- A.E. Brouwer, F.G.M.T. Cuypers and E.W. Lambeck, *The hyperplanes of the M_{24}-near polygon*, Discrete Algebra en Meetkunde, to appear.
- B. De Bruyn, *On near polygons and the Coxeter-cap in PG(5,3)*, to be published in Journal of Geometry.
- A. de Bruin, G. Kindervater, T. Vredeveld and A. Wagelmans, *Finding a feasible solution for a simple LP problem using agents*, Tinbergen Discussion paper (Int. r. no. 99-037/4), Capaciteitsgroep Wiskunde, 1999, p. 8.
- B. De Bruyn, *On near hexagons and spreads of generalized quadrangles*, to be published in Journal of Algebraic Combinatorics.
- B. De Bruyn, *On the number of nonisomorphic glued near hexagons*, to be published in Bulletin of the Belgian Mathematical Society Simon Stevin.
- B. De Bruyn, *Association schemes from regular near hexagons*, submitted to Journal of Algebraic Combinatorics.
- B. De Bruyn, *Glued near polygons*, submitted to European Journal of Combinatorics.
- B. De Bruyn, *Near hexagons with four points on a line*, preprint.
- F. Buekenhout, *Incidence geometry and finite groups*, Internal Report, 1999, p. 12.
- F. Buekenhout, *Géomtrie d'incidence et groupes finis*, Internal Report, 1999, p. 13.
- F. Buekenhout, *Veelvlakken: beginselen van regulariteit en semi-regulariteit*, Internal Report, 1999, p. 20.
- F. Buekenhout, *La spirale de la similitude*, Internal Report, 1999, p. 22.
- F. Buekenhout, D. Bonheure and D. Leemans, *On the Petrials of thin rank 3 geometries*, Journ. Geom, to appear.
- F. Buekenhout, Ph. Cara and K. Vanmeerbeek, *Geometries of the group $PSL(2,11)$*, Geom. Dedic., to appear.
- A. Buldas, H. Lipmaa and B. Schoenmakers, *Optimally efficient accountable time-stamping*, to appear.
- D. de Caen and E.R. van Dam, *Fissioned triangular schemes via the cross-ratio*, preprint.

- O. Caprotti and A.M. Cohen, *Integrating computational and deduction systems using OpenMath*, submitted to JSC, 1999.
- Ph. Cara, *An infinite family of Petersen geometries with nonlinear diagram*, Journ. Geom., to appear.
- Ph. Cara, *On the number of planes in Neumaier's A8- geometry*, Jour. Comb. Th. (A), to appear.
- Ph. Cara, *Graph theory for geometers*, Internal Report.
- Ph. Cara and D. Leemans, *the residually weakly primitive geometries of S5x2*, preprint. p. 24.
- Ph. Cara, S. Lehman and D.V. Pasechnik, *On the number of inductively minimal geometries*, Theoretical Computer Science, to appear.
- G. Celeux, S. Chrétien, F. Forbes and A. Mkhadri, *A component-wise EM algorithm for mixtures*, preprint.
- C. Cerf and A. Jorissen, *Is amino acid homochirality due to asymmetric photolysis in space?*, Space Science Reviews, to appear.
- C. Cerf and A. Stasiak, *A topological invariant to predict the 3-D writhe of ideal configurations of knots and links*, Proceedings of the National Academy of Sciences of the USA, Section on Applied Mathematics, to appear.
- F. De Clerck and M. Delanote, *Partial geometries and the triality quadric*, accepted for J. Geometry.
- F. De Clerck and M. Delanote, *Two-weight codes, partial geometries and Steiner systems*, accepted for Designs, Codes and Cryptography.
- F. De Clerck, M. Delanote, N. Hamilton and R. Mathon, *Perp-systems and partial geometries*, preprint.
- F. De Clerck, N. Hamilton, C. M. O'Keefe and T. Penttila, *Quasi-quadrics and related structures*, accepted for Australasian Journal of Combinatorics.
- A.M. Cohen and A.A. Ivanov, *Affine distance-transitive groups of dimension 1*, European Journal of Combinatorics, to appear.
- A.M. Cohen, A. Steinbach, R. Ushirobira and D. Wales, *Lie algebras generated by extremal elements*, submitted to J. Algebra.
- K. Coolsaet and H. Van Maldeghem, *Some new upper bounds for the size of partial ovoids in slim generalized polygons and generalized hexagons of order* (s, s^3), to appear in J. Alg. Comb.
- M. Coppens and C. De Volder, *Blowings-up of varieties and injectivity of Gauss maps*, to appear in Archiv der Matematik.
- P. Cowling and W. Rezig, *Integration of continuous caster and hot strip mill planning for steel production*, preprint.
- E.R. van Dam, *A characterization of association schemes from affine spaces*, Designs, Codes and Cryptography, to appear.
- E.R. van Dam and D. Fon-Der-Flaass, *Uniformly packed codes and more distance regular graphs from crooked functions*, J. Alg. Combinatorics, to appear.
- M. Dehon and D. Leemans, *Constructing coset geometries with MAGMA: an application to the sporadic groups M12 and J1*, preprint. p. 24.

- A. Delandtsheer, *Finite flag-transitive linear spaces with alternating socle*, preprint for the Proceedings of the Euroconference on Algebraic Combinatorics and Applications, to appear in Springer Lecture Notes.
- M. Delanote, *A new semipartial geometry*, accepted for J. Geometry.
- A. Devillers, *d-homogeneous and d-ultrahomogeneous linear spaces*, Journal of Combinatorial Designs, to appear.
- A. Devillers, *Ultrahomogeneous semilinear spaces*, preprint.
- A. Devillers, *Homogeneous semilinear spaces*, preprint.
- J.-P. Doignon, J.-Cl. Falmagne and M. Regenwetter, *Combinatoric and geometric aspects of some probabilistic choice models—A review*, in: Beliefs, Interactions and Preferences in Decision Making, eds. M. Machina and B. Munier, Kluwer Academic Publishers, to appear.
- J.-P. Doignon and J. Mitas, *Dimension of valued relations*, European Journal of Operational Research, to appear.
- T.S.H. Driessen and D. Paulusma, *Two extensions of the Shapley value for cooperative games*, Memorandum Faculteit TW no. 1494, Enschede: Universiteit Twente, ISBN 0169-2690, p. 16.
- S. Dye, L. Stougie and A. Tomasgard, *Single node service provision problem with fixed charges*, COSOR-Memorandum 99-04, TU Eindhoven, submitted to Discrete Applied Mathematics., p. 29.
- S. Dye, L. Stougie and A. Tomasgard, *The stochastic single node service provision problem*, COSOR-Memorandum 99-13, TU Eindhoven, submitted to Operations Research, p. 24.
- J. Eisfeld, L. Storme, and P. Sziklai, *Minimal covers of the Klein quadric*, J. Combin. Theory, Ser. A, submitted.
- J. Eisfeld, L. Storme and P. Sziklai, *Minimal $(n-1)$-covers and partial $(n-1)$-spreads of the hyperbolic quadric $Q^+(2n+1,q)$*, J. Algebraic Combin., submitted.
- J. Eisfeld, L. Storme, T. Szőnyi and P. Sziklai, *Covers and blocking sets of classical generalized quadrangles*, Proceedings of the The Third International Shanghai Conference on Designs, Codes and Finite Geometries, Shanghai, China, May 14-18, 1999, Discr. Math., to appear.
- S. Ferret and L. Storme, *Minihypers and linear codes meeting the Griesmer bound: Improvements to results of Hamada, Helleseth and Maekawa*, Des. Codes Cryptogr., submitted.
- E. Feuerstein, M. Mydlarz and L. Stougie, *On-line multi-threaded scheduling*, COSOR-Memorandum 99-21, TU Eindhoven, submitted to Theoretical Computer Science., p. 19.
- S. Fiorini, *Determining the automorphism group of the linear ordering polytope*, Discrete Applied Mathematics, to appear.
- S. Fiorini and P.C. Fishburn, *Weak order polytopes*, submitted.
- P. Flocchini, F. Geurts, A. Mingarelli and N. Santoro, *Convergence and aperiodicity in fuzzy cellular automata: Revisiting rule 90*, preprint.
- P. Flocchini, F. Geurts and N. Santoro, *Optimal irreversible dynamos in chordal rings*, preprint.
- B. Fortz and M. Labbé, *Facets for the polyhedron of two-connected networks with bounded rings*, preprint.
- B. Fortz and M. Labbé, *Exact and heuristic algorithms for the design of survivable networks with bounded rings*, preprint.

- B. Fortz and M. Labbé, *Structural results for two-connected networks with rings of bounded cardinality*, preprint.
- B. Fortz and M. Thorup, *Internet traffic engineering by optimizing OSPF weights*, preprint.
- O. Geil and G.R. Pellikaan, *The structure of order domains*, preprint.
- B. Goldengorin, G.A. Tijssen and M. Tso, *The maximization of submodular functions: Old and new proofs for the correctness of the Dichotomy algorithms*, SOM Research Report, 99A17, University of Groningen, 1999.
- B. Goldengorin and M. de Vink, *Solving large instances of te quadratic cost partition problem on dense graphs by data-correcting algorithms: a computational study*, SOM Research Report, 99A50, University of Groningen, 1999.
- H. Gottschalk and D. Leemans, *Geometries for the group* $PSL(3,4)$, preprint, p. 22.
- E. Govaert and H. Van Maldeghem, *Two remarks on generalized hexagons*, to appear in J. Geom. (Proceedings 2nd Pythagorean Conference).
- E. Govaert and H. Van Maldeghem, *Some combinatorial and geometric characterizations of the finite dual classical generalized hexagons*, to appear in J. Geom.
- R. Gramlich and H. van Maldeghem, *Epimorphisms of generalized polygons, part 1: Geometrical characterizations*, to appear in Des. Codes Cryptogr.
- Ü. Gürler, M.Ç. Pinar and M. Mehdi Jelassi, *On closed-form solutions of a resource allocation problem in parallel funding of R&D project*, preprint.
- W.H. Haemers, Preprints *Bicliques and eigenvalues*, Research Memorandum FEW 783, Tilburg University.
- W.H. Haemers, F.C. Bussemaker and E. Spence, *The search for pseudo orthogonal Latin squares of order six*, Research Memorandum FEW 780, Tilburg University.
- P. Hansen and N. Mladenovich, *J-MEANS: A new local search heuristic for minimum sum-of-squares clustering*, preprint.
- R. Hill, I. Landjev, C. Jones, L. Storme and J. Barát, *On complete caps in the projective geometries over* F_3, Proceedings of the Second Pythagorean Conference, Samos, Greece, May 30-June 5, 1999, J. Geom., to appear.
- C. Huybrechts, *$c.AG^*$-geometries and dimensional dual hyperovals in projective spaces*, preprint.
- C. Huybrechts, *A unified construction for $c^*.c$ and $L.L^*$-geometries in affine spaces*, preprint.
- C. Huybrechts, *On the non-existence of empty conics*, preprint.
- D. Jungnickel and L. Storme, *Packing and covering groups with subgroups*, J. Algebra, submitted.
- E. Kuijken, *A geometric description of Hermitian two-graphs and its applications*, preprint.
- M. Labbé, G. Laporte, I. Rodriguez Martin and J.J. Salazar Gonzalez, *The median cycle problem.*
- M. Labbé, R. Séguin, P. Soriano and Ch. Wynants, *Network synthesis with non-simultaneous multicommodity flow requirements: bounds and heuristics.*
- D. Leemans, *The residually weakly primitive geometries of the dihedral groups*, Atti Sem. Mat. Fis. Univ. Modena, to appear, p. 11.
- D. Leemans, *The rank 3 geometries of the simple Suzuki groups Sz(q)*, Note di Mat. 19, 1999, to appear, p. 25.

- D. Leemans, *The RWPRI pre-geometries of the simple Suzuki groups*, Note Mat., to appear, p. 27.
- D. Leemans, *On a rank five geometry of Meixner for the Mathieu group M12*, Geo. Dedicata, to appear.
- D. Leemans, *Incidence Geometry*, chapter in the Magma Handbook, University of Sydney, Australia, to appear, p. 25.
- D. Leemans, C. Lefèvre-Percsy and N. Percsy, *New geometries for finite groups and polytopes*, Bull. Belg. Math. Soc. Simon Stevin, to appear. p. 34.
- J.P.M.G. Linnartz, *Partial correlations and cyclic prefixes in direct sequence spread spectrum*, IEEE Veh. Tech. Conf, Fall 1999, Amsterdam, September 19-23, 1999.
- J.P.M.G. Linnartz, A.A.C. Kalker and G. Depovere, On the design of a watermarking system: considerations and rationales, Information Hiding Workshop, Dresden, September 1999. Preliminary Proc. and Springer Verlag, LNCS 1768, 254-269.
- J.P.M.G. Linnartz, A.A.C. Kalker and J. Haitsma, *Detecting electronic watermarks in digital video*, Paper 3010, Invited paper for special session at ICCASP ?99, Phoenix, AR, March 1999.
- D. Luyckx, *Blocking (n-2)-dimensional subspaces on Q(2n,q)*, to appear in Eur. J. Combin.
- H. Van Maldeghem, *Sharply* 2*-transitive groups of projectivities in generalized polygons*, to appear in Discr. Math.
- H. Van Maldeghem, *Distance transitive generalized quadrangles of prime order*, to appear in Geom. Dedicata.
- H. Van Maldeghem, *An elementary construction of the split Cayley hexagon ßH*(2), to appear in Atti Sem. Mat. Fis. Univ. Modena.
- K. Metsch and L. Storme, *2-Blocking sets in $PG(n,q)$, $n \geq 3$, q square*, Contrib. Algebra and Geom., to appear.
- K. Metsch and L. Storme, *Partial linear complexes in $PG(3,q)$*, Proceedings of Combinatorics '98, Mondello, Italy, June 14-20, 1998, Discrete Math., submitted.
- N. Mladenovich and F. Plastria, *A note on continuous p-defense-sum problem*, preprint.
- T. Namekata and T.S.H. Driessen, *Reduced game property of the egalitarian non-k-averaged contribution value and the Shapley value*, External report, Working Paper, Otaru, Hokkaido, Japan: Otaru University of Commerce, 1999, p. 20.
- B.J. Oosterman, G.J.C. Gaalman and F.P.J. Kuypers, *Finding structures in product development*, SOM Research Report, 99A06, University of Groningen, 1999.
- P. Patricio and R. Puystjens, *About the Von Neumann regularity of triangular block matrices*, submitted to LAA, p. 18.
- M.Ç Pinar, *A global error bound for quadratic perturbation of linear programs*, preprint.
- M.Ç. Pinar and W.M. Hartmann, *Huber approximation for the nonlinear I_1 problem*, preprint.
- R. Puystjens and M.C. Gouveia, *Drazin invertibility for matrices over an arbitrary ring*, submitted LAA, p. 9.

  P. Sanders, S. Egner and J. Korst, *Fast concurrent access to parallel disks*, Max-Planck-Institut für Informatik, Saarbrueken, Germany, Report MPI-I-1999-1-003.
- M. Sebille, *There exists a simple non-trivial t-design with an arbitrarily large automorphism group for every t*, Designs, Codes and Cryptography, to appear.

- M. Sebille, *On a result of Cameron and Praeger on block-transitive point-imprimitive t-designs*, proceedings of ALCOMA 99, to appear.
- M. Sebille, *An extension theorem for t-designs*, preprint.
- A. Steinbach and H. Van Maldeghem, *Generalized quadrangles weakly embedded of degree 2 in projective space*, to appear in Pacific J. Math.
- L. Storme, J.A. Thas and S.K.J. Vereecke, *New upper bounds on caps in* $PG(n, q)$, J. Geom., submitted.
- L. Storme and S.K.J. Vereecke, *The geometric description of a cyclic arc in* $PG(q-\sqrt{q}-3, q)$, J. Statist. Planning Infer., to appear.
- L. Storme and Zs. Weiner, *Minimal blocking sets in* $PG(n, q)$*,* $n \geq 3$, Des. Codes Cryptogr., to appear.
- H. Sun, S. Zhang, X. Li and T.S.H Driessen, *A coalitional powervalue for set games*, External report, Working Paper, Xian, P.R. China: Northwestern Polytechnical University, p. 20.
- R. Teunter, *Reverse logistics: On finding optimal inventory strategies*, preprint 19/99, University of Magdeburg, Germany, 1999.
- R. Teunter, *Economic ordering quantities for stochastic discounted cost inventory systems with demanufacturing*, preprint 11/99, University of Magdeburg, Germany, 1999.
- R. Teunter and D. Vlachos, *An inventory system with periodic regular review and flexible emergency review*, preprint 11/2000, University of Magdeburg, Germany, 1999.
- J.A. Thas, *SPG systems and semipartial geometries*, preprint.
- J.A. Thas, *Flocks and partial flocks of quadrics: A survey*, J. Stat. Plan. Inf., to appear.
- J.A. Thas, *Geometrical constructions of flock generalized quadrangles*, J. Combin. Theory (A), preprint.
- J.A. Thas, *Characterizations of translation generalized quadrangles*, Designs, Codes and Cryptography, preprint.
- J.A. Thas, *A result on spreads of the generalized quadrangle* $T_2(O)$*, with* O *an oval arising from a flock, and applications*, European J. Combin., preprint.
- J.A. Thas and B. Cooperstein, *On generalized k-arcs in* $PG(2n, q)$, Annals of Combin., preprint.
- J. A. Thas and H. Van Maldeghem, *Classification of embeddings of the flag geometries of projective planes in finite projective spaces, Part I*, to appear in J. Combin. Theory Ser. A.
- J. A. Thas and H. Van Maldeghem, *Classification of embeddings of the flag geometries of projective planes in finite projective spaces, Part 2*, to appear in J. Combin. Theory Ser. A.
- J. A. Thas and H. Van Maldeghem, *Classification of embeddings of the flag geometries of projective planes in finite projective spaces, Part 3*, to appear in J. Combin. Theory Ser. A.
- J. A. Thas and H. Van Maldeghem, *Some remarks on embeddings of the flag geometries of projective planes in finite projective spaces*, to appear in J. Geom.
- J.A. Thas and H. Van Maldeghem, *Lax embeddings of generalized quadrangles in finite projective spaces*, Proc. London Math. Soc., to appear.
- J.A. Thas, L. Storme and S.K.J. Vereecke, *New upper bounds for the sizes of caps in finite projective spaces*, J. of Geometry, preprint.
- Tran van Trung, *Recursive constructions for 3-designs and resolvable designs*, J. Stat. Plan. Infer., in press.

- Tran van Trung, *Constructions for 3-designs using parallelism*, J. Geom., in press.
- Tran van Trung and V. Canda, *A new mode of using of all-or-nothing transforms*, preprint.
- Tran van Trung, S.S. Magliveras and D.R. Stinson, *One-way functions and trap-doors in finite permutation groups*, preprint.
- Tran van Trung and R. Mathon, *Directed t-packings and directed t-Steiner systems*, Designs, Codes and Cryptography, to appear.
- Tran van Trung, D.R. Stinson and R. Wei, *Secure frameproof codes, key distribution patterns, group testing algorithms and related structures*, J. Stat. Plan. Infer., to appear.
- A.J. Han Vinck, *Channel models*, Final Report Concerted Action in Telecommunication Research, Contract No: INCO 950944 - African Telecom, September 1999.
- C. De Volder, *General Blowings-up of P^2 and Injectivity of Gauss Maps*, submitted to Geometriae Dedicata.
- D. De Wolf and Y. Smeers, *The gas transmission problem solved by an extension of the Simplex algorithm*, preprint.
- Ch. Wynants, M. Gendreau, M. Labbé and R. Séguin, *Optimizing reserve capacities of partially equipped SDH networks*, preprint.
- H. Yaman, O. Ekin KaraŞand and M.Ç. Pinar, *Minimum spanning tree problem with interval data*.

4.5 Patents

- K.A.S. Immink, *Record carrier containing a signal having a sequence of successive information signal portions*, USPatent 5,920,272, July 1999.
- D. Chaum, N. Ferguson, B. Schoenmakers and E. Voskuil, *Partitioned information storage systems with controlled retrieval*, U.S. patent # 5,956,400, September 21, 1999.
- KPN Research:
  - Sharon Prins, Gert Roelofsen en Frank Muller: patent (title still secret).
  - Frank Muller: 4 patents on smart card systems.
- Philips Research Laboratories:
  - C.P.M.J. Baggen and L.M.G.M. Tolhuizen, *Error correctable data transmission method and device based on semi-cyclic codes*, US Patent 5,872,798, February 16, 1999.
  - Marten van Dijk:
    Patent publication numbers: EP938790A2 and EP965175A2. More information available via http://www.delphion.com/
  - Jan Korst and Verus Pronk, *Method and system for reading data for a number of users*, US Patent 5,950,015, granted September 7, 1999.
  - Jean-Paul Linnartz:
    Patent publication numbers: WO9948290, EP0941605, WO9945706, EP0940037, EP0935872, EP0934656, US5933798, EP0920775, EP0906700, EP0902946, WO0012347, WO9912331, WO9911064, and EP0891674. More information available via http://www.delphion.com/
  - Joop Talstra:
    Patent applications: WO0064157, WO0045381, WO0014967, WO9965240, WO9948290, EP1046296 and EP0983687. More information available via http://www.delphion.com/
  - L.M.G.M. Tolhuizen and C.P.M.J. Baggen, *Method and deivce for error protection of programmable memories*, US Patent 5,896,397, April 20, 1999.
  - L.M.G.M. Tolhuizen and C.P.M.J. Baggen, *Method and apparatus for trackwise burst error correction in a multitrack storage format*, US Patent 5,910,961, June 8, 1999.

5 Lectures in 1999

- C. Archer
  - *Primitive geometries based on extensions of simple groups*, Université Libre de Bruxelles, Belgium, May 1999.
- V.B. Balakirsky
  - *A direct approach to searching with lies*, EIDMA Seminar Coding, Crypto & Information Theory, TU Eindhoven, January 8, 1999.
  - *Strategy for data transmission over binary channels with noiseless feedback and upper bound on the number of questions in searching with lies*, Final Symposium CINEMA, Essen, Germany, September 1999.
  - *Hashing of databases based on indirect observations of Hamming distances*, Seminar at the Institute for Experimental Mathematics, Essen, Germany, October 1999.
  - *Characterization of the secrecy of a common key constructed via data transmission over the two-way AND channel*, Seminar at the Institute for Problems of Information Transmission, Moscow, Russia, May 1999 (1), Seminar at the Aircraft Instrumentation Institute, St. Petersburg, Russia, May 1999 (2), Seminar at the TU Delft, October 1999 (3).
  - *An upper bound on the expected number of computations for maximum likelihood decoding of low-density codes*, EIDMA Seminar Coding, Crypto & Information Theory, TU Eindhoven, November 5, 1999 (1), Seminar at the Institute for Experimental Mathematics, Essen, Germany, November 1999 (2).
- P.H.T. Beelen
  - *What is* $N_8(4)$, EIDMA Seminar Combinatorial Theory, TU Eindhoven, March 3, 1999.
  - *Constructing AG codes*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 7, 1999.
  - *Genus and semigroups of complete intersections*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, October 20, 1999.
- A. Blokhuis
  - *The polynomial method in geometry*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 7, 1999.
- A. Bosselaers
  - *Software implementations of cryptographic algorithms,* International course on state of the art and evolution of computer security and industrial cryptography, Leuven, June 2, 1999.
- H.J. Broersma
  - *Graafkleuring en mobiele telecommunicatie*, Lustrum TW, Da Vinci, Enschede, April 14, 1999.
  - *Research in graph theory: personal history, future plans, and counterexamples to the 2-tough conjecture*, Royal Holloway College, Egham, UK, April 28, 1999.
  - *On some intriguing problems in Hamiltonian graph theory, a survey*, Workshop on Cycles and Colourings, Stara Lesna, Slowakije, September 6, 1999.
  - *Grafentheorie en telecommunicatie-netwerken*, Werkbezoek CvB aan TW, Toegepaste Wiskunde, Universiteit Twente, September 23, 1999.
  - *Counterexamples to the 2-tough conjecture*, EIDMA Lustrum congress, Mierlo, October 8, 1999.

- *Grafen in de praktijk*, Studiedag Nederlandse Vereniging van Wiskundeleraren, Bilthoven, November 13, 1999.
- *Equivalent conjectures on claw-free graphs*, DIMATIA Workshop on hamiltonicity of 4-connected line graphs, Nectiny, Tsjechie, November 15, 1999.
- *Counterexamples to the 2-tough conjecture*, DIMATIA Workshop on hamiltonicity of 4-connected line graphs, Nectiny, Tsjechie, November 16, 1999.
- *Over taai-taai en een vermoeden uit de grafentheorie*, Mathematisch Café, TW-Universiteit Twente, December 6, 1999.

• A.E. Brouwer

- *TBA*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, February 3, 1999.
- *Algebraic topology and discrete mathematics*, EIDMA Course Discrete Algebra and Geometry 2, TU Eindhoven, December 6, 13 and 20, 1999, January 10, 17 and 24, 2000.

• N.G. de Bruijn

- *Model voor associatief geheugen*, Katholieke Universiteit Nijmegen, May 19, 1999.
- *J.J.Seidel, carreer of a mathematician*, International Conference on Geometric and Algebraic Combinatorics, Oisterwijk, August 20, 1999.
- *Quasicrystals for beginners*, International Conference on Geometric and Algebraic Combinatorics, Oisterwijk, August 20, 1999.
- *Teaching logic in a style inspired by Automath*, LC99 Logic Colloquium 1999, Utrecht.
- *A model for associative memory, with possibilities to accommodate consciousness and thinking*, ICALP'99 26th International colloquium, Praag, 1999.

• B. De Bruyn

- *A common construction for several classes of generalized quadrangles*, Second Pythagorean Conference, Samos, Greece, May 31 - June 5, 1999.
- *Near hexagons with four points on a line*, Geometric and Algebraic Combinatorics, Oisterwijk, August 15-20, 1999.

• F. Buekenhout

- *The O'Nan-Scott Ttheorem*, Seminar Bingen-Cara on Permutation groups (4 hours), Vrije Universiteit Brussel, Belgium, January 1999.
- *Incidence geometry and finite groups*, 51st British Mathematical Colloquium, University of Southampton, Main Speaker, April 1, 1999.
- *Histoires de polyèdres*, Contact day of the Université libre de Bruxelles and the Ville de Bruxelles, April 27, 1999.
- *Géométrie d'incidence et groupes finis*, Colloquium at the Université de Picardie, Amiens, France, April 28, 1999.
- *Incidence geometry and finite groups*, Joint Congress of the Belgian Mathematical Society and the London Mathematical Society, Brussels, Belgium, May 15, 1999.
- *Veelvlakken: beginselen van Regulariteit en semi-Regulariteit*, VVWL Congress, Oostende, Belgium, July 2, 1999.
- *Les démonstrations: une vision génétique et en spirale*, SBPM Congress, Morlanwelz, Belgium, August 25, 1999.
- *La relation entre les géométries et les groupes*, Le programme d'Erlangen de Félix Klein (1872), Séminaire CREM-GEPEMA-UREM, November 19, 1999.

• Ph. Cara

- *Extending the Petersen graph with truncated inductively minimal geometries*, Seminar on Buildings and Finite geometry, Brussels, Belgium, Organisers: F. Buekenhout e.a., April 23, 1999.
- *Extensions of the Petersen graph with a nonlinear diagram*, Second Pythagorean Conference in Geometry, Combinatorial designs & related structures, Samos, Greece, organisers: M.-L. de Resmini e.a., May 31, 1999.
- *RWPRI geometries for the alternating group A8*, Conference on Geometric and Algebraic Combinatorics on the occasion of the 80th birthday of J.J. Seidel, Oisterwijk, organisers: A. Blokhuis and W. Haemers, August 20, 1999.

• C. Cerf

- *Detecting the chirality of knots and links*, Seminar on Buildings and Finite Geometry, University Gent and Université Libre de Bruxelles, May 7, 1999.
- *Noeuds et Chimie I*, Séminaire de la section de Mathématiques de l'Université de Genève, Switzerland, June 3, 1999.
- *Detecting the chirality of knots and links, with application to chemistry*, Minisymposium "Research Results by Women Postdocs", IVth International Congress on Industrial and Applied Mathematics, Edinbourgh, Scotland, July 5-9, 1999.
- Topological chirality-tutorial and lecture on Chirality of knots and links, Special session "DNA Topology" of the American Math. Society meeting, Austin, Texas, October 8-10, 1999.

• J. Claessens

- with M. Vandenwauver, *Web security,* International course on state of the art and evolution of computer security and industrial cryptography, Leuven, Belgium, June 3, 1999.
- *Web Security,* BIRA studiedag Computer- en Internetbeveiliging, December 2, 1999.

• F. De Clerck

- *Quasiquadrics in projective spaces*, Università di Roma "La Sapienza", Italy, April 1999.
- *Replaceable spreads of partial geometries, an update*, Università di Napoli, "Federico II", Italy, April 1999.
- *Two-weight codes, designs and partial geometries*, Geometric and Algebraic Combinatorics, Oisterwijk, August 15-20, 1999.
- *New constructions of (semi)partial geometries* and *Quasiquadrics and applications to designs*; two talks at Eötvös Lorànd University, Budapest, November 1999.

• A.M. Cohen

- *Algebras generated by extremal elements*, IWR, Universität Heidelberg, January 27, 1999.
- Presentation of "Algebra Interactive", Springer-Verlag, Heidelberg, January 28, 1999.
- *Groepen voortgebracht door spiegelingstori*, Colloquium TU Delft, January 29, 1999.
- *The OpenMath way of connecting proof checkers and computer algebra systems*, University of Saarbrücken, February 18, 1999.
- *The OpenMath way of connecting computer algebra and proof checking*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, February 24, 1999.
- *Lie algebra and geometry*, EIDMA Seminar Combinatorial Theory, Eindhoven, February 24, 1999.
- *Lie algebra and geometry*, L'Aquila, March 3, 1999.
- Opening talk, Seminar on OpenMath for Industry, June 11, 1999.

- *On the use of defining properties in content dictionaries*, 12-th OpenMath Workshop, Eindhoven, June 15, 1999.
- *Lie algebras and geometry*, Seidel Conference, August 18, 1999.
- lLecture at GROSTAT III, Eindhoven, September 9, 1999.
- *Connecting proof checkers and computer algebra using OpenMath*, TP-HOLS, Nice, September 14, 1999.
- IDA Demonstration, CLUSTER Open Distance Learning, Lausanne, October 1, 1999.
- *Linear representations of braid groups*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, October 27, 1999.
- *IDA, the next generation*, RIACA, Eindhoven, November 12, 1999.
- with F.G.M.T. Cuypers *Various facets of transvection groups, geometries and Lie algebras*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, December 8, 1999.

• G. Cornelissen

- *Zeros of Eisenstein series*, Journées arithmetiques, Rome, Italy, 1999.
- 2-*power torsion in the Jacobian of hyperelliptic curves over finite fields*, Finite Fields and Applications, Augsburg, 1999.
- *Automorphisms of Mumford curves*, Max-Planck-Institut für Mathematik, 1999.

• F.G.M.T. Cuypers

- *Embeddings of Delta spaces*, TU Eindhoven, April 28, 1999.
- *Linear groups generated by transvections*, University of Ghent, Belgium, June 21, 1999.
- Two talks for the 'scholierenmanifestatie', entitled *Foutje? Dat verbeteren we wel*, TU Eindhoven, October 13-14, 2000.
- *Dual affine planes and k-transvection groups*, TU Eindhoven, November 1, 1999.
- *The special linear groups generated by transvections*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, November 10, 1999.
- with A.M. Cohen *Various facets of transvection groups, geometries and Lie algebras*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, December 8, 1999.
- *Geometries, graphs and transvections in classical groups*, Universiteit Utrecht, December 9, 1999.

• E.R. van Dam

- *Fissions of classical self-dual association schemes*, Seventeenth British Combinatorial Conference, Canterbury, England, July 12, 1999.
- *Association schemes from affine spaces*, International Conference on Geometric and Algebraic Combinatorics, Oisterwijk, The Netherlands, August 19, 1999.
- *Amorphic association schemes*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 7, 1999.

• A. Delandtsheer

- *Finite flag-transitive linear spaces with alternating socle*, Euroconference on Algebraic Combinatorics and Applications, Goessweinstein, September 1999.

• M. Delanote

- *New classes of semipartial geometries*, Second Pythagorean Conference, Samos, Greece, May 31-June 5, 1999.
- *Partial geometries and the triality quadric*, Geometric and Algebraic Combinatorics, Oisterwijk, August 15-20, 1999.

- A. Devillers
  - *Espaces homogènes - un problème sur les corps gauches*, Sèminaire interuniversitaire d'algèbra, Mons, February 22, 1999.
  - *Ultrahomogeneous semilinear spaces*, Second Pythagorean Conference, Samos, Greece, June 1, 1999.
  - *Ultrahomogeneous semilminear spaces and symmetric groups*, Conference Algebraic Combinatorics and Applications (ALCOMA 99), Gossweinstein, Germany, September 12-19, 1999.
  - *Ultrahomogeneous semilinear spaces*, Kolloquium über Kombinatorik, B. Braunschweig, Germany, November 12, 1999.
- J.M. Doumen
  - *Weights of subcodes and curves with many rational points*, EIDMA Seminar Coding, Crypto & Information Theory, TU Eindhoven, May 7, 1999.
  - *Quantum Computing (1) – Introduction*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, November 3, 1999.
  - *Quantum Computing (3/3) – Factoring and Discrete Logarithms*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, November 17, 1999.
- J. Doyen
  - *Ancient Greek Mathematics*, Second Pythagorean Conference, Samos, Greece, May 29-June 5, 1999.
- J. Draisma
  - *Elements from Lie's classification*, EIDMA Seminar Combinatorial Theory, March 3, 1999.
  - *Realizing transitive Lie algebras*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 8, 1999.
- T.S.H. Driessen
  - *A bilateral probabilistic approach to solutions for cooperative TU-games*, 13th Italian Conference on Game Theory and Applications, Bologna, Italy, June 4, 1999.
  - *A bilateral probabilistic approach to cost allocation problems*, International Conference on Axiomatic Resource Allocation Theory, Namur, Belgium, July 2, 1999.
  - *A survey on cooperative TU-games and its solution theory*, Seminar at the Institute of Economic Research, Kyoto University, Kyoto, Japan, July 23, 1999.
  - *A weighted pseudo-potential approach to values for cooperative TU-games*, Seminar at the School of Political Science and Economics, Waseda University, Tokyo, Japan, July 27, 1999.
  - *A survey on cooperative TU-games and its solution theory*, Seminar at the Department of Value and Decision Science, Graduate School of Decision Science and Technology, Tokyo Institute of Technology, Tokyo, Japan, July 30, 1999.
  - *A weighted pseudo-potential approach to values for cooperative TU-games*, Seminar at the Department of Information and Management Science, Otaru University of Commerce, Otaru, Hokkaido, Japan, July 31, 1999.
  - *A survey on cooperative TU-games and its solution theory*, Seminar at the Hokkaido Chapter of Operations Research Society of Japan, Sapporo, Japan, August 2, 1999.
  - *A survey on cooperative TU-games and its solution theory*, Seminar at the Institute of Applied Mathematics, National Tsing Hua University, Hsinchu, Taiwan, August 12, 1999.

- *The potential approach to solutions for cooperative TU-games*, The 15th IFORS-conference, Beijing, China, August 19, 1999.
- *A survey on cooperative TU-games and its solution theory*, Seminar at the Department of Applied Mathematics, Northwestern Polytechnical University, Xian, China, August 30, 1999.
- *A survey on the classical potential approach to values for cooperative TU-games*, Seminar at the Department of Applied Mathematics, Northwestern Polytechnical University, Xian, China, August 31, 1999.
- *A survey on cooperative TU-games and its solution theory*, Seminar at the Department of Finance and Decision Sciences, Hong Kong Baptist University, Hong Kong, September 2, 1999.

- M.E. van Dijk
  - *Secret sharing schemes*, EIDMA course Coding Theory, Information Theory and Cryptology, TU Eindhoven, February 25, 1999.
  - *Generalized key equations*, EIDMA Seminar Coding, Crypto & Information Theory, TU Eindhoven, March 5, 1999.
  - with L. Tolhuizen *Efficient encoding for a class of subspace subcodes*, EIDMA Seminar Coding, Crypto & Information Theory, TU Eindhoven, May 7, 1999.
- S. Egner
  - *Randomized placement of blocks ond disks – Throwing wired pairs of balls into bins*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, December 1, 1999.
- C. Feremans
  - *The generalized minimum spanning tree, polyhedra and Branch-and-Cut*, Orbel 13, Brussels, Belgium, January 21-22, 1999.
  - *The generalized minimum spanning tree facets, Journées du troisiéme cycle FNRS en Programmation Mathématique*, Han-sur-Lesse, Belgium, March 4-5. 1999.
  - *The generalized minimum spanning tree, polyhedra and branch-and-cut*, Aussois workshop on combinatorial optimization, Aussois, France, March 8-12, 1999.
  - *The generalized minimum spanning tree, polyhedra and branch-and-cut*, Journées de l'Optimisation, Montréal, Canada, May 10-12, 1999.
  - *The generalized minimum spanning tree, polyhedra and branch-and-cut*, Twente Workshop on graphs and combinatorial optimization, Enschede, The Netherlands, May 26-28, 1999.
  - Ecotel'99, Deuxième école d'hiver des télécommunications de Sofia Antipolis, Antibes, France, December 6-10, 1999.
- S. Fiorini
  - *Transitive orientations, extended transitive orientations and some related 0/1-polytopes*, ULB-RUG Seminar, Gent, Belgium, April 1999.
  - *Automorphism groups of some order polytopes*, European Chapter on Combinatorial Optimization XII, Bendor Island, France, May 1999.
  - *Adjacency on weak order polytopes*, Order, Algorithms and Applications '99, Montpellier, France, August 1999.
- B. Fortz
  - *Design of survivable networks with bounded rings*, Centre de Recherches sur les Transports, Université de Montréal, Canada, March 1999.
  - C.R.T. Seminar, Montréal, Canada, March 25, 1999.

- *Internet traffic engineering by optimizing OSPF weights*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 8, 1999.
- *Internet traffic engineering by optimizing OSPF weights*, Philips Research Seminar, Eindhoven, The Netherlands, November 23, 1999.

• J. Van Geel

- *The u-invariant of function fields over curves over local fields*, Quadratic Forms, Oberwolfach, Germany, May 1999.

• B.S. Gelbord

- *Spaces of bounded rank in an exterior algebra*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, November 24, 1999.

• F. Geurts

- *Modélisation, simulation et régulation de réseaux de transports collectifs*, Faculté Universitaire Notre Dame de Namur, Groupe de Recherche sur les Transports, Namur, Belgium, May 12, 1999.
- *le bug de l'an 2000*, Administration Communale de Woluwé Saint Lambert, Bruxelles, Belgium, June 4, 1999.
- *Preuve d'algorithmes probabilistes*, PhiDani Software, Bruxelles, Belgium, July 7, 1999.
- *Optimal irreversible dynamos in chordal rings*, 25th International Workshop on Graph-Theoretic Concepts in Computer Science, WG'99, Ascona, Switzerland, June 17-19, 1999.

• P. Gober

- *Multi access communication*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 8, 1999.

• B. Goldengorin

- *An old and new justification of the dichotomy algorithm for submodular set function maximization problem*, 19th IFIP TC7 Conference on System Modelling and Optimization, Cambridge University, England, July 15, 1999.
- *The data-correcting algorithm for maximization of submodular functions*, Optimization Seminar, Department of Technical Mathematics and Informatics, Faculty of Information Systems and Technology, Delft University of Technology, The Netherlands, September 21, 1999.
- *The maximization of submodular functions: theory and applications*, Mathematical Programming Seminar, Center for Operations Research and Econometrics, Louvain-la-Neuve, Belgium, November 16, 1999.
- *Non-binary branching rules in submodular optimization*, Stern School of Business, New York University, New York, USA, December 2, 1999.
- *Data-correcting algorithms in combinatorial optimization*, DIMACS, Center for Discrete Mathematics and Theoretical Computer Science, Rutgers University, New Brunswick, New Jersey, USA, December 6, 1999.
- *Implicit enumeration algorithms for the maximization of submodular functions*, Center for Operations Research, Rutgers University, New Brunswick, New Jersey, USA, December 9, 1999.

• E. Govaert

- *Distance-preserving maps in generalized polygons*, Second Pythagorian Conference, Samos, Greece, June 1, 1999.
- *A quadrangle and a forbidden hexagon in the generalized hexagon $H(q)$*, Conference Generalized Polygons, Würzburg, Germany, October 6, 1999.

- R. Gramlich
  - *Locally P_n graphs*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, March 10, 1999.
  - talk at Geometry Seminar in Gent, Belgium, March 18, 1999.
  - *Concepts of algebraic topology* and *Algebraic topology in geometry*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, June 2, 1999.
  - talk at Conference in Würzburg, Germany, October 5, 1999.
  - *Homomorphisms of polar spaces*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, December 1, 1999.
- Ph. Grégoire
  talks at:
  - Politecnico di Milano, Italy, February 1999.
  - Universität Kaiserslautern, Germany, March 1999.
  - Università degli Studi di Padova, Italy, May 1999.
  - Politecnico di Milano, Italy, October 1999.
  - Università degli Studi di Padova, Italy, November 1999.
  - *Les journées industrielles de la ROADEF: Transport et logistique: Apport des nouvelles technologies*, Université de Valenciennes et du Hainaut-Cambrésis, Valenciennes, France, November 1999.
  - Third ALIO-EUROPE Workshop on Applied Combinatorial Optimization, Ettore Majorana Centre, Erice, Italy, November 2-6, 1999.
- W.H. Haemers
  - *Pseudo orthogonal Latin squares of order six*, Gent, Belgium, February 5, 1999.
  - *Zoektocht naar pseudo orthogonale Latijnse vierkanten van de orde zes*, Utrecht, April 8, 1999.
  - *Graphs, eigenvalues and bicliques*, Brussels, Belgium, May 15, 1999.
  - *An infinite family of quasi-symmetric designs*, Samos, Greece, June 3, 1999.
  - *Resolveble coverings, een tafelschikkingsprobleem*, Nijmegen, December 10, 1999.
- A. Hekstra
  - *Turbo error control coding*, Philips Research, Eindhoven, December 11, 1999.
- C. Huybrechts
  - *An interplay between diagram geometries and a problem in projective spaces*, Siena, Italy, January 9, 1999.
  - *Flag-transitive $c.AG^*$ -geometries*, Firenze, Italy, January 11, 1999.
  - *Polyhedra and incidence geometries*, London, February 8, 1999. in the "pure Mathematics monday seminar" organised by Steve Donkin.
  - *The plane of Cremona: a flavour of Tits' lessons at the ULB*, Combinatorics Study Group, London, March 19, 1999.
  - *Approaching diagram geometry via polyhedra*, University of Chicago, April 22, 1999.
  - *An incursion into diagram Ggeometry*, Tufts University, April 30, 1999.
  - *A unified construction for $c^*.c$- and $L.L^*$ -geometries in $AG(3, q)$*, Congress Third Shanghai Conference on Designs, codes and Finite Geometries, Shanghai, China, organized by E. Bannai e.a., May 14-18, 1999.

  - *A unified construction for c^*.c- and $L.L^*$ - geometries in projective spaces*, Second Pythagorean Conference, Samos, Greece, organised by de Resmini e.a., May 29-June 5, 1999.
  - *A unified construction for c^*.c- and $L.L^*$ - geometries in projective spaces*, 17th British Combinatorial Conference, University of Kent, Canterbury, England, July 12-16, 1999.
  - *A unified construction for c^*.c- and $L.L^*$ - geometries in projective spaces*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, October 5, 1999.
  - *Approaching diagram geometry via polyhedra*, University of Sussex, November 5, 1999.
  - *Some procedures to construct diagram geometries*, Università di Catania, December 6, 1999.

- K.A.S. Immink
  - *A Survey of high-rate codes*, Asian Symposium on Information Storage Technology, Singapore, Jan. 25-26, 1999.
  - *Comparison of two coding schemes for generating dc-free RLL sequences* (joint work with W.Y.H. Wang, X.B. Xu and C.T. Chong), Int. Symp. on Optical Data Storage, Hawaii, July 1999.

- G. Ivanyos
  - *Fast randomized algorithms for matrix algebras over finite fields*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, January 20, 1999.
  - *On the isomorphism problem of simple algebras*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, April 20, 1999.
  - *Extremal elements in Lie algebras of characteristic two*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, June 29, 1999.
  - *Extremal elements*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, December 15, 1999.

- C.J.A. Jansen
  - *Stream ciphers based on more LFSR's*, EIDMA course Coding Theory, Information Theory and Cryptology 3, TU Eindhoven, March 4, 1999.
  - *Protection of intellectual property: an information security issue*, Philips Research, Eindhoven, April 1999.

- P. Kazakov
  - *On the CRC codes with 16 bit redundancy*, EIDMA Seminar Coding, Crypto and Information Theory, Eindhoven, May 7, 1999.

- M. Labbé
  - *The Median cycle problem*, Aussois workshop on combinatorial optimization, Aussois, France, March 8-12, 1999.
  - *Binlinear bilevel programming*, Trondheim Seminar on Industrial Economics and Operations Research, Norwegian University of Science and Technology, Trondheim, March 18, 1999.
  - *Bilinear bilevel programming*, Seminar at Facultad de Mathemeticas, Universitad de la Laguna, Tenerife, April 7, 1999.
  - *The uncapacitated network design with bifurcated routing*, Seminar at Limos, Université Blaise Pascal-Clermont II, Clermont-Ferrand, May 3-5, 1999.
  - *The Median cycle problem*, International Workshop on Locational Decisions VIII (ISOLDE VIII), June 23-29, 1999.
  - *Obnoxious p-Median problems*, IFORS'99, Beijing, China, August 16-20, 1999.

- *Reliable network design problems*, EIDMA Lustrum Congress, Mierlo, The Netherlands, October 8, 1999.
- *Reliable network design problems*, Third ALIO-EUROPE Workshop on Applied Combinatorial Optimization, Ettore Majorana Centre, Erice, Italy, November 2-6, 1999.
- *Survivable network design*, Ecotel'99, Deuxième école d'hiver des télécommunications de Sofia Antipolis, Antibes, France, December 6-10, 1999.
- *Course "Location Theory"*, 15 hours, DEIS, Universita dei Bologna, Italy, December 14-17, 1999.

• M. Lavrauw

- *Scattered spaces with respect to a spread in $PG(n, q)$*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, May 26, 1999.

• D. Leemans

- *Constructing coset geometries with MAGMA*, University of Newcastle, Australia, April 22, 1999.
- *Constructing coset geometries with MAGMA*, Algebra Seminar, University of Sydney, Australia, April 23, 1999.
- *Incidence geometry and finite groups*, Conference (Moufang) Polygons and (Twin) Buildings organised by H. Van Maldeghem, Gent, June 21-25, 1999.
- *On a rank five geometry of Meixner for the Mathieu group M12*, Universität Halle-Wittenberg, September 26, 1999.

• J.K. Lenstra

- *Newspapers, timetables, and whizzkids*, Technische Universität Berlin, Berlin, Germany, February 2, 1999.
- *Whizzkids: two exercises in computational discrete optimization*, Fourth International Conference on Industrial and Applied Mathematics Edinburgh, Scotland, July 5, 1999.
- *De strijd tegen de complexiteit*, Informatica Instituut, Universiteit Utrecht, November 25, 1999.
- *Deterministic scheduling: The mystical power of twoness*, Philips Workshop on Scheduling and Resource Management SCHARM'99, Eindhoven, The Netherlands, December 8, 1999.

• J.-P. Linnartz

- *Digital watermarking*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 8, 1999.

• J.H. van Lint

- Invited speaker at the symposium Combinatorics and Communications Applications", Royal Holloway College, London, April 14 and 15, 1999.
- *The identifiable parent property*, Royal Holloway College, London, April 15, 1999.
- *The identifiable parent property*, Symposium Beveiliging in de Telematica, Universiteit Twente, April 16, 1999.
- *The compact disc (twice)*, KU Leuven, Belgium, April 21, 1999.
- Invited speaker at the congress Geometric and Algebraic Combinatorics, Oisterwijk, August 16-20, 1999.
- *De wiskunde van de CD*, Congress Geometric and Algebraic Combinatorics, Oisterwijk, August 19, 1999.
- *De wiskunde van de CD*, Symposium 'Tussen Bits en Signalen', KU Nijmegen, September 10, 1999.

- *An elementary exposition of the mathematics of the CD player*, Columbia University, New York, November 8, 1999.
- *On perfect ternary constant weight codes*, DIMACS, Rutgers University, New Jersey, November 9, 1999.
- *Codes with the identifiable parent property*, November 11, 1999.
- *40 jaar THE-TUE*, valedictory lecture TU Eindhoven.

• A. Lukito

- *Bounds for snake-in-the-box codes*, SEAMS Conference on Mathematics and its Applications, Yogyakarta, July 7, 1999.

• J.G. Maks

- *Optimal subcodes of second order Reed-Muller codes and maximal linear subspaces of bivectors of maximal rank*, International Conference on Algebraic Combinatorics, Maratea, October 14, 1999.

• H. Van Maldeghem

- *Slim polar and projective spaces of low rank*, Finite Geometry Summer School Workshop on Projective and Polar Geometry, Adelaide, Australia, January 11-15, 1999.
- *Embeddings, distance, ovoids and spreads of generalized polygons*, Finite Geometry Summer School Workshop on Projective and Polar Geometry, Adelaide, Australia, January 11-15, 1999.
- *Generalized polygons*, BLMS'99, Combinatorics and Finite Geometries, Brussels, Belgium, May 14-16, 1999.
- *Embeddings of line-regular hexagons in finite projective spaces*, Combinatorial Designs and Related Structures, Pythagorion, May 30-June 5, 1999.
- *Regular actions on generalized polygons*, Geometry seminar, Würzburg, June 12, 1999.
- *Epimorphisms of generalized polygons*, Geometric and Algebraic Combinatorics, Oisterwijk, August 15-21, 1999.
- *Constructions of small polygons*, Generalized Polygons, Würzburg, Germany, October 4-7, 1999.
- *Involutions, embeddings, distances & applications*, Generalized Polygons, Würzburg, Germany, October 4-7, 1999.
- *Geometries, buildings, groups*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 8, 1999.
- *Universal Embeddings for Hexagons of order 2*, Geometry Seminar, Würzburg, December 6, 1999.

• K. Martin

- *Key recovery and escrow,* International course on state of the art and evolution of computer security and industrial cryptography, Leuven, June 3, 1999.

• R.H. Motwani

- *Simultaneous zero-tailing of parallel concatenated codes*, joint work with M.E. van Dijk, S. Egner and A. Koppelaar, EIDMA Seminar Coding, Crypto & Information Theory, TU Eindhoven, November 5, 1999.

• C. Nocq

- *A relaxation of the 2-connected subgraph polytope*, Journées du troisième cycle FNRS en Programmation Mathématique, Han-sur-Lesse, Belgium, March 4-5, 1999.

• R. Pellikaan

- *Algebraisch geometrische codes, reine oder angewandte Mathematik?*, Math. Seminar, Univ. Kassel, April 27, 1999.
- *On the dimension of order domains*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, May 12, 1999.
- *Order domains and codes*, IMECC, Univ. Campinas, Brasil, June 11, 1999.
- *An elementary approach to algebraic geometry codes*, Elec. Eng., Univ. Campinas, Brasil, June 14, 1999.
- *The Newton-polygon and curves with many rational points*, IMPA, Rio de Janeiro, Brazil, June 16, 1999.
- *Error-correcting pairs*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, November 24, 1999.

• B. Preneel

- *Authentication codes* and *Cryptanalysis*, EIDMA course Coding Theory, Information Theory and Cryptology 3, TU Eindhoven, February 4, 1999.
- *Technical approaches to information security,* International course on state of the art and evolution of computer security and industrial cryptography, Leuven, Belgium, June 1, 1999.
- *Public-key cryptography,* International course on state of the art and evolution of computer security and industrial cryptography, Leuven, Belgium, June 1, 1999.
- *Hash functions and MACs: state of the art,* International course on state of the art and evolution of computer security and industrial cryptography, Leuven, Belgium, June 2, 1999.
- *International standarization of IT security*, International course on state of the art and evolution of computer security and industrial cryptography, Leuven, Belgium, June 4, 1999.
- *How secure should your application be?* ECE99 – The 12th EEMA Annual Conference & Exhibition, Paris, France, June 8-11, 1999.
- *Protecting your communications with cryptography*, EUFIS, Second European Open Sources Workshop, Archennes, Belgium, June 17-18, 1999.
- with C. D'Halluin, G. Bijnens, V. Rijmen, *Belgian comments on US pudding,* presented at the rump session of Crypto'99, Santa Barbara, CA, USA, August 15-19, 1999.
- *CBC-MAC revisited,* Workshop on Cryptology, (by invitation), Luminy, France, September 27-30, 1999.
- *AES and the next generation of cryptographic algorithms*, ISSE '99, Berlin, October 4-6, 1999.
- *AES (Advanced Encryption Standard): an update on progress,* Compsec'99, London, UK, November 3-5, 1999.
- *PKI: an introduction to the essentials,* EEMA Legal Workshop, Brussels, Belgium, November 23-24, 1999.
- *Cryptografie: een inleiding,* BIRA studiedag Computer- en Internetbeveiliging, December 2, 1999.

• R. Puystjens

- *Generalized inverses of morphisms in additive categories*, Centro de Matematica, Universidade do Minho, Portugal, June 1999.
- *About the von Neumann Regularity of lower triangular Toeplitz matrices with von Neumann regular components*; (with P. Patricio), 8th ILAS conference, Barcelona, July 1999.
- *The Moore-Penrose inverse of von Neumann regular matrices over rings* (with P. Patricio), 8th ILAS conference, Barcelona, July 1999.

- P.L.A. Roelse
  - *Cryptanalysis of the Wu-Dawson public key cryptosystem*, Fifth International Conference on Finite Fields and Applications, University of Augsburg, Germany, August 20, 1999.
- V. Rijmen
  - *Basic concepts of cryptography*, International course on state of the art and evolution of computer security and industrial cryptography, Leuven, June 1, 1999.
  - *Linear codes in modern cryptographic algorithms,* EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 7, 1999.
- S. van Rijnswou
  - *Distinguishing orbits of the action of L_3 on ternary quartics*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, January 13, 1999.
- L.A.M. Schoenmakers
  - *Protocols for electronic payment systems*, EIDMA course Coding Theory, Information Theory and Cryptology 3, TU Eindhoven, February 11, 1999.
  - *Modern cryptographic protocols for electronic voting and electronic payment, part I*, Palmse, Lahemaa, Estland, 4th Estonian Winter School in Computer Science, March 2, 1999.
  - *Modern cryptographic protocols for electronic voting and electronic payment, part II*, Palmse, Lahemaa, Estland, 4th Estonian Winter School in Computer Science, March 3, 1999.
  - *Modern cryptographic protocols for electronic voting and electronic payment, part III*, Palmse, Lahemaa, Estland, 4th Estonian Winter School in Computer Science, March 4, 1999.
  - *Electronic voting through publicly verifiable secret sharing*, COSIC seminar, KU Leuven, Belgium, March 17, 1999.
  - *Electronic payments and electronic voting*, Multimedia Paviljoen, Euforce / Informatiebeveiliging, Eindhoven, March 23, 1999.
  - *Anonieme transacties in de digitale wereld*, Symposium Vrede en Veiligheid, Universiteit Twente, section: "We liggen bloot - de risico's van elektronische handel", March 24, 1999.
  - Kerberos and SESAME, Multimedia Paviljoen, Euforce / Informatiebeveiliging, March 30, 1999.
  - Demo and Practicum Electronic Voting, Multimedia Paviljoen, Euforce/Informatiebeveiliging, Eindhoven, April 20, 1999.
  - *Cryptographic protocols for electronic voting*, TU Eindhoven, EIDMA Seminar Combinatorial Theory, May 26, 1999.
  - *The future of electronic money, State of the art and evolution of computer security and industrial cryptography*, ESAT-COSIC course, KU Leuven, Belgium, June 4, 1999.
  - *A simple publicly verifiable secret sharing scheme and its application to electronic voting*, CRYPTO'99: 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16, 1999.
  - *Quantum computing, part II*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, November 10, 1999.
- K.A. Schouhamer Immink
  - *Comparison of two coding schemes for generating dc-free RLL sequences*, (joint with W.Y.H. Wang, X.B. Xu and C.T. Chong), International Symposium on Optical Data Storage, Hawaii, July 1999.

- A. Schrijver
  - *Permanents*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 7, 1999.
- P. Schuurman
  - *Approximate schedules*, EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 7, 1999.
- M. Sebille
  - *There exists a simple non-trivial t-design with an arbtrarily large automorphism group for every t*, Seminar on Buildings and Finite Geometry, Universiteit Gent and Université libre de Bruxelles, organisers: F. Buekenhout e.a., April 22, 1999.
  - *On a result of Cameron and Praeger on block-transitive point-imprimitive t-designs*, Conference Algebraic Combinatorics and Applications (ALCOMA 99), Gossweinstein, Germany, September 12-19, 1999.
  - *For every t, there is a t-design with arbitrarily large automorphism group*, Kolloquium über Kombinatorik, Braunschweig, Germany, November 12-13, 1999.
- G. Sierksma
  - *Duality and degenaracy degrees*, IFORS'99 Conference, Institute of Applied Mathematics, Chinese Academy of Sciences, Beijing, China, August 16-20, 1999.
  - *Solving large instances of the quadratic cost partition problems by the data-correcting algorithm*, IFORS'99 Conference, Institute of Applied Mathematics, Chinese Academy of Sciences, Beijing, China, August 16-20, 1999.
  - *The computer coach*, DCCN'99, Tel Aviv, Israel, November 8-12, 1999.
- J. Simonis
  - *Strengthening the Gilbert-Varshamov bound*, Workshop on Coding and Cryptography, Paris, January 12, 1999.
  - *Adding a parity check bit*, Discrete Mathematics Seminar of the Bulgarian Academy of Sciences, Sofia, March 26, 1999.
  - *Optimal subcodes of second order Reed-Muller codes and maximal linear subspaces*, Geometric and Algebraic Combinatorics Conference, Oisterwijk, August 19, 1999.
  - *Almost affine codes*, Fields Institute for research in Mathematical Sciences, Toronto, September 15, 1999.
- M. Stam
  - *Toggling schemes for electronic voting* (master's thesis), EIDMA Cryptography Working Group, La Vie, Utrecht, April 16, 1999.
- H.J.M. Sterk
  - *On the space of quartic curves*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, April 20, 1999.
- L. Storme
  - *Caps in finite projective spaces and their links to coding theory*, main speaker at the conference The Third Shanghai International Conference on Designs, Codes and Finite Geometries, Shanghai, China, May 1999.
  - *Partial spreads in $PG(3, q)$*, Second Pythagorean Conference, Samos, Greece, May 1999.
  - *On the cardinality of the smallest covers of $Q(4, q)$, q odd*, Geometric and Algebraic Combinatorics, Oisterwijk, The Netherlands, August 1999.
  - *Caps in $PG(N, 3)$*, Eötvös Loránd University Budapest, Hungary, September 1999.

- L. Stougie
  - *On-line single server dial-a-ride problems*, Universiteit Utrecht, January 29, 1999.
  - *On-line single server dial-a-ride problems minimizing average completion time*, Farewell seminar for Han Hoogeveen, TU Eindhoven, February 19, 1999.
  - *Classification of dial-a-ride problems*, University of Rome "La Sapienza", Rome, Italy, April 23, 1999.
  - *On-line multi threaded scheduling*, Dagstuhl Workshop on on-line algorithms, Schloss Dagstuhl, Dagstuhl, Germany, June 21-26, 1999.
  - *A fast randomized algorithm for stochastic programming problems*, DIMACS Workshop on Probabilistic Analysis, DIMACS, Piscataway, NJ, USA, November 1-3, 1999.
- R. Teunter
  - talk at the Life Cycle Conference, Kingston Ontario Canada, June 1999.
  - *EOQ's for reverse logistics*, ISIR Summer School, Exeter England, August 1999.
  - talk at SOR '99, Symposium on Operations Research, Magdeburg Germany, September 1999.
- J.A. Thas
  - Six talks on *m-Systems and partial m-systems of polar spaces: old and new results*, Seminar on Incidence Geometry, University of Gent, February - March 1999.
  - *Weak embeddings of line-regular generalized hexagons in finite projective spaces*, Second Pythagorean Conference, Samos, Greece, May 30 - June 5, 1999.
  - *Generalized Quadrangles: The axiom of Veblen, Property (G), flocks and BLT-sets*, Main speaker at the Conference (Moufang) Polygons and (Twin) Buildings, Gent, Belgium, June 1999.
  - *Finite geometries, varieties and codes* and *Embeddings of the flag geometry of projective planes in finite projective spaces and applications*, two talks on *3-Regularity in generalized quadrangles: a survey, recent results and the solution of a longstanding conjecture*, two talks on *m-Systems and partial m-systems of polar spaces: old and new results*, University of Canterbury, Christchurch, New Zealand, July - August 1999.
  - Two talks on *Veronese varieties in $PG(n, q)$: applications*, *Flocks and hyperovals* and *Constructions of semipartial geometries* at the Seminar on Incidence Geometry, University of Gent, Belgium, November 1999.
- H.C.A. van Tilborg
  - *A construction of systematic authentication codes based on error-correcting codes*, 1999 Workshop on Coding and Cryptography, Paris, France, January 13, 1999.
  - *Cryptologie en wachtwoorden in de moderne tijd*, Panama Voorjaarsdag 1999, Gouda, April 16, 1999.
  - *ECC: new solutions for old problems?*, Workshop Cryptographic Security Aspects of Smartcards & Internet, Amsterdam, May 21, 1999.
  - *Review of cryptographic algorithms*, Workshop Cryptographic Security Aspects of Smartcards & Internet, Amsterdam, May 21, 1999.
  - *A tutorial introduction to EC-cryptography*, IEEE International Symposium on Information Theory, Metsovo, Greece, June 30, 1999.
  - *Why Are elliptic curve cryptosystems of interest?*, Mathematics Colloquium, Debrecen, Hungary, April 27, 1999 (1), EIDMA Lustrum Congress, Carlton De Brug, Mierlo, October 8, 1999 (2).
  - Lectures on Cryptography, Tianjin, China, Visit Chinese Universities, Tianjin, China, October 1999.

– Series of Lectures on Cryptography, Beijing and Xi'an China, Visit Chinese Universities, October 1999.

- Tj.J. Tjalkens
  - *Variable-to-fixed length codes: a geometrical approach*, presentation for Information Theory Seminar, Lund University of Technology, Lund, Sweden, April 13, 1999.
  - *Random-access data compaction*, presentation for Information Theory Seminar, Lund University of Technology, Lund, Sweden, May 11, 1999.
  - *On the complexity of the Huffman-Shannon-Fano code*, EIDMA Seminar Coding, Crypto & Information Theory, September 3, 1999.
  - *On the complexity of minimum redundancy codes*, Workshop on Data Compression, 1-2 November 1999, University of Bielefeld, Germany, November 1-2, 1999.
- V. Venugopal
  - *Managing variety and short life cycle products in supply chain*, Supply Chain World Europe Conference, Amsterdam, September 20-22, 1999.
- W.F.J. Verhaegh
  - *Multidimensional periodic scheduling*, Fourth Workshop on Models and Algorithms for Planning and Scheduling Problems (MAPSP), Renesse, The Netherlands, June 1999.
  - *Capacity scheduling for data services over digital networks*, Philips Workshop on Scheduling and Resource Management (SCHARM), Eindhoven, The Netherlands, December 1999.
- E.R. Verheul
  - *Key-recovery techniques*, EIDMA course Coding Theory, Information Theory and Cryptology 3, TU Eindhoven, February 18, 1999.
- A.J. Han Vinck
  - *Optical communications*, Universiteit Twente, February 8, 1999.
  - *Basic elements in random access communications*, University of Duisburg, Germany, February 11, 1999.
  - *Coding for the optical OR channel*, EIDMA Seminar Coding, Crypto and Information Theory, TU Eindhoven, March 5, 1999.
  - *Introduction to source, channel and security coding*, Third African Regional Workshop on Communications, Lusaka, Zambia, July 25-30, 1999.
  - *Error detection/correction: Point-to-point and links*, Third African Regional Workshop on Communications, Lusaka, Zambia, July 25-30, 1999.
  - *Coding for random access communications*, 1st International OFDM Workshop in Hamburg, September 21-22, 1999.
  - *Coding and modulation for power line communications*, Graduate College Multimedia, Rostock, Germany, November 18, 1999.
  - With T. Wadayama, *DC-free binary convolutional codes*, SITA 99, Yuzawa, Niigata, Japan, November 30 - December 3, 1999.
  - with J. Häring and T. Wadayama, *Combined M-FSK modulation and coding*, SITA 99, Yuzawa, Niigata, Japan, November 30 - December 3, 1999.
- P.A.J. Volf
  - *Maximizing, weighting and switching*, Workshop on Data Compression, University of Bielefeld, Germany, November 1-2, 1999.
- T. Vredeveld

- *Semidefinite relaxations for combinatorial optimization problems: some attempts*, Utrecht, 4th HPMMO One-day seminar, January 22, 1999.
- *On local search for* $Q||C_max.$, Eindhoven, Eidma Optimization Seminar, July 22, 1999.
- *Experimental analysis of approximation algorithms*, Eindhoven, 6th HPMMO One-day seminar, September 1, 1999.
- *Empirical analysis of approximation algorithms for* $R||w_jC_j$, 7th HPMMO One-day seminar, November 19, 1999.

- H.L.T. Wanders
  - *Integrating cognitive science and operations research techniques for building a better planning support system for a solid board factory*, HCP'99, Human Centered Processes, 10th Mini Euro Conference, Brest, France, September 22-24, 1999.
- M. van Weert
  - *Virtual private network guard*, EIDMA Cryptography Working Group, La Vie, Utrecht, April 16, 1999.
- E. De Win
  - *Elliptic-curve public-key cryptography,* International course on state of the art and evolution of computer security and industrial cryptography, Leuven, June 4, 1999.
- C. Wynants
  - *Optimizing reserve capacities of a partially equipped SHD network*, Orbel 13, Brussels, Belgium, January 21-22, 1999.
- A.J. van Zanten
  - *Upper bounds for snake-in-the-box codes*, EIDMA Seminar Coding, Crypto and Information Theory, Eindhoven, January 8, 1999.
  - *Complexity and combinatorial algorithms*, SIKS course, Zeist, May 31, 1999.
  - *Rekenend denken*, Inaugural Address, Maastricht, November 5, 1999.

6 External Grants in 1999

- P. Beelen
  - PhD position at the TU Eindhoven financed by NWO till September 2002.
- B. De Bruyn
  - Position financed by ”Fund of scientific research - Flanders”.
  - Grant of ”Fund of scientific research - Flanders” for visiting the University of Colorado at Denver (from April 11th till May 21th 1999).
- F. Buekenhout
  - Research grant of the FNRS (Fonds National de la Recherche Scientifique de Belgique) in order to run MAGMA at the Université Libre de Bruxelles
- Ph. Cara
  - Position paid by FNRS ”Fonds National de la Recherche Scientifique de Belgique”.
- C. Cerf
  - Travel grant of the ”Program in Mathematics and Molecular Biology”, USA, January 2000.
  - Selection by a threefold committee (Association for Women in Mathematics-USA, European Women in Mathematics, Society for Industrial and Applied Mathematics-USA) to present results at ”Research Results by Women Postdocs”, Edimbourgh, Scotland, July 5-9, 1999.
- A.M. Cohen received financial support for the following projects:
  - AIDA (SWON).
  - Hongarije-Nederland exchange (OTKA/NWO).
  - OpenMath (ESPRIT, EC project no. 24969).
  - Meaningful Mathematical Messages on World Wide Web (SION).
- A. Devillers
  - Position paid by FNRS ”Fonds National de la Recherche Scientifique de Belgique”.
- C. Huybrechts
  - Position paid by FNRS (Fonds National de la Recherche Scientifique de Belgique) (permanent position).
  - Research Assistant at Queen Mary and Westfield College, London in the context of a ”Marie Curie Research Training Grant” from the program ”Training and Mobility for Researches” of the European Commission.
  - ”Chargè de cours á temps partiel” at the Université libre de Bruxelles.
- E. Kuijken
  - Position financed by the FWO-Vlaanderen since October 1999.
- D. Leemans
  - Travel grant from the FNRS to go to Sydney, 1999.
  - Travel grant from the FNRS to go to Halle (Germany), 1999.
- J.K. Lenstra organised a workshop on models and algorithms for planning and scheduling problems that was held in Renesse from June 14-18, 1999, and for which he received about NLG 50.000 financial support from several companies and institutes.

- E. Levner
  - Position at University of Groningen - Scholarship financed by NWO and SOM.
- D. Luyckx
  - Position financed by the FWO-Vlaanderen since October 1999.
- M. Sebille
  - Grant of the FRIA (Fonds pour la formation la Recherches dans l'Industrie et l'Agriculture).
- J.A. Thas, F. De Clerck, L. Storme and H. Van Maldeghem (University of Gent, Belgium).
  - a grant "Krediet aan Navorsers" from F.W.O.-Vlaanderen (Fund for Scientific Research Flanders, Belgium)
  - a GOA-grant (2000-2005) from the University of Gent.
- F.M.J. Willems received a grant from KNAW to participate in the IEEE Information Theory and Communications Workshop in the Kruger National Park, South Africa, from June 20-25, 1999.
- COSIC (K.U.Leuven) acknowledges financial support from K.U.Leuven Research Council, the Flemish (FWO-V and IWT) and Federal Government (S.S.T.C.), and The European Commission.
- Institute for Experimental Mathematics, Essen, Germany
  - DFG Project "Informations- und Codierungstheorie f"ur Vielfachzugriffsverfahren" with Yerevan, Armenia (Prof. Khachatrian), 1999-2002.
  - NRW Research Project "Datensicherheit" of the universities of Essen, Bochum, Hagen, Dortmund and Siegen, 1999-2002.
  - VW Project "Entwicklung von "Ubertragungsverfahren in einem System mit mehreren Teilnehmern", Cooperation with the "Korea Advanced Institute of Science and Technology", Taejon, S"udkorea, until 31 March, 1999.
  - Graduate College CINEMA, "Consumer and Industrial Networks for Electronic Data Transfer and Multi-Media Applications", Cooperation with the universities of Duisburg (Prof. Wolff, Prof. Geisselhardt), Twente (Prof. Niemegeers) and Delft (Prof. Biemond), until 31 October, 1999.

7 Noteworthy Activities in 1999

7.1 Awards

- K.A.S. Immink
  - Edison Medal awarded by the IEEE, 1999, for a career of creative contributions to the technologies of digital video, audio, and data recording.
  - AES Gold Medal awarded by the Audio Engineering Society, 1999, for significant contributions to the advancement of consumer audio technology.

7.2 Ph.D. Degrees

- M.S. Bargh, *Coding Strategies for Channels with Feedback*, TU Eindhoven, September 28, 1999. Supervisors: prof.dr.ir. J.P.M. Schalkwijk and prof.dr.ir. Van der Meulen.
- R.J. Blok, *On geometries related to buildings*, TU Delft, May 18, 1999. Supervisors: prof.dr. A.E. Brouwer and prof dr.ir. T.H.M. Smits.
- S.A. Brands, *Rethinking public-key infrastructures and digital certificates - building in privacy*, TU Eindhoven, October 1, 1999. Supervisors: prof.dr.ir. H.C.A. van Tilborg and prof. A. Shamir.
- P. Gober, *Aspekte des unkoordinierten Mehrfachzugriffs*, Universität GH Essen, Germany, December 21, 1999. Supervisor: Prof.dr. A.J. Vinck.
- C. Haslach, *Array Codes auf der Basis interleavter Blockcodes*, University of Essen, Germany, November 1999. Supervisor: Prof.dr. A.J. Vinck.
- P.W. Heijnen, *Some classes of linear codes observations about their structure, construction, (non)existence, decoding*, TU Eindhoven, August 27, 1999. Supervisors: prof.dr.ir. H.C.A. van Tilborg, prof.dr. J. Simonis and dr. G. R. Pellikaan.
- S.R. Tiourine, *Decision Support by Combinatorial Optimization: case studies*, TU Eindhoven, September 21, 1999. Supervisors: A.M.H. Gerards and J.K. Lenstra.
- C. Wyants, *Network Synthesis Problems*, Université Libre de Bruxelles, Belgium, June 1, 1999. Supervisor: M. Labbé.
- K. Zahidi, *Existential indecidability for rings of algebraic functions*, Universiteit Gent, Belgium, October 28, 1999. Supervisor: prof.dr. J. Van Geel.

7.3 Ph.D. Committees

- A.E. Brouwer
  - R.J Blok, TU Delft, May 18, 1999.
- A.M. Cohen
  - R.J. Blok, TU Delft, May 18, 1999.
  - J. Vogels, TU Eindhoven, June 29, 1999.
  - P.W. Heijnen, TU Eindhoven, August 27, 1999.
  - A. de Boo, Universiteit Utrecht, November 29, 1999.
  - F. van Abeelen, TU Eindhoven, December 16, 1999.
- J. Van Geel
  - K. Zahidi, Universiteit Gent, October 28, 1999.
- A.M.H. Gerards

- S.R. Tiourine, TU Eindhoven, September 21, 1999.

- J.K. Lenstra
  - W.H.M. Raaymakers, TU Eindhoven, September 10, 1999.
  - J.P. Warners, TU Eindhoven, September 14, 1999.
  - A.M.C.A. de Koster, Maastricht University, November 4, 1999.
  - E. de Kock, TU Eindhoven, December 15, 1999.
  - S.R. Tiourine, TU Eindhoven, September 21, 1999.
- J.H. van Lint
  - Van der Veerdonk, March 3, 1999.
  - Reniers, June 7, 1999.
  - S. Wiegeraad, September 30, 1999.
  - P.J. Slikkerveer, October 27, 1999.
- H. Van Maldeghem
  - R. Blok, TU Delft, May 18, 1999.
  - D. Van Heule, Universiteit Gent, September 8, 1999.
- G.R. Pellikaan
  - P.W. Heijnen, TU Eindhoven, August 27, 1999.
  - M. Boguslavsky, Universiteit van Amsterdam, June 23, 1999.
- B. Preneel
  - H. Handschuh, ENST, Paris, France, September 24, 1999.
- L.A.M. Schoenmakers
  - S.A. Brands, TU Eindhoven, October 4, 1999.
- J. Simonis
  - P.W. Heijnen, TU Eindhoven, August 27, 1999.
- T.H.M. Smits
  - R.J Blok, TU Delft, May 18, 1999.
- J.A. Thas
  - K. Zahidi, Universiteit Gent, October 28, 1999
- H.C.A. van Tilborg
  - S.A. Brands, TU Eindhoven, October 1, 1999.
  - P.W. Heijnen, TU Eindhoven, August 27, 1999.
  - B.-J. Koops, KU Brabant, January 6, 1999.
  - B. Zwaneveld, Open Universiteit, June 4, 1999.
  - M. Shoae Bargh, TU Eindhoven, September 28, 1999.
  - P. Gober, Universität GH Essen, Germany, December 21, 1999.
- A.J. Vinck
  - C. Haslach, University of Essen, Germany, November 1999.
  - P. Gober, University of Essen, Germany, December 21, 1999.

  - C. Freek, University of Essen, April 8, 1999.
  - P. Heijnen, TU Eindhoven, August 28, 1999.
  - L. Selander, University of Lund, Sweden, December 10, 1999.

- F.M.J. Willems
  - Jossy Sayir, ETH Zürich, March 29, 1999.
  - Gabriele Buch, TU München, August 20, 1999.
  - M. Shoae Bargh, September 28, 1999.

7.4 Editorship

- A.E. Brouwer
  - Editor Algebraic Journal of Combinatorics.
  - Editor European Journal of Combinatorics.
- F. Buekenhout
  - Editor Journal of Combinatorial Theory (A).
  - Editor Journal Européen de Combinatoire,
  - Editor Atti del Seminario di Matematico e Fisico de'll Universitá di Modena.
  - Editor Contributions to Algebra and Geometry
  - Editor Journal of Group Theory.
- H. Broersma
  - Associate editor Discussiones Mathematica - Graph Theory.
  - Associate editor Networks.
  - Member editorial board Graphs and Combinatorics.
  - Contributing editor International Abstracts of Operations Research.
  - Guest editor Discrete Applied Mathematics.
- A.M. Cohen
  - Editor Geometriae Dedicata.
  - Editor Discrete Mathematics and Computer Science (electronic).
  - Editor Mathematics op Computation.
  - Editor Journal of Symbolic Computation.
- J.-P. Doignon
  - Member board of editors Journal of Mathematical Psychology.
  - Member "Comité de Rédaction" of Mathématiques, Informatique et Sciences Humaines (Paris).
- J. Doyen
  - Editor Journal of Combinatorial Designs.
  - Editor Bulletin of the Belgian Mathematical Society - Simon Stevin.
- J. Van Geel
  - Editor Bulletin of the Belgian Mathematical Society - Simon Stevin.
- A.M.H. Gerards
  - Editor CWI Tracts, CWI Syllabi.

- Editor Discrete Mathematics and Theorectical Computer Science.
- Associate editor Mathematical Programming, Series A.
- Editor SIAM Journal on Discrete Mathematics.

- K.A.S. Immink
  - Editor SMPTE Journal.
  - Associate editor IEEE Communications Magazine.
  - Member review board Journal of the Audio Engineering Society.
- M. Labbé
  - Associate editor Location Science.
  - Associate editor Operations Research.
  - Associate editor Operations Research Letters.
  - Associate editor Rivista di Informatica.
  - Associate editor Transportation Science.
- J.K. Lenstra
  - Member advisory board, ACM Journal of Experimental Algorithmics.
  - Member editorial board CWI Monographs, CWI Tracts, CWI Syllabi.
  - Member advisory board, Excerpta Informatica.
  - Editor Handbooks in Operations Research and Management Science, North-Holland.
  - Area editor for Design & Analysis of Algorithms, INFORMS Journal on Computing.
  - Associate editor, International Journal of Foundations of Computer Science.
  - Member editorial board, Journal of Scheduling.
  - Member editorial advisory board, Kluwer Series in Operations Research/Computer Science Interface.
  - Advisory editor Mathematics of Operations Research.
  - Member advisory board MPS-SIAM Series in Optimization.
  - Area editor for optimization, Operations Research Letters.
  - Member advisory board SCIMA Special Series.
  - Advisory editor Wiley/Interscience Series in Discrete Mathematics and Optimization.
- J.-P. Linnartz
  - Editor-in-Chief "Wireless Communication, the Interactive Multimedia CDROM", Baltzer Science Publishers.
- J.H. van Lint
  - Editor Designs, Codes and Cryptography.
  - Editor Discrete Mathematics.
  - Editor Geometriae Dedicata.
  - Editor Journal of Combinatorial Theory (A).
  - Editor Zentralblatt für Mathematik und Ihre Grenzgebiete.
  - Member editorial board Matrix (TU Eindhoven) (till September 1, 1999).
- G.R. Pellikaan
  - Editor Discrete Mathematics.
  - Editor Finite Fields and Their Applications.

  - Editor IEEE Transactions on Information Theory.
  - Editor Journal of Algebra.
  - Editor Journal of Symbolic Computation.
  - Editor Utilitas Mathematica.

- B. Preneel
  - Member editorial board Journal of Cryptology.
  - Member editorial board Cryptologia.
  - Member advisory board Computer & Communications Security Reviews.

- A. Schrijver
  - Editor-in-chief Combinatorica.
  - Editor Discrete Applied Mathematics.
  - Advisory editor Journal of Combinatorial Optimization.
  - Editor Journal of Combinatorial Theory, Series B.
  - Editor Journal of Combinatorics, Information and System Sciences.
  - Associate editor Mathematics of Operations Research.
  - Advisory editor North-Holland Mahtematical Library.
  - Member editorial board SIAM Monographs on Discrete Mathematics and Applications.
  - Editor SIAM Journal on Discrete Mathematics.

- L. Stougie
  - Associate editor Statistica Neerlandica.

- H.C.A. van Tilborg
  - Associate editor Designs, Codes and Cryptography.
  - Associate editor Journal of Combinatorics, Information and System Sciences.

- J.A. Thas
  - Editor Bulletin of the Belgian Mathematical Society – Simon Stevin.
  - Editor Atti Seminario Matematica e Fisico dell'Università di Modena.
  - Editor Journal of Algebraic Combinatorics.

- Tj.J. Tjalkens
  - Editor Newsletter of the WIC.

- V.T. Tran
  - Associate editor Journal of Discrete Mathematical Sciences and Cryptography.

- J. Vandewalle
  - Member of the Editorial board of the International Journal of Circuit Theory and its Applications (1985 - present).
  - Associate Editor of the Journal of Circuits, Systems and Computers (1991-present).
  - Associate Editor of Neurocomputing (1994 - present).
  - Associate Editor of Neural Networks (1998 - present).

7.5 Organisation of workshops and conferences

- E.H.L. Aarts
  - With W.F.J. Verhaegh and J.H.M. Korst: Organization Philips Workshop on Scheduling and Resource Management (SCHARM), Eindhoven, December 1999.
- F. Buekenhout
  - Co-organization of seminar University Gent-University Bruxelles on Finite Geometry and Buildings (4 meetings).
  - Organizer of a "Collège de France" course of 8 hours by Jacques Tits on "Le plan de Cremona", Université libre de Bruxelles, March 1999.
- H.J. Broersma
  - Organizer (with C. Hoede) of the 6th Twente Workshop on Graphs and Combinatorial Optimization, Universiteit Twente, May 26-28, 1999.
- Ph. Cara
  - Co-organizer (with F. Bingen and H. Van Maldeghem) of a Seminar on Permutation Groups, Vrije Universiteit Brussel and Universiteit Gent. There were 17 lectures.
- F. De Clerck
  - Co-organizer of the interuniversity seminar "Finite Geometry and Buildings" (organized by the University of Gent and the ULB).
- A.M. Cohen
  - Organizer OpenMath Workshop, Eindhoven, May 22-23, 1999.
  - Member MEGA 2000 advisory programme committee. item Chairman/coordinator poster session ISSAC2000 at St. Andrews.
  - Member program committee RWCA 2000 at Zürich (Rhine Workshops in Computer Algebra).
- G. Cornelissen
  - Co-organizer of the Workshop: Hilbert's 10th Problem, Relations with Arithmetic and Algebraic Geometry, Gent, Belgium, November 2-5, 1999.
- M. Dehon
  - Co-organization of seminar University Gent-University Bruxelles on Finite Geometry and Buildings (4 meetings).
- A. Delandtsheer
  - Co-organiser of the interuniversity seminar "Finite Geometry and Buildings" (organised by the University of Ghent and the ULB).
- J. Doyen
  - Co-organization of seminar University Gent-University Bruxelles on Finite Geometry and Buildings (4 meetings).
- B. Fortz
  - Member of the scientific committee of Orbel 13, Brussel, Belgium.
- J. van Geel
  - Co-organizer Workshop: Hilbert's 10th Problem, Relations with Arithmetic and Algebraic Geometry, Gent, Belgium, November 2-5, 1999.

- A.M.H. Gerards
  - Member organizing committee, Twenty-Fourth Conference on the Mathematics of Operations Research, Lunteren, The Netherlands, January 12-15, 1999.
- W.H. Haemers
  - Co-organization Conference 'Geometric and Algebraic Combinatorics' (On the occasion of J.J. Seidel's 80th birthday), Oisterwijk, August 15-20, 1999.
- C. Hoede
  - Organizer (with H.J. Broersma) of the 6th Twente Workshop on Graphs and Combinatorial Optimization, Universiteit Twente, May 26-28, 1999.
- J.H.M. Korst
  - With W.F.J. Verhaegh and E.H.L. Aarts: Organization Philips Workshop on Scheduling and Resource Management (SCHARM), Eindhoven, December 1999.
- M. Labbé
  - Member of the scientific committee of IFORS conference, Beijing, China.
- J.K. Lenstra
  - Member programming committee, 7th European Symposium on Algorithms, Praag, Czech Republic, June 9-11, 1999.
  - Chair program and organizing, 4th Workshop on Models and Algorithms for Planning and Scheduling Problems, Renesse, The Netherlands, June 14-18, 1999.
- J.-P. Linnartz
  - Member of the technical program committee of EPMCC 99, Paris, France, March 1999.
  - Member of the program committee of the Workshop on Information Hiding, Dresden, September 29 - Oct. 1, 1999.
  - Member of the technical program committee of Wireless 99, Bonn, Germany, September 1999.
- J.H. van Lint
  - Member scientific committee ECM 2000 (Barcelona), April 9-11, 1999.
- H. Van Maldeghem
  - Organizer of the international conference (Moufang) Polygons and (Twin) Buildings, Gent, June 21-25, 1999.
  - Co-organiser of the interuniversity seminar "Finite Geometry and Buildings" (organized by the University of Gent and the ULB).
- B. Preneel
  - Co-organization of 1999 International course on State of the art and evolution of computer security and industrial cryptography, Leuven, Belgium, June 1-4, 1999.
  - Co-organization of BIRA/KVIV studiedag 'Computer- en Internetbeveiliging', December 2, 1999.
  - Program chair of CMS'99: IFIP Workshop, Communications and Multimedia Security, 1999.
  - Member program committee Workshop on Fast Software Encryption'99.
  - Member program committee Crypto'99: Workshop on the Theory and Applications of Cryptographic Techniques.

- Member program committee ISSE'99: Information Security Solutions.
- Member program committee ICISC'99: International Conference on Information Security and Cryptology.

- L.A.M. Schoenmakers
  - Member program committee Financial Cryptography 1999, Anguilla, February 22-25, 1999.
- A. Schrijver
  - Member organizing committee, Workshop on Polyhedral and Semidefinite Programming Methods, The Fields Institute for Research in Mathematical Sciences, Toronto, Canada, November 1-6, 1999.
- L. Storme
  - Co-organizer of the interuniversity seminar "Finite Geometry and Buildings" (organized by the University of Gent and the ULB).
- M. Struik
  - Vice-chair of the technical program committee of the (IFIP) 7th Annual Working Conference on Information Security Management & Small Systems Security, Amsterdam, September 30, 1999.
- J.A. Thas
  - Co-organizer of the interuniversity seminar "Finite Geometry and Buildings" (organized by the University of Gent and the ULB).
- H.C.A. van Tilborg
  - Member program committee Workshop on Coding and Cryptography, Paris, France, January 11-14, 1999.
  - Organizer of a special session on "Cryptology, Algorithms and Mathematics", 1999 Information Theory Workshop, Berg en Dal, South Africa, June 2-25, 1999.
  - Organizer of a special session on "Cryptology and Network Security", 1999 Information Theory and Networking Workshop, Metsovo, Greece, June 27-July 1, 1999.
  - Organizer and member program committee EIDMA Lustrum Congress, Congrescentrum Carlton De Brug, Mierlo, October 7-8, 1999.
  - Organizer EIDMA Seminar Coding, Crypto & Information Theory.
  - Organizer EIDMA Cryptography Working Group.
- M. Vandenwauver
  - Member program committee IEEE WETICE'99: International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises.
- J. Vandewalle
  - Co-organization of 1999 State of the art and evolution of computer security and industrial cryptography, Leuven, Belgium, June 1-4, 1999.
- W.F.J. Verhaegh
  - With J.H.M. Korst en E.H.L. Aarts: Organization Philips Workshop on Scheduling and Resource Management (SCHARM), Eindhoven, December 1999.
- A.J. Vinck
  - Co-organizer of Future Directions in Information and Communication Theory, Final Conference of the CINEMA Graduate College, September 16 and 17, 1999.

- Co-organizer Multi-Media, Lecture Series, April - June 1999.

- F.M.J. Willems
  - Member of the program committee of the IEEE International Symposium on Information Theory, Sorrento, Italy.
  - Session organizer at the IEEE Information heory and Communications Workshop in Kruger National Park, South Africa.

- K. Zahidi
  - Co-organiser of the Workshop: Hilbert's 10th problem, relations with arithmetic and algebraic geometry, Gent, Belgium, November 2-5, 1999.

7.6 Memberships

- H.J. Broersma
  - Consultant professor of the mathematics department of the Northwestern Polytechnical University of Xian, China.

- A.E. Brouwer
  - Member of the Scientific Council of EIDMA.

- F. Buekenhout
  - Membre correspondant of the Académie Royale de Belgique, Classe des Sciences.
  - Member "Conseil d'Administration" of the CREM (Centre de Recherche sur l'Enseignement des Mathématiques).
  - Member jury Olympiade Mathématique Belge".
  - Member Belgian Mathematical Society.
  - Member American Mathematical Society.
  - Member Deutsche Mathematiker Vereinigung.
  - Member Société Mathématique de France.
  - Member European Mathematical Society.
  - Member Mathematical Association of America.
  - Member National Council of Teachers of Mathematics.
  - Member Société Belge des Professeurs de Mathématique.
  - Member Association des Professeurs de Mathématique de l'Enseignement Public.
  - Member Institute of Combinatorics and Applications.
  - Member Altaïr(History of Science).
  - Member Discreet Nederland.
  - Member of the Scientific Council of EIDMA.

- Ph. Cara
  - Member Belgian Mathematical Society.
  - Member European Mathematical Society.
  - Member Discreet Nederland.

- C. Cerf
  - Member Society for Mathematical Biology.
  - Member International Society for Mathematical Chemistry.
  - Member Belgian Mathematical Society.

- Member European Mathematical Society.
- Member Discreet Nederland.

- A.M. Cohen
  - Scientific director RIACA.
  - Chairman of the board of EIDMA.
  - President OpenMath Society.
  - Member OpenMath ESPRIT Council.
  - Member scientific advisory council Mathematical Research Institute (MRI), Nijmegen.
  - Coordinator applied mathematics department of CLUSTER.
  - Member search committee professorships at Grenoble.
  - Member STW jurykamer.
- M. Dehon
  - Member Belgian Mathematical Society.
  - Member Discreet Nederland.
- A. Devillers
  - Member Belgian Mathematical Society.
  - Member Discreet Nederland
- J.-P. Doignon
  - Chairman of the department of mathematics, Université Libre de Bruxelles.
- J. Doyen
  - Member scientific commitee of the Troisiéme Université Européenne d'Été d'Histoire des Mathématiques held in Louvain-la-Neuve and Leuven (Belgium) in July 1999.
  - Founding member Altaïr (History of Sciences) and co-organiser of conferences.
  - Member Comité National de Logique et d'Histoire des Sciences (Belgium).
  - Member Belgian Mathematical Society.
  - Member American Mathematical Society.
  - Member Mathematical Association of America.
  - Member Institute of Combinatorics and Applications.
  - Member Discreet Nederland.
- A.M.H. Gerards
  - Member KNAW Akademie Raad voor de Wiskunde - Commissie Toekomst Wiskunde Onderzoek in Nederland.
  - Member Landelijk Netwerk Mathematische Besliskunde.
- E. Govaert
  - Member Belgian Mathematical Society.
- C. Hoede
  - Consultant professor of the mathematics department of the Northwestern Polytechnical University of Xian, China.
  - Board member EIDMA.
- C. Huybrechts

- Member Belgian Mathematical Society.
- Member Discreet Nederland.

- K.A.S. Immink
  - Director Turing Machines Inc., Geldrop.
  - Adjunct professor Institute for Experimental Mathematics, University of Essen, Essen, Germany.
  - Member Royal Netherlands Academy of Arts and Sciences (KNAW).
  - Member IEEE Fellow Committee.
  - Member AdCom Committee IEEE Consumer Electronics Society.
  - Vice-president Audio Engineering Society.
  - Chairman IEEE Benelux Chapter on Consumer Electronics.
  - Chairman IEEE Masaru Ibuka Consumer Electronics Award Committee.
  - Trustee Shannon Foundation.
- D. Leemans
  - Member Belgian Mathematical Society.
  - Member Discreet Nederland.
- J.K. Lenstra
  - Member Management Team BETA, Research Institute for Business Engineering and Technology Applications.
  - Director Institute for Operations Research and the Management Sciences.
  - Chair Review and Search Committee INFORMS Journal on Computing.
  - Board member KNAW Akademie Raad voor de Wiskunde.
  - Member Programme Committee STW-SWON Programma Wiskunde Toegepast.
  - Chair Wiskundig Genootschap.
  - Member Adviescommissie Wiskunde, NWO, Gebiedsbestuur Exacte Wetenschappen.
  - Member jury SIAM Activity Group on Optimization Prize, Society for Industrial and Applied Mathematics.
  - Member Science Council SOM, Onderzoekschool voor Systemen, Organisatie en Management (Groningen University).
  - Chair nomination committee Mathematical Programming Society.
  - Member Landelijk Netwerk Mathematische Besliskunde.
  - Member of the Scientific Council of EIDMA.
- J.-P. Linnartz
  - Senior member IEEE.
  - Member NERG.
- J.H. van Lint
  - Director Stan Ackermans Institute, TU Eindhoven (till September 1, 1999).
  - Advisor Natuurkundig Laboratorium (Philips Electronics).
  - Member of the board of STW.
  - Chairman Platform Medische Technologie (till November 22, 1999).
  - Member sectie wiskunde KNAW.
  - Advisor Stichting Steunfonds Eindhovense Studentensport (till October 22, 1999).

- Chairman project Geschiedenis van het Eindhovense Studentenleven.

- H. Van Maldeghem
  - Member Belgian Mathematical Society.
  - Member Diskreet Nederland.
  - Member European Mathematical Society.
  - Member Institute of Combinatorics and its Applications (Canada).
- G.R. Pellikaan
  - Coordinator student exchange program in the Galois Network under the terms of ERASMUS/SOCRATES of the European Union.
- B. Preneel,
  - Director of the IACR, the International Association for Cryptologic Research.
  - Belgian expert in ISO/IEC JTC1/SC27 on Security Techniques.
- M. Sebille
  - Member Discreet Nederland.
- J. Simonis
  - Board member EIDMA.
- A. Schrijver
  - Board member EIDMA.
  - Member KNAW Akademie Raad voor de Wiskunde.
  - Member Koninklijke Nederlandse Akademie van Wetenschappen.
  - Member governing board Landelijk Netwerk Mathematische Besliskunde.
  - Member Symposium advisory committee, Mathematical Programming Society.
  - Member Science council Stieltjes Instituut voor Wiskunde.
  - Board member EIDMA.
- G. Sierksma
  - Member of the Scientific Council of EIDMA.
- L. Storme
  - Member Belgian Mathematical society.
  - Member European Mathematical society.
  - Member American Mathematical society.
  - Member Institute for Combinatorics and Its Applications.
- J.A. Thas
  - Member Royal Academy of Sciences, Letters and Fine Arts of Belgium (director in 1999).
  - Secretary National Committee for Mathematics.
  - Member of the Scientific Council of EIDMA.
- H.C.A. van Tilborg
  - Scientific director EIDMA.
- Tj.J. Tjalkens

- Member of the board (Benelux) Werkgemeenschap voor Informatie- en Communicatietheorie (WIC).

- L. Tolhuizen
  - Senior member IEEE.
  - Secretary "Werkgemeenschap voor Informatie en Communicatie theorie in de Benelux".

- J. Vandewalle
  - director of the IACR, the International Association for Cryptologic Research.
  - Member of the Scientific Council of EIDMA.
  - Member International Neural Network Society since 1987.
  - Fellow of IEEE the Institute of Electrical and Electronics Engineers.
  - Member of the Koninklijke Academie voor Wetenschappen, Letteren en Schone Kunsten van België (October 1996 - present).
  - Member Academia Europaea in 1999.

- A.J. Vinck
  - Member board of governors of the IEEE Information Theory Group, 1997-2000.
  - Chairman ADV (Data Processing) commission of the University of Essen.
  - Chairman Information Theory Association of the Benelux Countries.
  - Member of the Scientific Council of EIDMA.
  - Director Institute of Experimental Mathematics, 1998-2000.

- F.M.J. Willems
  - Member board of governors IEEE Information Theory Society.
  - Member technical program committee of the IEEE 2000 International Symposium on Information Theory, Sorrento, Italy.
  - Advisor Philips Research Laboratories.
  - Board member EIDMA.