

DIAMANT

Discrete, interactive & algorithmic mathematics, algebra & number theory

A. Cluster title

DIAMANT: Discrete, interactive & algorithmic mathematics, algebra & number theory.

Contact: Prof. dr. A.M. Cohen, Faculteit Wiskunde en Informatica, TUE, Postbus 513, 5600 MB Eindhoven;

email amc@win.tue.nl, tel. 040-2474270 (office), 030-6921115 (home), fax 040-2435810.

B. Summary

Twentieth-century mathematics focused primarily on the *existence* of mathematical objects. Will the trend towards *constructing* them lead to a change of emphasis in the new century? With the continuing explosion in computer technology, striking applications have been discovered for several of the traditionally purest parts of mathematics. Modern computer security depends crucially on number theory and algebra, and one cannot imagine operations research without discrete mathematics or program verification without logic. Dutch scholars, both in the Netherlands and abroad, have made remarkable contributions to all of these subjects.

The DIAMANT initiative is built around the algorithmic approach in algebra, discrete mathematics, logic, and number theory. The theme is interpreted broadly, with special attention given to subjects on the interface with neighboring disciplines. DIAMANT concentrates on high-level original research, drawing its techniques largely from fundamental mathematics. Research of this nature has yielded many applications in recent years and has the potential to create important new ones. The principal application area is *networks*, especially optimization and security. In addition to the fundamental study of algorithms and their correctness, the actual design and development of usable software systems form part of the DIAMANT research effort.

DIAMANT is a well-integrated collaborative structure based at four mathematical institutes. It brings coherence to its area of research, fostering interaction between the participating groups, realizing new educational opportunities, and maintaining active links with society. By creating a critical mass of internationally recognized experts, DIAMANT will strengthen and secure the position of the Netherlands in algorithmic research for many years to come.

1. Research plan

Key scientific questions and long-term research goals. The branches of learning represented in DIAMANT have their origins in pure mathematics. Numerous developments since World War II have shown that it is exactly their sophistication that is crucial to their great relevance to modern society. The DIAMANT research plan fully recognizes that differentiating between pure and applied mathematics is not a fruitful attitude, and that present-day applications draw upon the full spectrum of mathematics.

DIAMANT research covers all problems that, regardless of the possible application, (a) have mathematical interest, (b) involve algorithmic thinking, and (c) belong to the branches of mathematics that are ‘discrete’ in the sense of not being primarily concerned with continuously varying quantities. These common properties result in strong, intrinsic connections between the research problems considered, and DIAMANT makes these connections both visible and productive.

Applications drive much of DIAMANT. Not only do they inspire many problems for which DIAMANT offers solutions, but also does today’s DIAMANT research address tomorrow’s applications.

The following list of sample questions and research problems is representative of the ambitions of DIAMANT. The list is emphatically not exclusive, and other problems within the scope of DIAMANT will be considered as well. It is obviously vital for DIAMANT immediately to pursue new and unexpected developments, and to trigger such developments in the first place.

- (i) Investigate lattice algorithms. The LLL algorithm, introduced in 1982, is of importance to virtually all areas covered by DIAMANT, especially algorithmic number theory, computer algebra, and integer programming. Many complexity issues related to lattice algorithms remain unresolved. This topic takes on added urgency with the advent of lattice-based cryptosystems and the development of lattice methods as a competitive tool for solving certain classes of integer programming problems.
- (ii) How hard is integer factorization, and how secure are elliptic curve based cryptosystems? It may not be realistic to expect great progress on these famous and difficult problems, but cryptologists always have them in the back of their minds, and use them as a test for any new idea that emerges. The recent breakthrough in primality testing confirms that one should always be prepared for the unexpected.
- (iii) Develop algorithms for solving diophantine equations or, in modern parlance, for finding all rational points on algebraic varieties. Problems of this nature are as old as number theory itself, and many significant classes of varieties have been dealt with successfully.

The relatively recent insight that techniques of algebraic geometry apply, has given rise to a great increase of activity in the area. The known unsolvability of the problem in full generality indicates that the formulation of proper conjectures already poses a challenge.

- (iv) Design new point counting techniques for varieties over finite fields. This subject, of well-known importance in coding and cryptology, originated with Schoof's algorithm in 1985 and it is currently going through a transformation. Very recently, the existing p -adic method was extended by the use of differential equations on p -adic cohomology. A new l -adic method that uses Arakelov theory will also make the Langlands correspondence computable in certain cases.
- (v) Analyze security systems logically and quantitatively. Cryptology provides the tools for building secure systems. Evaluating and certifying such systems becomes increasingly important, and needs to take the computing infrastructure into account. Mathematical techniques play an important role in this growing area, both for the logical analysis of the protocols and for the quantitative analysis of the various risk factors. Results can be used for mathematical advice to the financial industry on the minimal mandatory compliance with the recently adopted Basel 2 international banking regulations.
- (vi) Locate the borderline between hard and easy problems in combinatorial optimization. This is an ongoing quest, directly related to the notorious $P \neq NP$ -conjecture. Subject to this conjecture, the classification of hard problems has recently been refined, based on the existence or non-existence of polynomial-time approximation algorithms with constant or arbitrarily small relative worst-case error. For example, geometric versions of the famous traveling salesman problem admit the latter type of algorithm, whereas the optimal solution value of the set cover problem cannot be approximated within any fixed constant. For most combinatorial problems a gap remains to be closed between what has actually been achieved and the known limits of what is achievable. This subject is at the interface between complexity theory and operations research.
- (vii) Discrete tomography. The problem of reconstructing objects from X-ray images used to be tackled by continuous techniques. Recently, a discrete approach has proven to be more efficient, needing fewer images to be taken. Can the breakthrough that was achieved by the introduction of network algorithms be extended to other aspects of image analysis? Application areas include medicine, crystallography, and metallurgy.
- (viii) Study properties of polytopes. The primary target is the Hirsch conjecture, which states that the diameter of a polytope is bounded above by the number of facets minus the dimension. However, a bound that is polynomial in these two quantities would already

be a major achievement. A related problem is the existence of a linear programming algorithm whose running time is polynomial in only the number of variables and the number of restrictions. This is a fundamental open problem in high-dimensional geometry, which is central to computational geometry and has direct applications in operations research.

- (ix) Study algorithmic and structural problems in networks and more general structures like matroids. Experiments have shown that most communication and transportation networks have a high degree of decomposability, which breaks up algorithmic, visualizability, and other problems. Parallel to this practically observed phenomenon is a recent breakthrough in graph theory, the graph minors theorem, which states that decomposability and embeddability of a network can be described by finitely many ‘forbidden subnetworks’. The main issue now is to identify such bottlenecks. The research comprises matroid minors, polyhedral and spectral network representations, and knotless visualization of networks in three-dimensional space. Most of the problems are motivated by optimization.
- (x) Investigate the interplay between semi-definite optimization and representations of positive polynomials as sums of squares. Existence results for such representations go back to the nineteenth century. Due to the recent insight that semi-definite programming can be used for their efficient construction, they are once again under active investigation. Applications include the design of efficient approximation algorithms for optimizing a polynomial over a semi-algebraic set, which includes the integer programming problem. This subject is related to the study of approximation algorithms mentioned in (vi).
- (xi) Develop algorithms for the computation of differential Galois groups of linear differential equations. Recent theoretical work shows much promise in this direction. Such algorithms may lead to methods for solving linear differential equations that can be incorporated in mathematical software systems, which are used in applied sciences.
- (xii) Investigate methods for analyzing and constructing algebraic groups and Lie algebras, and implement these in existing computer algebra systems. Related questions concern algorithms for non-commutative algebra and for representations of Lie algebras and quantum groups. An algorithm was recently found for computing the algebraic group generated by a given finite set of matrices over a field; can this algorithm be made practically feasible? Results of this nature have a bearing on quantum computing and the algebraic analysis of linear differential equations mentioned above.
- (xiii) Build a system allowing interaction between computer algebra and proof checking. For example, an automatic construction method for formal (i.e., computer checkable)

primality proofs is already available, and it should be feasible to treat the Risch integration algorithm and the graph isomorphism problem in a similar manner. This subject has the potential of drawing together all groups participating in DIAMANT, since it requires expertise in differential equations, number theory, computer algebra, graph theory, and logic. It will lead to a new, interactive form of mathematics.

- (xiv) Study quantum computing in relation to discrete-mathematical problems. The natural challenge is finding quantum algorithms for problems that classically do not admit satisfactory solutions, such as the graph isomorphism problem or the problems on which the security of sophisticated cryptosystems depends. Research problems of a different type are suggested by the surprising discovery that the mere axioms of quantum computing have valuable implications in combinatorics and classical computer science, whether or not the concept of a quantum computer can be physically realized. An exponential lower bound on the length of certain locally decodable error correcting codes was recently established by a combination of quantum information theory and a classical-to-quantum reduction. Similar techniques gave new bounds for the cryptographic task of private information retrieval. Many more results along these lines are expected.

Research methods and innovativeness. The main scientific instrument of the DIAMANT cluster is front-line original research in mathematics. Top priority will be given to enhancing the research team and broadening the range of expertise represented in DIAMANT. Top Dutch and foreign mathematicians who are active abroad will be attracted to the Netherlands, either on a temporary basis or permanently.

The main organizational instrument is sustained structured interaction between the participating groups. DIAMANT strives to build coherence and strength in algorithmic ‘discrete’ mathematics in the Netherlands. The first step in this direction is intensifying and expanding existing modes of interaction, including intercity seminars, workshops, and mini-courses; these bring together researchers from different fields and combine knowledge transfer, instruction, and research. New activities will be started, such as master classes, special years, and interdisciplinary meetings.

DIAMANT will pay special attention to its relationship with society at large and it will publicize its activities widely. To this end, DIAMANT will introduce a national colloquium addressing a broad audience, maintain an attractive and informative website, and actively promote the popularization of mathematics. As part of its effort to strengthen interaction with industry, non-profit organizations, and neighboring disciplines, DIAMANT will create a national forum for the exchange of expertise and relevant problems.

Coherence. DIAMANT is based at four sites: the Centrum voor Wiskunde en Informatica (CWI) in Amsterdam, the Radboud Universiteit (RU) in Nijmegen, the Technische Universiteit Eindhoven (TUE), and the Universiteit Leiden (UL). In addition, there are a number of participants from the Universiteit Utrecht (UU) and the Rijksuniversiteit Groningen (RUG) whose involvement is important to the operations of the cluster. These members will be administratively allocated to RU, their partner in the research school MRI.

Involvement of sites in problems														
no.	(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	(ix)	(x)	(xi)	(xii)	(xiii)	(xiv)
CWI	●	●			○	●	●	●	●	●			○	●
RU	●	●	●	●	●						●	○	●	●
TUE	●	●	○	●	●	●		●	●	○	○	●	●	○
UL	●	●	●	●	○		●			○	○		○	○

The table above illustrates the coherence of DIAMANT using the sample problems (i)–(xiv) listed before. A leading role of a site in a problem area is indicated by ●, and ○ means that the site is expected to contribute. The table suggests that closer and more systematic cooperation, as envisaged by the cluster, has great potential benefits, both mathematically and from an applied point of view.

Combining existing small scale activities into strong joint efforts. In several fields covered by DIAMANT biweekly intercity seminars will be organized. The scheduling will maximize the opportunities for all members to participate. Experience shows that rotating the location of the seminar among the sites maximizes the impact, the number of regularly attending participants, and the attractiveness of the seminar for students and junior researchers. Typically, a seminar lasts a full day, and it provides ample possibilities for interaction, both formal and informal.

In addition, DIAMANT will organize semi-annual or annual cluster-wide research meetings of broader scope. These will enhance the coherence of the DIAMANT research efforts and facilitate the sharing of recent achievements and new targets. In addition, these meetings will serve as a platform for invited foreign experts whose input is likely to stimulate DIAMANT research, and as a means to monitor the impact of DIAMANT research in the presence of industrial contacts.

DIAMANT will run semester-long programs devoted to special topics. During such semesters, it will invite visits from leading researchers in the area concerned and, if appropriate, from neighboring disciplines.

Proposed research in relation to NWO and OOW themes. Existing and potential applications range over many fields, including information technology and security, chip design,

network traffic and design, logistics, electronic commerce and publishing, statistics, data analysis and data mining, and molecular biology. Of the NWO and OOW themes, the one most prominently served by DIAMANT is *mathematics and networks*. The optimization and security aspects of this theme are particularly central to DIAMANT.

The TUE, where coding theory has strong roots, is the only Dutch university with an active mathematical research group in cryptology. Recently, RU built an active group in cryptology within their computer science department, where the appointment of a part-time professor in mathematics for information security is foreseen. More recently, the importance of cryptology was underlined by the joint appointment of a top researcher at CWI and UL. As part of the DIAMANT effort, TUE intends to attract a prominent cryptologist and CWI and UL will each establish an additional position in cryptology.

Researchers at CWI and TUE are renowned for their algorithmic work in combinatorial optimization, quantum computing, and computational geometry. A leading expert in approximation algorithms has recently been appointed to a TUE chair. Also, at TUE, a part-time professorship in network algorithms is being prepared. CWI guarantees continuation of a DIAMANT position in algorithmic game theory, an area that has network design as its principal application.

Relation to research done elsewhere and the position of the Netherlands. The Netherlands occupies a strong international position in the areas covered by the DIAMANT cluster. Dutch researchers in the Netherlands and abroad have made fundamental contributions to these areas, and several members of the research team have gained high recognition, both nationally and internationally.

All the groups belonging to DIAMANT cooperate closely with other leading research groups around the world. DIAMANT members participate in several European collaborative networks, make frequent visits to research centers elsewhere, and serve on the scientific committees of the authoritative meetings in their fields. The algorithms they design are implemented in widely used packages and systems, and their former students occupy positions in research institutions and universities on all continents.

One of the goals of DIAMANT is to strengthen the role that Dutch research institutions play in the international arena. The national impact of Dutch research in this field should be commensurate with its international importance, and the Netherlands should become a prime location for performing algorithmic research in ‘discrete’ mathematics.

2. Quality of the research team

The scientific board of DIAMANT consists of:

Prof. dr. H. Barendregt	computer mathematics	RU
Prof. dr. A.M. Cohen	algebra, discrete mathematics	TUE
Prof. dr. H.W. Lenstra	number theory, algebra	UL
Prof. dr. A. Schrijver	discrete mathematics and optimization	CWI & UvA

The scientific board provides leadership at all levels of the DIAMANT initiative. Its members are personally committed to active involvement in all DIAMANT research efforts. Their particular responsibility is recognizing and exploiting opportunities for interaction between different areas or participating groups.

Prof. dr. H. Barendregt (RU)

Barendregt studied mathematics at Utrecht, where he obtained his Ph.D. degree in 1971. He remained at Utrecht until 1986, working first in philosophy and then in mathematics. He was appointed full professor at Nijmegen in 1986, where he presently occupies the Chair of Foundations of Mathematics and Computer Science. He was visiting professor at the ETH Zürich, Kyoto, Wollongong (Australia), and the École Normale Supérieure in Paris. From 1999 until 2005 he will be an adjunct professor at Carnegie Mellon (Pittsburgh, USA). In 1992, 1996, and 1997 he was elected to the Academia Europaea, the Koninklijke Nederlandse Maatschappij der Wetenschappen, and the Koninklijke Nederlandse Akademie van Wetenschappen. In 1998, his home university awarded him a seven year personal grant, and in 2002 he received the NWO Spinoza award. Barendregt is known for his work in lambda calculus and type theory. His monograph on untyped lambda calculus has been translated into Russian and Chinese. Twenty-eight students have obtained their Ph.D. degree under his supervision. He published 59 items, including the monograph just mentioned and four handbook chapters. In addition, he has published several popular articles, as well as three papers and a review on the theory of mind.

Prof. dr. A.M. Cohen (TUE)

Cohen studied mathematics and theoretical computer science at Utrecht, where he obtained his Ph.D. degree in 1975. He worked at the Openbaar Lichaam Rijnmond (Rotterdam), the Technische Universiteit Twente (Enschede), CWI (Amsterdam), and at the Universiteit Utrecht, where he became a full professor in 1990. Since 1992, he has been a full professor of Discrete Mathematics at the Technische Universiteit Eindhoven. He is the scientific director of RIACA, chairman of the board of the research school EIDMA, and president of the OpenMath Society. He occupied visiting positions in Ann Arbor, Ber Sheva, Jerusalem,

Kobe, Naples, Pasadena, Rome, Santa Cruz, and Sydney. Cohen's main scientific contributions are in groups and geometries of Lie type, and in algorithms for algebras and their implementations. He is also known for his work on interactive mathematical documents. Nine students have received a Ph.D. under his supervision. Currently, he is on the editorial board of three research journals and the ACM book series of Springer-Verlag. He published 86 papers, coauthored four books, and (co-)edited another eight.

Prof. dr. H.W. Lenstra (UL)

Lenstra obtained his Ph.D. degree at the Universiteit van Amsterdam in 1977, was a full professor in Amsterdam from 1978 until 1986, at the University of California, Berkeley, from 1987 until 2003, and at the Universiteit Leiden since 1998. Lenstra is best known for introducing advanced techniques in the area of number-theoretic algorithms. In 1985 he was awarded the Fulkerson prize by the American Mathematical Society and the Mathematical Programming Society, and in 1998 he was the recipient of an NWO Spinoza award. Since 1984 he has been a member of the Koninklijke Nederlandse Akademie van Wetenschappen, and since 1996 a fellow of the American Academy of Arts and Sciences. In 1990/1991 he held a Distinguished Visiting Professorship in the Institute for Advanced Study (Princeton). He received an honorary doctorate from Besançon in 1995. Thirty students have completed their Ph.D. theses under his supervision. He is on the editorial board of six research journals and one book series, the *Ergebnisse der Mathematik und ihrer Grenzgebiete*. His current list of publications counts 158 items, including three jointly written or edited books.

Prof. dr. A. Schrijver (CWI & UvA)

Schrijver did his Ph.D. research at the Mathematisch Centrum and obtained his degree from the Vrije Universiteit in Amsterdam in 1977. He specializes in discrete mathematics and optimization. From 1983 until 1989 he was a full professor at Tilburg, after which he joined the Centrum voor Wiskunde en Informatica as a researcher, with a part-time professorship at the Universiteit van Amsterdam. He held visiting positions at Oxford, Szeged, Bonn, Bell Communications Research, Rutgers University, Yale University, and Microsoft Research. In 1982 and 2003 he was awarded Fulkerson prizes by the American Mathematical Society and the Mathematical Programming Society, in 1987 a Lanchester prize by the Operations Research Society of America, and in 2003 a Dantzig prize by the Mathematical Programming Society and the Society for Industrial and Applied Mathematics. Since 1995 he has been a member of the Koninklijke Nederlandse Akademie van Wetenschappen, and in 2002 he received an honorary doctorate from the University of Waterloo in Canada. Eight students have completed their Ph.D. theses under his supervision. He is on the editorial board of eight research journals and two book series. He has written 140 articles and four books.

Other team members. Listed below are the other team members who are full professor or associate professor (UHD). Several mathematicians at Utrecht (UU) and Groningen (RUG) are included, as are a number of computer scientists. They all have expertise which is essential to the theme of DIAMANT, and their participation is necessary.

<i>name</i>	<i>area of expertise</i>	<i>affiliation</i>
Prof. dr. K. Aardal	optimisation	CWI & TUE
Prof. dr. M. de Berg	computational geometry	TUE
Prof. dr. F. Beukers	number theory, differential equations	UU
Prof. dr. A. Blokhuis	geometric combinatorics	TUE
Dr. W. Bosma	computer algebra	RU
Prof. dr. A.E. Brouwer	discrete mathematics	TUE
Prof. dr. H. Buhrman	quantum computing	CWI & UvA
Prof. dr. R.J.F. Cramer	cryptology	CWI & UL
Dr. H. Cuypers	groups, geometry	TUE
Prof. dr. S.J. Edixhoven	number theory, algebraic geometry	UL
Prof. dr. ir. A.M.H. Gerards	discrete mathematics	CWI & TUE
Dr. H. Geuvers	computer mathematics	RU
Prof. dr. H. Gluesing-Luerssen	coding, systems theory	RUG
Prof. dr. B. Jacobs	correctness, security	RU
Dr. M. Laurent	combinatorial optimization	CWI
Prof. dr. M. van der Put	geometry, differential equations	RUG
Dr. B. de Smit	number theory	UL
Prof. dr. P. Stevenhagen	number theory	UL
Dr. L. Stougie	combinatorial optimization	TUE & CWI
Prof. dr. R. Tijdeman	number theory	UL
Prof. dr. ir. H.A. van Tilborg	coding, cryptology	TUE
Dr. J. Top	number theory, algebraic geometry	RUG
Prof. dr. ir. P.M.B. Vitányi	algorithms, complexity	CWI & UvA
Prof. dr. G.J. Woeginger	combinatorial optimization	TUE

In addition, about 30 assistant professors (UDs), 10 postdocs, and 40 Ph.D. students (AIOs and OIOs) form part of the team. In several special subject areas, scholars from neighboring disciplines will be involved in the DIAMANT effort. For example, research related to networks can profit from the expertise of the TUE groups led by Prof. dr. E.H.L. Aarts, Prof. dr. J.C.M. Baeten, Prof. dr. ir. O.J. Boxma, Prof. dr. ir. B.M. ter Haar Romeny, Prof. dr. W.T.F. den Hollander, and Prof. dr. A.G. de Kok.

3. Cluster structure

Location of the cluster hub and nodes. DIAMANT comprises sites in Eindhoven, Amsterdam, Nijmegen, and Leiden. The TUE is the *hub* of the cluster, and CWI, RU, and UL constitute the *nodes*.

Organization, management, and coordination of the cluster. The scientific board of DIAMANT provides leadership for the research efforts of the cluster. Together, the board members represent the main research areas of DIAMANT, roughly *computational number theory and cryptology, combinatorial optimization, and computer algebra and computer mathematics*. The borderlines between these areas are ill-defined and run across sites; DIAMANT establishes further integration.

The nodes UL, CWI, and RU bear the respective responsibility for the cluster-wide organization of activities in the three individual areas mentioned, while stimulating interaction among different groups.

The hub is responsible for joint research initiatives of all groups and for coordinating all non-scientific activities, such as public relations, fund raising, and practical assistance to visitors. Generally, it creates conditions favorable for research. Public relations activities include the maintenance of the DIAMANT website, the dissemination of research results, and initiatives aimed at a wide audience.

Strengthening of the local infrastructure of the cluster hub. The hub is committed to providing administrative support and to creating facilities for hosting seminars, workshops, instructional activities, and cluster-wide meetings. Collaboration with EURANDOM in matters of infrastructure is being sought.

Involvement of researchers from other institutes. The members of DIAMANT will participate both in the biweekly, rotating intercity seminars and in the cluster-wide meetings. These are organized to attract a critical mass of attendants, including visitors and guest researchers from neighboring disciplines. Researchers from other institutes interested in the activities will obviously be welcome to participate.

4. Plan for investment of the funds

All amounts in this section are in k€, where k€ 1 = € 1000.

The creation of tenured positions is a key tool for producing the long-lasting effects of DIAMANT funding. Each of the participating institutions has committed itself to the continued funding of a number of tenured DIAMANT appointments. These positions, which are listed below, will strengthen the links between the fundamental DIAMANT research and

the NWO and OOW theme *networks*. Their estimated total annual cost is k€ 445.

Investment of funds in tenured positions		
position	site	amount
full professor in cryptology	TUE	133
researcher in cryptology	CWI	52
researcher in algorithmic network games	CWI	52
UD in cryptology	UL	52
UD in arithmetic geometry	UL	52
UD in computational algebra	RU	52
UD in computer mathematics	RU	52

The hub center TUE commits itself to the establishment of DIAMANT facilities. This involves an investment of k€ 150, which forms a one-time contribution of TUE to DIAMANT.

With the present grant proposal, DIAMANT requests the maximum funding of NWO for a Wiskundecluster, *viz.*, k€ 700 per year for four years. TUE will contribute k€ 120 annually to the DIAMANT funds during the cluster funding period. This increases the annual DIAMANT budget to k€ 820.

Annual budget			
credit		debit	
source	amount	object	amount
NWO	700	tenured positions	445
TUE	120	administrative support	20
		research manager	50
		managing director	25
		part-time network algorithms position at TUE	25
		visiting researchers	130
		public relations	15
		meetings	60
		instructional activities	50
total	820	total	820

The table above contains both the credit side and the debit side of the annual budget. It includes, in addition to the reservation of k€ 445 for tenured positions mentioned above, a budget for administrative and organizational support. An amount of k€ 20 of the annual TUE contribution is earmarked for administrative support by the Department of Mathematics and Computer Science. One of the full professors at TUE will assume special responsibility as a managing director for DIAMANT; k€ 25 from TUE's annual contribution is

reserved for this part-time task. An equal amount will be spent on a part-time professorship in network algorithms. The remaining k€ 50 from TUE's annual contribution is intended for instructional activities such as master classes, mini-courses, and summer courses.

The scope of the activities to be developed by DIAMANT necessitates the recruitment of a research manager responsible for daily organization, public relations, and fund raising. This is an appealing position for a young mathematician with the ambition and talent to combine research with management. An annual amount of k€ 50 is reserved for the research manager.

For visiting researchers, DIAMANT allocates k€ 130 per annum, for meetings k€ 60, and for public relations k€ 15.

5. Possibilities for hiring researchers

The conditions for attracting mathematicians who are active abroad are decidedly favorable. DIAMANT expects to benefit from the current trend for European scholars working outside of Europe to reconsider their positions. Special attention will be paid to the possibility of recruiting researchers with a Dutch background.

The list of eligible candidates is long and diverse, containing experts in all fields represented in DIAMANT, both at a junior and at a senior level. An alphabetical and necessarily incomplete listing includes Nils Bruin (Vancouver), Harm Derksen (Ann Arbor), Tim Dokshitzer (Durham), Jan Draisma (Basel), Willem de Graaf (Sydney), Bertrand Guenin (Waterloo, Canada), Mark van Hoeij (Tallahassee), Hein van der Holst (Amsterdam), Rob de Jeu (Durham), Jack Koolen (Korea), Daan Krammer (Warwick), Arjen Lenstra (Lucent), Pieter Moree (Amsterdam), Scott Murray (Sydney), Peter van Rossum (Trento), Jasper Scholten (Leuven), René Schoof (Rome), René Sitters (Saarbrücken), Martijn Stam (Bristol), Arjen Vestjens (CQM, Eindhoven), and Harm Voskuil (ABN-AMRO).

Several researchers on this list have been sounded out, and no difficulties in filling the DIAMANT vacancies are foreseen.

6. Viability

Viability after the first four years. Most of the DIAMANT funding is spent on the creation of tenured positions at the host institutions. This guarantees the long-term viability of the project. After the first four years, DIAMANT will re-evaluate its research priorities and apply for continuation of the cluster support. The institutions hosting DIAMANT have committed themselves to continuing the positions created after expiration of the cluster funding period. Most of the infrastructural facilities and organizational and administrative support provided by TUE will continue after the first four years.

DIAMANT has many sources of additional funding. Its members are currently involved in at least 24 nationally or internationally funded projects, and this number is likely to increase in the future. Several participants perform consultancy for industry, and all prospects for financial involvement of industrial partners in DIAMANT will be pursued.

Impact on the sites. TUE has always championed discrete mathematics in the Netherlands. They host the Euler Institute for Discrete Mathematics and its Applications (EIDMA), which, among the Dutch research schools in mathematics, is unique in being thematically defined. Virtually all DIAMANT research areas are represented at the TUE, in particular coding and cryptology, combinatorial optimization, and discrete algebra and geometry. Several recent appointments confirm the algorithmic profile of its Department of Mathematics and Computer Science. As the hub of the DIAMANT cluster, TUE will occupy a focal position in Dutch mathematics. The proposed DIAMANT chair will consolidate the prominence of TUE in coding and cryptology.

Discrete algorithms form traditionally a major field of research at CWI, and quantum computing is a newer one. The institute houses renowned groups in networks and optimization, and in algorithmic theoretical computer science, the latter being one of the very few groups of its sort in the Netherlands. In addition, a group in evolutionary and agent systems is emerging and a group in cryptology and information security has just been created. The proposed DIAMANT positions at CWI in cryptology and in algorithmic game theory will strengthen these two younger groups and reinforce the bonds between algorithmically oriented mathematicians and computer scientists at CWI.

At RU, computer mathematics is considered a core topic, as witnessed by the grant that the board of RU awarded to Barendregt, and by the establishment of computer algebra as one of three active research areas in the restructured mathematics department. The proposed UD positions in computational algebra and geometry and in computer mathematics will strengthen the focus in Nijmegen on converting discrete and algebraic mathematics into usable and coherent software (Magma), on the enhancement of interactive formalization of parts of mathematics (Coq), and on the integration of both. DIAMANT forms the ideal environment for the wide range of mathematics spanned by these efforts, and will provide the small research group with additional mathematical momentum.

UL has a broad and strong number theory group that is unique in the Netherlands. DIAMANT will strengthen the group in more applied directions, most notably in the direction of cryptology. The joint appointment of Ronald Cramer by CWI and UL is a first step in this direction. The proposed DIAMANT positions in Leiden, in cryptology and arithmetic

geometry, will create a group of researchers covering the full spectrum from advanced theory to tangible applications.

7. Added value for Dutch mathematics

One of the main developments in mathematics in recent decades is the emergence of algorithmic thinking in its traditionally purest branches. Applications are found at all levels of society, and the term *applied mathematics* is acquiring an entirely new meaning.

DIAMANT will turn the Netherlands into one of the principal sites where this worldwide development is taking place. It will do so by appointing top players in the field to permanent positions in Dutch institutions. This will lead to a stable community of researchers headed by internationally recognized authorities. This community will, through cluster-wide cooperation and through the attraction that it exercises on foreign scholars, acquire the critical size that is conducive to first-rate research.

Through the national masters courses in which DIAMANT members will participate, Dutch students will have the best possible teachers. Some of the students may develop into the top researchers of the future, while others will play a leading role in the knowledge-based economy.

The increased interaction with industry envisaged by DIAMANT will be a source of inspiration and, hopefully, renewed funding for mathematical research. DIAMANT's publicity will bolster the public perception of mathematics and mathematicians, and increase the attractiveness of the exact sciences for prospective students.

8. Added value for other scientific disciplines, Dutch R&D institutions, industry, and for society at large

Many areas of pure mathematics were not developed with a view towards specific applications, but were at a later stage found to have numerous applications in unexpected places. The areas covered by DIAMANT have a particularly strong track record in this respect. The nature of mathematical research makes it impossible to predict future developments, let alone breakthroughs; the only guide to what may happen tomorrow is provided by what happened yesterday. Looking back at the recent past, one sees that daily life has become pervaded by applications of DIAMANT-type research, many of which arise in the context of computers and internet. The following examples illustrate how rapidly these applications have become ubiquitous.

Storage of digital data on CD and DVD is a spectacular application of coding theory. The functioning of the internet, from routing connections to network design and commercial exploitation, is based on theory developed in combinatorial optimization and algorithmic

theoretical computer science. Search engines use clustering algorithms based on discrete mathematics and linear algebra. Secure information transfer, be it on the web or at an automatic teller machine, depends crucially on coding theory and cryptology. Personal computers control their working memory by means of a combinatorial algorithm that is based on scheduling theory. On mainframe computers, software for distributed computing is largely based on network scheduling. Generally, combinatorial algorithms are indispensable for applications as diverse as the unraveling of the genetic code and the exploitation of public transportation and air traffic.

Despite the diversity of these examples, one clearly perceives *networks* as a common theme and, more particularly, the optimization and security of networks. This is the NWO and OOW theme that DIAMANT serves par excellence.

The broad spectrum of applications creates links, not only with other parts of mathematics, but also with other disciplines, ranging from computer science to biology. Whereas some applications, such as the use of discrete tomography in medicine or the application of graph algorithms in chemistry, may not be entirely unexpected, others are completely unpredictable at this stage, and can therefore not be listed here. The availability of computing power has generated a demand for efficient algorithms for a virtually unlimited number of practical problems of a discrete nature. Indeed, this demand is already created by the *potential* existence of such algorithms, due to the laws of economic competition.

Existing contacts of DIAMANT members with industry include a variety of companies such as ABN-AMRO, ASML, CAN-Diensten, CLEAN, DSM, ING, NS Reizigers, Océ, ORTEC, Philips, ProRail, Rabo, SKF, TNO-Telecom, and Wolters-Noordhoff. The national forum for exchanging expertise and relevant problems with industry envisaged by DIAMANT will expand and intensify such contacts, and enhance DIAMANT researchers' awareness of the industrial and technological implications of their work.

9. Knowledge transfer

Education. With its wide-ranging expertise and close internal collaboration, DIAMANT is an eminently suitable instrument for realizing the currently emerging vision of masters level education in the Netherlands.

Earlier this year, a *Regieorgaan* representing all Dutch mathematics institutes was created with the task of coordinating and *clustering* the basic courses offered in the Dutch masters programs in mathematics. In the subdivision of mathematics of the Regieorgaan, the mathematics of DIAMANT mostly falls in the sections *algebra and geometry* and *operations research*. The latter section is essentially a continuation of the educational activities of the national graduate network in mathematics of operations research LNMB. A significant part

of the LNMB program is taught by DIAMANT researchers. In the algebra and geometry section, three of the four courses offered in 2004/2005 are taught by DIAMANT researchers. Clearly, the national courses taught by DIAMANT researchers will share the characteristics of DIAMANT research: modern, high-powered mathematics taught with a view towards algorithms and applications. Thus, the national masters courses in algebra, geometry, and operations research could be viewed as a substantial part of a virtual DIAMANT masters program.

Formally setting up a DIAMANT masters program would not serve the interests of the newly created Regieorgaan, and must at this stage be considered premature. However, DIAMANT will clearly be in a position to offer students at *all* Dutch universities a broad and coherent masters program in a prominent area of modern mathematics, a program that will be virtually compulsory for those students that choose the DIAMANT masters track at one of the institutions participating in DIAMANT. In fact, the DIAMANT masters tracks at TUE, RU, and UL will present themselves as such to the outside world, so that their students will in practice, if not formally, be enrolled in the entire cluster, rather than in a single university. The DIAMANT profile and the many existing close contacts between EIDMA and research groups in neighboring countries will simplify the recruitment of international students. In due time, changes in the administrative environment may allow the formal creation of a DIAMANT masters program based at TUE, UL, and RU.

The interaction of DIAMANT with the existing research schools Stieltjes, MRI, and EIDMA will need particular attention, because Stieltjes and MRI include institutions and researchers not taking part in DIAMANT. In the case of EIDMA, a complete integration of its educational activities in the DIAMANT cluster is natural.

Independently of possible changes in organizational structures, existing forms of education organized by DIAMANT researchers will be continued and expanded in the context of DIAMANT. Among these are the four successful *Stieltjes-* and *EIDMA-Stieltjesweken* on number theoretic and cryptologic topics that have been organized at the Lorentz Center since 2000. Also included are the intensive one-week EIDMA mini-courses, taught by eminent mathematicians such as Noga Alon, Peter Cameron, and László Lovász. The DIAMANT-type Stieltjesweken and the EIDMA mini-courses consistently attracted large numbers of participants, mostly masters and Ph.D. students from the Netherlands and abroad, but also researchers working in industry. DIAMANT will intensify these activities, and will consider the introduction of summer courses of a similar nature.

In view of the number of Ph.D. students (about 40) and masters students working under the supervision of DIAMANT researchers, it is clear that the critical mass to make such initiatives worthwhile is already present and that DIAMANT will create an excellent envi-

ronment for training future researchers. It goes without saying that the biweekly intercity seminars, the cluster-wide research meetings, and the special semesters featuring focused workshops, form an integral part of this environment.

Knowledge transfer to society at large, including public relations for mathematics, and visibility of the cluster. As indicated in Section 1, DIAMANT will pay special attention to its relationship with society at large by introducing a national colloquium, maintaining a website, and cherishing public relations. Many DIAMANT team members have a fine track record in this respect, as witnessed by the *Pi in de Pieterskerk* ceremony, by the popular Leiden website *Escher and the Droste effect*, by their visibility in the press, and by their involvement with *Vierkant voor Wiskunde*.

Apart from DIAMANT's efforts to strengthen its interaction with industry mentioned in Section 8, another strategic initiative will be the creation of a DIAMANT alumni association. Many former students of DIAMANT members occupy industrial positions. They, and their future colleagues, will be instrumental in multiplying the connections between DIAMANT and industry, and in facilitating the organization of short courses with speakers from both categories.

Literature

Below is a list of representative books and papers (co-)authored by members of research groups participating in DIAMANT.

1. R. Auer and J. Top, Legendre elliptic curves over finite fields, *Journal of Number Theory* **95** (2002), 303–312.
2. H. Barendregt, Towards an interactive mathematical proof language, pp. 25–36 in: F. Kamareddine (ed.), *Thirty five years of Automath*, Kluwer, 2003.
3. H. Barendregt and A.M. Cohen, Electronic communication of mathematics and the interaction of computer algebra systems and proof assistants, *Journal of Symbolic Computation* **32** (2001), 3–22.
4. H. Barendregt and H. Geuvers, Proof-checking using dependent type systems, pp. 1149–1238 in: J.A. Robinson and A. Voronkov (eds.), *Handbook of automated reasoning*, Volume 2, Chapter 18, Elsevier, 2001.
5. B. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, Quantum lower bounds by polynomials, *Journal of the Association for Computing Machinery* **48** (2001), 778–797.
6. M. de Berg, M. van Kreveld, M. Overmars, and O. Schwarzkopf, *Computational geometry: algorithms and applications*, Second Edition, Springer-Verlag, 2000.

7. F. Beukers, On Dwork's accessory parameter problem, *Mathematische Zeitschrift* **241** (2002), 425–444.
8. F. Beukers and H.A. van der Waall, Lamé equations with algebraic solutions, *Journal of Differential Equations* **197** (2004), 1–25.
9. W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: the user language, *Journal of Symbolic Computation* **24** (1997), 235–265.
10. W. Bosma and H.W. Lenstra, Jr., Complete systems of two addition laws for elliptic curves, *Journal of Number Theory* **53** (1995), 229–240.
11. W. Bosma and B. de Smit, Class number relations from a computational point of view, *Journal of Symbolic Computation* **31** (2001), 97–112.
12. R. Bröker and P. Stevenhagen, Elliptic curves with a given number of points, pp. 117–131 in: *Algorithmic Number Theory Symposium VI*, LNCS **3076**, Springer-Verlag, 2004.
13. A.E. Brouwer, Bounds on linear codes over a small alphabet, Appendix, pp. 412–454 in: D. Nogin, M.A. Tsfasman, and S. Vladuts, *Algebraic geometry codes. Basic notions*, Moscow Center for Continuous Mathematical Education, 2003.
14. H. Buhrman, P. Høyer, S. Massar, and H. Roehrig, Combinatorics and quantum nonlocality, *Physical Review Letters* **91** (2003), no. 047903.
15. O. Cheong, X. Goaoc, and Hyeon-Suk Na, Disjoint unit spheres admit at most two line transversals, pp. 127–135 in: *Proceedings of the 11th Annual European Symposium on Algorithms*, LNCS **2832**, Springer-Verlag, 2003.
16. O. Cheong, S. Har-Peled, N. Linial, and J. Matousek, The one-round Voronoi game, *Discrete and Computational Geometry* **31** (2004), 125–138.
17. A.M. Cohen, S. Murray, and D.E. Taylor, Computing in groups of Lie type, *Mathematics of Computation* **73** (2004), 1477–1498.
18. A.M. Cohen, G. Nebe, and W. Plesken, Maximal integral forms of the algebraic group G_2 defined by finite subgroups, *Journal of Number Theory* **72** (1998), 282–308.
19. R.J.F. Cramer and V. Shoup, A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, pp. 13–25 in: *Proceedings of Crypto 1988*, LNCS **1462**, Springer-Verlag, 1998.
20. K.M.J. De Bontridder, B.V. Halldórsson, M.M. Halldórsson, C.A.J. Hurkens, J.K. Lenstra, R. Ravi, and L. Stougie, Approximation algorithms for the test cover problem, *Mathematical Programming, Series B* **98** (2003), 477–492.
21. M.M. Deza and M. Laurent, *Geometry of cuts and metrics*, Springer-Verlag, 1997.

22. B. Edixhoven and A. Yafaev, Subvarieties of Shimura varieties, *Annals of Mathematics* **157** (2003), 621–645.
23. J. Fresnel and M. van der Put, *Rigid analytic geometry and its applications*, Birkhäuser, 2003.
24. J.F. Geelen, A.M.H. Gerards, and A. Kapoor, The excluded minors for $GF(4)$ -representable matroids, *Journal of Combinatorial Theory, Series B* **79** (2000), 247–299.
25. H. Gluesing-Luerssen and W. Schmale, On cyclic convolutional codes, *Acta Applicandae Mathematicae* **82** (2004), 183–237.
26. T. Hoeholdt, J.H. van Lint, and R. Pellikaan, Algebraic geometry codes, pp. 871–961 in: V.S. Pless and W.C. Huffman (eds.), *Handbook of coding theory*, Part 1, Elsevier, 1998.
27. P.H. van der Kamp, J.A. Sanders, and J. Top, Integrable systems and number theory, pp. 171–201 in: B.L.J. Braaksma et al. (eds.), *Differential equations and the Stokes phenomenon*, World Scientific, 2002.
28. I. Kerenidis and R. de Wolf, Exponential lower bound for 2-query locally decodable codes via a quantum argument, pp. 106–115 in: *35th Annual ACM Symposium on Theory of Computing (STOC)*, Association for Computing Machinery, 2003.
29. M. Laurent, Tighter linear and semidefinite relaxations for max-cut based on the Lovász-Schrijver lift-and-project procedure, *SIAM Journal on Optimization* **12** (2001), 345–375.
30. M. Laurent, A comparison of the Sherali-Adams, Lovász-Schrijver and Lasserre relaxations for 0-1 programming, *Mathematics of Operations Research* **28** (2003), 470–496.
31. M. Laurent, Lower bound for the number of iterations in semidefinite relaxations for the cut polytope, *Mathematics of Operations Research* **28** (2003), 871–883.
32. A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen* **261** (1982), 515–534.
33. A.K. Lenstra and E.R. Verheul, The XTR public key system, pp. 1–19 in: *Advances in cryptology—Crypto 2000*, LNCS **1880**, Springer-Verlag, 2000.
34. M. Li, X. Chen, X. Li, B. Ma, and P. Vitányi, The similarity metric, pp. 863–872 in: *Proceedings of the 14th Annual ACM-SIAM Symposium on Discrete Algorithms*, Association for Computing Machinery, 2003.
35. M. Li and P.M.B. Vitányi, *An introduction to Kolmogorov complexity and its applications*, Second Edition, Springer-Verlag, 1997.
36. L. Lovász and A. Schrijver, A Borsuk theorem for antipodal links and a spectral char-

acterization of linklessly embeddable graphs, *Proceedings of the American Mathematical Society* **126** (1998), 1275–1285.

37. W.E. de Paepe, R.A. Sitters, and L. Stougie, A competitive algorithm for the general 2-server problem, pp. 624–636 in: *Proceedings of the 30th International Conference on Automata, Languages and Programs ICALP*, LNCS **2719**, Springer-Verlag, 2003.

38. W. Plesken and B. Souvignier, Analyzing finitely presented groups by constructing representations, *Journal of Symbolic Computation* **24** (1997), 335–349.

39. M. van der Put and B.H. Matzat, Constructive differential Galois theory, Galois groups and fundamental groups, *MSRI Publications* **41** (2003), 425–467.

40. M. van der Put and M.F. Singer, *Galois theory of linear differential equations*, Springer-Verlag, 2003.

41. B. Schoenmakers, A simple publicly verifiable secret sharing scheme and its application to electronic voting, pp. 148–164 in: *Advances in cryptology—CRYPTO’99*, LNCS **1666**, Springer-Verlag, 1999.

42. A. Schrijver, Bipartite edge-colouring in $O(\Delta m)$ time, *SIAM Journal on Computing* **28** (1999), 841–846.

43. A. Schrijver, A combinatorial algorithm minimizing submodular functions in strongly polynomial time, *Journal of Combinatorial Theory, Series B* **80** (2000), 346–355.

44. A. Schrijver, *Combinatorial optimization—polyhedra and efficiency*, Springer-Verlag, 2003.

45. R. Schultz, L. Stougie, and M.H. van der Vlerk, Solving stochastic programs with integer recourse by enumeration: A framework using Gröbner basis reductions, *Mathematical Programming* **83** (1998), 229–252.

46. P. Schuurman and G.J. Woeginger, Polynomial time approximation algorithms for machine scheduling: ten open problems, *Journal of Scheduling* **2** (1999), 203–213.

47. B. Souvignier, Enantiomorphism of crystallographic groups in higher dimensions with results in dimensions up to 6, *Acta Crystallographica, Section A* **59** (2003), 210–220.

48. H.C.A. van Tilborg, *Fundamentals of cryptology. A professional reference and interactive tutorial*, Kluwer Academic Press, 2000.

49. G.J. Woeginger, When does a dynamic programming formulation guarantee the existence of a fully polynomial time approximation scheme (FPTAS)?, *INFORMS*