

## LE BULLETIN DU CRM

Le Bulletin d'information du Centre de recherches mathématiques  
www.crm.umontreal.ca**A word from the  
Director**

We are announcing in this Bulletin, the program for the next year's thematic program in the Mathematics of Computer Science. It covers a whole range of areas in which mathematics and computer science interact: complexity, quantum computing, combinatorics and algorithmics, logic, cryptography, random numbers and machine learning. The year incorporates several large conferences which will serve as focal points for the concentration periods, as well as a series of exciting workshops. There will be three Aisenstadt chairs for the year: Manuel Blum (Carnegie Mellon), Laszlo Lovasz (Microsoft Research), Endre Szemerédi (Rutgers University). They represent rather well the variety of fields in this vast subject. I would like to thank all the organisers for their superb work.

This year's program, in Groups and Geometry, is in full swing. The first session in particular, in topology and geometry in low dimensions, was a huge success: three weeks, with over one hundred participants for each week, including seventy students; two workshops, a week of advanced courses, and a lot of interaction. We are holding a similar session on the Langlands

*(continued page 2)*

1. Word from the Director
1. Année thématique 2002-2003
1. Lancement du LUTE
2. Le mot du directeur
3. Hommage André Aisenstadt
6. Groups and Geometry 2002
8. Topology and PhysNum
9. Physique Mathématique
10. CIRANO et MITACS
11. Rcm<sub>2</sub>
12. Tribute to / Hommage à Bob Sharp
13. Les prix, etc
14. Les stagiaires postdoctoraux
16. Les publications

Dans ce numéro...  
In this issue...**Theme year 2002-2003  
Mathematics in Computer Science**

The field of computation, formally born only last century but with roots that stretch back to Euclid, is now a mathematical discipline in its own right, with solid theoretical foundations on which are based its spectacular development. The CRM special year in the mathematics of computer science proposes to explore in depth a significant spectrum of the many sub-areas that are core foundational material for modern computer science, that exhibit significant and new mathematical content, and that have indeed influenced the development of mathematics.

Mathematically, the areas with the earliest influence on computer science were logic and discrete mathematics. Since then, the theoretical foundations of computer science have blossomed, and ideas from the area (like effectiveness, complexity and tractability) have grown to occupy an ever more important role in mathematics. More recently, a recurrent theme in many of the domains examined are probabilistic methods. These have permeated the whole of computer science, and so particular emphasis will be placed on the utilisation of these techniques, both in theoretical areas and in more applied ones such as simulation and machine learning.

*(Continued page 4)****Le rcm<sub>2</sub> lance son deuxième laboratoire  
universitaire, le LUTE***

Le 6 décembre 2001, a eu lieu le lancement du Laboratoire Universitaire sur le Temps Extrême du rcm<sub>2</sub>, en même temps que celui de trois autres initiatives dans le domaine des sciences de l'atmosphère: le Programme canadien de recherches sur la météorologie, la chaire en recherche sur le temps extrême de McGill, et deux réseaux de recherche en temps extrême. Ces initiatives sont financées par la Fondation canadienne pour les sciences du climat et de l'atmosphère, l'Institut de prévention des sinistres catastrophiques et le Service météorologique du Canada d'Environnement Canada.

**Collaboration et objectif**

Le Laboratoire Universitaire sur le Temps Extrême (LUTE) est, quant à lui, le fruit de la collaboration entre le Réseau de calcul et de modélisation mathématique (rcm<sub>2</sub>), qui regroupe huit centres montréalais de recherche ou de liaison et de transfert dans le domaine du calcul et de la modélisation

mathématique (dont le CRM), et le Service météorologique du Canada d'Environnement Canada.

L'objectif du laboratoire est de coordonner et favoriser la recherche et les collaborations dans le domaine des sciences de l'atmosphère et, plus particulièrement, du temps extrême, tout en assurant la formation de main-d'oeuvre hautement qualifiée dans ces domaines. Le LUTE est le deuxième laboratoire universitaire lancé par le rcm<sub>2</sub>, le premier étant les Laboratoires universitaires Bell inaugurés en décembre 1998.

**Diversités des expertises**

La structure qu'offre le rcm<sub>2</sub> permet non seulement de mettre l'accent sur une coordination à grande échelle des organismes partenaires dans un domaine donné, mais aussi de bénéficier de la diversité des

*(suite en page 11)*

program for function fields next April and May. It is preceded by an intense period at Queen's and followed by two excellent workshops at CRM. We hope that the same magic will happen. The program of the period is certainly a strong one: it is given later in this Bulletin.

We have the privilege this fall of witnessing the birth of a new laboratory of the Network for computing and mathematical modelling: the Laboratoire Universitaire sur le Temps Extrême (LUTE). This laboratory is the fruit of an accord concluded with Environment Canada, which includes not only some very important credits for research as well as an important contribution of computing time, but also a major commitment of research personnel, which will, I hope, nourish a long-term interaction.

One of the articles of this Bulletin is about a new company which has seen the light at CRM. It is piloted by one of our students, Philippe Saint-Jean in collaboration with D. Clonda and E. Lapalme. A start-up is a great adventure, and an unusual one in mathematics. It requires a certain audacity, as well as a great deal of energy to start a business, especially in the current economic climate, and they possess these qualities in abundance. They have all our support and all our wishes for his success.

We mourn the loss of two members of the mathematical community. Robert T. Sharp, a member of the CRM since its establishment, died last October 1st. His important contributions to science were highlighted in a special issue of the *Canadian Journal of Physics* in 1994, including notably a series of articles on generating functions in group representation theory. Two colleagues and friends, P. Winternitz and J. Patera, pay homage in this Bulletin. A few days later, André Aisenstadt, the great supporter of mathematics in Montreal, died at the age of 104. He has had a remarkable life, of which the obituary in this Bulletin gives some details. I had the privilege of meeting him many times over the years, and his interest for what was happening in "his" centre never flagged. We will be holding a small workshop in his memory on the 18th of January. Dr. Aisenstadt always paid a particular attention to young mathematicians, and a prize for them was inaugurated in 1991 bearing the Aisenstadt name. It is therefore quite appropriate that the prize-winners for 1991 and 2001, Niky Kamran and Jingyi Chen, should be giving two of the talks in January; the third will be given by the Director of the CRM who launched the prize, Francis Clarke.

Jacques Hurtubise

## Mot du directeur



Nous distribuons, avec ce bulletin, le programme de la nouvelle année thématique du CRM sur les mathématiques en informatique. Le programme couvre toute une gamme de domaines où les mathématiques et l'informatique interagissent: complexité, informatique quantique, combinatoire et algorithmique, logique, cryptographie, nombres aléatoires et apprentissage automatisé. L'année comportera plusieurs grandes conférences qui serviront de points focaux pour des périodes de concentration, et une variété excitante de

conférences. Il y aura trois titulaires de la chaire Aisenstadt pour l'année: Manuel Blum (Carnegie Mellon), Laszlo Lovasz (Microsoft Research), Endre Szemerédi (Rutgers University). Je dois remercier les organisateurs pour un travail superbe.

Le programme de cette année, en Groupes et géométrie, bat son plein. La période qui portait sur la topologie et géométrie en basse dimension, en particulier, fut un grand succès: trois semaines, avec plus de cent participants chaque semaine, dont soixante-dix étudiants; deux ateliers, une semaine de cours avancés, et beaucoup d'interaction. Nous avons une période semblable sur le programme de Langlands sur les corps de fonctions, qui se tiendra en avril et mai; il est précédé d'une période intense à Queen's et suivi de deux excellents ateliers ici au CRM. Nous espérons voir la même magie se produire. Le programme de la session, certes, est prometteur: voir plus loin dans ce Bulletin.

Nous avons aussi eu le privilège de voir cet automne la naissance d'un nouveau laboratoire de notre Réseau de calcul et de modélisation mathématique: le Laboratoire Universitaire sur le Temps Extrême (LUTE). Ce laboratoire est le fruit d'un accord conclu avec Environnement Canada et comprend des crédits importants pour financer la recherche, ainsi que du temps machine, mais aussi des contributions importantes en personnel, ce qui permettra, je l'espère, de développer une interaction à long terme.

Un des articles de ce Bulletin traite d'une nouvelle entreprise qui a vu le jour au CRM, pilotée par un de nos étudiants, Philippe Saint-Jean en collaboration avec D. Clonda, E. Lapalme et G. Dumas. L'aventure est grande, et n'est pas usitée en mathématiques. Il faut un certain cran et une grande quantité d'énergie pour démarrer une entreprise, surtout dans le climat économique actuel. Ce sont des qualités que Philippe et son équipe possèdent en abondance. Nous leur vouons tout notre appui, et leur souhaitons un grand succès.

Deux disparitions endeuillent la communauté mathématique, Robert T. Sharp, membre du CRM depuis ses débuts, décédait le 1er octobre. Ses importantes contributions scientifiques ont fait l'objet d'un numéro spécial de la Revue canadienne de physique en 1994, incluant notamment une série d'articles sur les fonctions génératrices dans la théorie de représentation des groupes. Un bel hommage lui est rendu dans le Bulletin par deux de ses collègues et amis, Pavel Winternitz et Jiri Patera. Quelques jours plus tard, à l'âge de 104 ans décédait André Aisenstadt, le grand mécène des mathématiques à Montréal. Il a eu une vie remarquable; la nécrologie dans ce Bulletin en donne une esquisse. J'ai eu le privilège de le rencontrer bien des fois au cours des années, et son intérêt pour ce qui se passait dans « son » centre n'a jamais diminué. Nous allons tenir un atelier en sa mémoire, le 18 janvier. Le Dr. Aisenstadt portait toujours une attention particulière aux jeunes mathématiciens, et un prix qui porte son nom pour ces jeunes mathématiciens a été créé en 1991. Il est donc de mise que deux des conférences de janvier soient données par les lauréats du prix en 1991 et en 2001, M. Niky Kamran et M. Jingyi Chen; la troisième sera prononcée par le Directeur du CRM qui a lancé le prix, M. Francis Clarke.

Jacques Hurtubise

## Hommage à André Aisenstadt

Le 4 octobre dernier s'éteignait André Aisenstadt, grand bienfaiteur du CRM. Il avait un jour déclaré, au cours d'une conversation reproduite dans ces pages (Oct. 90): "L'âge est sans importance. C'est ce que vous faites qui compte." Une exceptionnelle longévité lui a permis d'illustrer ce propos de façon éclatante.

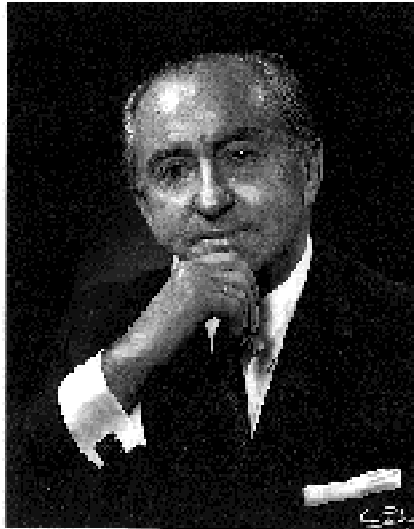
### Les sciences

Après avoir quitté sa Russie natale, il entreprend des études de génie à Darmstadt, au cours desquelles il se découvre plus d'attrait pour les mathématiques que pour l'ingénierie. Il se met donc à l'étude des mathématiques, aux Universités de Wurzburg et d'Iena, pour aller faire ensuite un doctorat en physique mathématique à Zurich sous la direction d'Erwin Schrödinger. Il compte parmi ses professeurs Hermann Weyl et Andreas Speiser, et parmi ses condisciples John von Neumann et Enrico Fermi. Quoiqu'Einsteïn eût déjà quitté Zurich à cette époque, il y retournait souvent et c'est au cours de l'une de ces visites qu'André Aisenstadt eut l'occasion de nouer une amitié qui se poursuivra jusqu'à la mort de l'illustre physicien.

### La venue au Canada

Une fois son doctorat terminé, André Aisenstadt se trouve devant un dilemme: Herman Weyl entreprend des démarches pour qu'il poursuive ses recherches en Angleterre, à Oxford ou à Cambridge, mais son père, homme d'affaires prospère, s'inquiète de voir son fils s'engager dans une carrière académique et l'invite à se joindre à l'entreprise familiale. Le père l'emporte, mais le fils regrettera toujours, semble-t-il, d'avoir abandonné les mathématiques. En 1939, André

Aisenstadt émigre au Canada et s'établit à Montréal pour des raisons d'ordre culturel. Peu de temps après son arrivée, Mackenzie King lui demande de participer à la création de la Société centrale d'hypothèque et de logement ainsi qu'à un programme de construction de logements pour les vétérans. Pendant qu'il s'occupe de ces projets à Ottawa, il



lance une entreprise à Montréal, la Parkdale Homes Development Corporation, qui construira de larges secteurs de la ville.

### Le mécénat

Vers 1967, sa fortune assurée, André Aisenstadt délaisse la construction pour le mécénat. Sa femme, Niussia Rosenstein, une pianiste accomplie, le convainc de participer activement à la mise sur pied du Festival et de l'École de

musique de Marlboro. Tous ceux qui eurent le plaisir de le rencontrer savent avec quelle verve il évoquait ses souvenirs de Marlboro, en particulier ceux qui avaient traité ses deux amis Rudolf Serkin et Pablo Casals. La même époque voit le début de son aide financière au CRM. Un premier don conduit, entre autres, à la création de la Chaire Aisenstadt, qui permettra au Centre d'inviter au fil des années plusieurs des mathématiciens les plus remarquables de l'époque. Le Prix André-Aisenstadt, qui souligne le talent de jeunes mathématiciens canadiens, verra le jour en 1991 grâce à un autre don. Et le pavillon des sciences mathématiques de l'Université de Montréal porte son nom en reconnaissance de l'appui financier essentiel qu'il a donné à sa construction.

### Les mathématiques en tête

Il serait difficile de donner une liste exhaustive de tous les autres organismes qui ont bénéficié de la générosité d'André Aisenstadt, comme par exemple, l'Hôpital juif de Montréal, l'Institut de recherches cliniques et l'Orchestre symphonique de Montréal. Il semble cependant avoir éprouvé une satisfaction toute particulière à favoriser le développement des mathématiques. "Grâce à ma relation avec le CRM, avouait-il dans la conversation déjà citée, j'ai eu une renaissance comme mathématicien." C'est donc avec un plaisir toujours renouvelé qu'il rencontrait les titulaires de la Chaire Aisenstadt et les récipiendaires du Prix.

### Un amour pour l'art

Le Pavillon, la Chaire et le Prix Aisenstadt rappelleront aux générations futures la reconnaissance qu'elles doivent à celui dont ils portent le nom. Mais nous serions également bien inspirés de ne pas oublier l'échelle des valeurs qui sous-tendait l'action philanthropique chez cet homme remarquable. Ne déclarait-il pas, toujours au cours de la même conversation: "Pour moi, l'art — et par art j'entends les mathématiques aussi bien que la musique, la littérature et la peinture — n'est ni un hors-d'oeuvre ni un dessert. C'est le plat principal de la vie."

Jean LeTourneux  
Directeur adjoint

### Activité spéciale en l'honneur d'André Aisenstadt

Le vendredi 18 janvier 2002, une activité spéciale aura lieu en l'honneur du Dr. André Aisenstadt. Trois conférenciers prendront part à cet événement. Niki Kamran (McGill), le premier récipiendaire du Prix Aisenstadt en 1991 prononcera une conférence intitulée «*L'opérateur de Dirac en géométrie de Kerr*». Francis Clarke (Institut Universitaire de France et Université de Lyon), directeur du CRM de 1984 à 1993 suivra avec sa conférence intitulée «*La conception de retours d'état (feedbacks) en théorie du contrôle: une introduction*»; finalement, Jingyi Chen (University of British Columbia), récipiendaire du Prix Aisenstadt 2001 prononcera une conférence intitulée: «*Quaternionic mappings between hyperkähler manifolds*». Des allocutions ainsi qu'une réception suivront en l'honneur du disparu.

(continued from page 1)

## SUMMER SCHOOL

### Summer School on Quantum Information Processing July 15-19, 2002

*Organizer:* Gilles Brassard (Montréal)

Classical information theory is firmly rooted in the classical physics of Newton and Einstein. But the world is quantum mechanical. This has prevented us from tapping the full potential of physical reality for information processing purposes. For instance, quantum mechanics allows for unbreakable cryptographic codes and such a high level of parallelism in computation that a classical computer the size of the universe would be left behind. The goal of this school is to make the field of quantum information processing accessible to a general audience of mathematicians and computer scientists who have little or no familiarity with quantum mechanics.

*Lecturers:* A. Ambainis, C.H. Bennett, G. Brassard, H. Buhrman, R. Cleve, C. Crépeau, N. Gisin, P. Høyer, R. Laflamme, M. Mosca, A. Tapp, J. Watrous.

## AIENSTADT CHAIR LECTURE SERIES

The holders of the Aisenstadt Chair for the year will be Manuel Blum (Carnegie Mellon), Laszlo Lovasz (Microsoft Research), Endre Szemerédi (Rutgers University).

## CONCENTRATION PERIODS Complexity Theory, Analysis of Algorithms

### May-June 2002

*Organizers:* Pierre McKenzie (Montréal), Denis Thérien (McGill)

In May 2002, the CRM will host two of the most important international conferences in theoretical computer science, namely the ACM Symposium on Theory of Computing and the IEEE Conference on Computational Complexity. In addition, there will be several one-week workshops on topics that lie at the core of the theory of computing. Each workshop will bring together a number of leading scientists who will present both expository lectures and state-of-the-art research.

**May 13-17, 2002:** *Lecture series on*

*branching programs, by Ingo Wegener (Dortmund)*

**May 19-21, 2002:** *A CM Symposium on Theory of Computing (STOC)*

**May 21-24, 2002:** *IEEE Conference on Computational Complexity*

**May 27-31, 2002:** *Randomness in Branching program*

Random techniques play an important role in computer science, through algorithms which give an efficient solution to problems for which no good deterministic solution is known, or through the probabilistic study of complexity. A week will be devoted to this theme, starting with the links between probabilistic methods and branching programs.

**June 3-7, 2002:** *Verification and model-checking*  
In the past ten years, theoretical work in the area of verification has started to bear fruit. The workshop will cover the major areas of this development, in particular those linked to model-checking.

**June 10-14, 2002:** *Descriptive complexity*

An area that has come to the fore in recent years, descriptive complexity gives a tool which complements more classical approaches to complexity theory. After a survey of the area, the workshop will concentrate on links between branching programs and algebraic structures.

*Invited speakers for the one-week workshops include:* M. Ajtai, D. Barrington, P. Beame, P.L. Crescenzi, R. Gavalda, N. Immerman, K.J. Lange, P. Pudlak, M. Sachs, R. Raz, P. Schnoebelen.

## Quantum Foundations in the Light of Quantum Information

**October 13 - November 2, 2002**

*Organizers:* Gilles Brassard (Montréal), Christopher A. Fuchs (Los Alamos National Laboratory)

Rolf Landauer's best-known aphorism is *information is physical*. This workshop is centred around the belief that *physics is informational!*

Our long-term purpose is to reformulate the foundations of quantum mechanics in the light of quantum information theory. Rather than being counterintuitive, could it be that quantum mechanics was inevitable for information to behave as we understand it now? For instance, what can we derive from the fact that unconditionally secure cryptographic key distribution is possible but bit commitment is not?

sible but bit commitment is not?

*Invited speakers include* H. Bamum, G. Brassard, H. Briegel, J. Bub, A. Cabello, C. Caves, R. Cleve, C. Fuchs, N. Gisin, D. Greenberger, L. Hardy, P. Hayden, A. Holevo, R. Jozsa, A. Kent, D. Mayers, D. Mermin, T. Mor, M. Nielsen, A. Peres, I. Pitowsky, R. Schack, B. Schumacher, J. Smolin, R. Spekkens, A. Steane, D. Wallace, W. Wootters, A. Zajonc.

## Combinatorics, Probability and Algorithms May 2003

*Organizers* David Avis (McGill), Luc Devroye (McGill), Bruce A. Reed (McGill)

Leave nothing to chance. This cliché embodies the common belief that randomness has no place in well-planned methodologies, every  $i$  should be dotted and every  $t$  should be crossed. In discrete mathematics, at least, nothing could be further from the truth. Introducing random choices into algorithms can improve their performance. The application of probabilistic tools has led to the resolution of combinatorial problems which have resisted attack for decades.

A month-long concentration period will take place around this general theme. Lecturers at the school will introduce participants to a number of weapons, mostly from the probabilistic arsenal, and their applications in combinatorics and in the study of algorithms. We anticipate a significant amount of collaboration between participants at the school during the month.

*There will be 5 hour mini-courses given by:* N. Alon (Technion), V. Chvatal (Rutgers), A. Frieze (Carnegie-Mellon), L. Lovasz, (Microsoft), C. McDiarmid (Oxford), M. Molloy (Toronto), J. Pach (City College New York and Hungarian Academy of Sciences).

## INTERNATIONAL ANNUAL MEETINGS

*ACM Symposium on Theory of Computing (STOC)*

**May 19-21, 2002**

*IEEE Conference on Computational Complexity*

**May 21-24, 2002**

*Organizers:* Pierre McKenzie (Montréal), Denis Thérien (McGill)

These two conferences are part of the concentration period on *Complexity theory, analysis of algorithms Mathematical Foundations of Programming Semantics (MFPS)*.

**March 17-22, 2003**

*Organizer:* Prakash Panangaden (McGill)  
Conferences and workshops in this series, held annually since 1985, aim to provide a forum for researchers in all areas surrounding semantics to present their latest research results, and to improve communication and interactions between mathematicians and computer scientists who work in these areas. The areas of relevance include category theory, domain theory, logic and topology on the mathematics side, and type theory, semantics, and the design and implementation of programming languages on the computer science side.

### IEEE Symposium on Logic in Computer Science (LICS)

**June 20-26, 2003**

*Organizers:* Amy P. Felty (Ottawa), Philip Scott (Ottawa)

To be held at the University of Ottawa in 2003, the IEEE Symposium on Logic in Computer Science (LICS) is an annual international forum on theoretical and practical topics in computer science that relate to logic in a broad sense. The CRM will be sponsoring four satellite workshops for this conference.

## WORKSHOPS

### Random Number Generation and Highly Uniform Point Sets

**June 17-28, 2002**

*Organizer:* Pierre L'Ecuyer (Montréal)

This workshop will bring together the world leaders in the theoretical and practical aspects of random number generation by computer and the design of highly uniform point sets for quasi-Monte Carlo integration. The general theme is the development of practical random number generation software for various classes of applications, such as simulation, statistics, numerical analysis, computer games, lotteries, cryptography, etc. In simulation, highly uniform (or low-discrepancy) point sets can often advantageously replace the traditional random numbers. Their construction and analysis can be based on ideas and tools that are very similar to those used for random number generators and we want to strengthen this connection.

*Invited speakers include:* G. Chaitin, C. Crépeau, L. Devroye, M. Evans, B.L. Fox, M. Fushimi, J. Gentle, P. Hellekalek, S. Heinrich, W. Hormann, A. Keller, G. Larcher, P.L'Ecuyer, J. Leydold, C. Lemieux, M. Mascagni, M. Matsumoto, S. Ninomiya,

T. Nishimura, A.B. Owen, G. Pirsic, W. Schmid, I. Sloan, S. Tezuka, H. Wozniakowski, C. Xing.

### Mathematical Models and Techniques for Analysing Systems

**September 30 - October 4, 2002**

*Organizer:* Prakash Panangaden (McGill)

The analysis of systems has both diversified and deepened tremendously in the last few years. In terms of diversification, systems of interest now include stochastic systems, real-time systems and hybrid systems, that is, systems where the state space is partly discrete and partly continuous. Applications include flight management systems for aircraft, process control systems, telecommunication systems and battle management systems. In all of these one has to deal with continuous time evolution and usually with probabilistic aspects as well. Perhaps the most successful mathematical technique for dealing with these problems - now almost 20 years old - is model checking. This is now being extended to probabilistic systems and the theory has advanced to the point where tools have been designed and built. In terms of the general mathematical theory co-inductive techniques, like bisimulation, have proved their value repeatedly.

The workshop would have two main speakers, who will each give five lectures: Prof. Marta Kwiatkowska, U. Birmingham *Probabilistic Model Checking* and Dr. Jan Rutten, CWI Amsterdam *Coinductive Calculus*.

*Other invited speakers include:* R. Alur, P. Caines, L. de Alfaro, R. Jagadeesan, D. Precup, R. Segala, F. van Breugel and M. Vardi.

### Finite Model Theory

**March 2-9, 2003**

*Organizer:* Denis Thérien (McGill)

This workshop will focus on the expressive power of logics and on the deep relationship between logic and computational complexity. The principal speaker will be Phokion Kolaitis (U.C. Santa Cruz). The workshop will be held at the Bellairs Research Institute of McGill University.

### Semigroups and Automata

**March 9-16, 2003**

*Organizer:* Denis Thérien (McGill)

This workshop will discuss recent developments in the theory of automata and semigroups, in particular some dealing with long-standing open problems such as decidability of the dot-depth hierarchy and

decidability of Rhodes complexity.

### Cryptographic Reduction of Quantum and Classical Protocols

**April 28 - May 2, 2003**

*Organizer:* Claude Crépeau (McGill)

Cryptographic protocols have been studied for two decades in the classical scenario under various computational assumptions. Such protocols as Bit Commitment, Oblivious Transfer and Multiparty Computations have been implemented and reduced to each other. Over the last few years, similar results are now achieved in the context of adversaries equipped with quantum computers. This workshop will bring together specialists of both classical and quantum cryptographic protocols who will present the state of the art in this fascinating area of research.

*Invited speakers include:* D. Beaver, C. Cachin, R. Cramer, C. Crépeau, I. Damgaard, P. Dumais, D. Gottesman, J. van de Graaf, R. Impagliazzo, J. Kilian, D. Mayers, M. Naor, S. Rudich, L. Salvail, A. Smith, A. Tapp, S. Wolf, M. Yung.

### Advances in Machine Learning

**June 2-13, 2003**

*Organizers:* Yoshua Bengio (Montréal), Balázs Kégl (Montréal), Doina Precup (McGill)

Probabilities are at the core of recent advances in the theory and practice of machine learning algorithms. The workshop will focus on three broad areas where these advances are crucial: statistical learning theory, learning algorithms, and reinforcement learning. The workshop will therefore bring together experts from each of these three important domains. Among the sub-topics that will be covered, we note: variational methods, graphical models, the curse of dimensionality, empirical methods to take advantage of theories of generalization error, and some of the applications of these new methods.

*Invited speakers include:* P. Bartlett, A. Barto, P. Frasconi, G. Hinton, M. Jordan, V. Koltchinskii, Y. Le Cun, M. Littman, G. Lugosi, S. Roweis, B. Scholkopf, D. Schuurmans, S. Singh, R. Sutton.

## ORGANIZING COMMITTEE

David Avis (McGill), Yoshua Bengio (Montréal), Gilles Brassard (Montréal), Luc Devroye (McGill), Pierre L'Ecuyer (Montréal), Pierre McKenzie (Montréal), Prakash Panangaden (McGill), Bruce Reed (McGill), Denis Thérien (McGill).

# GROUPS and GEOMETRY

## Thematic Programme 2001-2002

### GROUPS AND ALGEBRIC GEOMETRY



January - June 2002

*The importance of algebraic geometry in representation theory has grown enormously during the past decades, with the arrival of such techniques as  $D$ -modules and perverse sheaves. Geometry intervenes in a crucial fashion in the proof of such results as the Kazhdan-Lusztig conjecture, the construction of canonical bases for representations, and the work of Beilinson-Drinfeld on the Geometric Langlands programme. A number of deep connections have arisen between the algebraic geometry and algebraic combinatorics, whose ramifications extend all the way to mathematical physics and topology. A special emphasis of the programme will be in graduate training, and a variety of short courses will be organised, as well as graduate courses of a more introductory nature. Funding is available for graduate students wishing to attend.*

#### January-April 2002

#### Graduate Courses

- Abram Broer (Montréal)  
"Hilbert schemes of points and their applications"
- Henri Darmon (McGill)  
"Automorphic forms"
- Eyal Goren (McGill)  
"Curves, vector bundles on curves and their moduli"

- Frédéric Lesage (Montréal)  
"Kac-Moody algebras"

May 19-25, 2002

#### Number Theory Association, VII Meeting

*Organizers:* Hershy Kisilevsky (Concordia) and Eyal Z. Goren (McGill).

Registration and Submission of Abstract (deadline Feb. 15, 2002)

#### Session organizers:

- M. Kolster (McMaster): *Algebraic Number Theory*
- G. Walsh (Ottawa): *Computational Number Theory*
- K. S. Williams (Carleton): *Analytic Number Theory*
- D. Roy (Ottawa): *Diophantine Analysis and Approximation*
- E. Z. Goren (McGill): *Arithmetic Algebraic Geometry*

January 21-28, 2002

#### Winter School on Computations in Coxeter groups

*Organizers:* William Casselman (UBC), Robert Bédard (UQAM), Fokko Du Cloux (Lyon I)

These short courses are designed to show how techniques from computer algebra can be applied to effective computation in Coxeter groups. This course will take place at the Far Hills Inn, in the ski-resort town of Val Morin, about 150 km north of Montreal. This charming inn will provide an intimate setting for the workshop.

February 27-March 3, 2002

#### Group Actions on Rational Varieties

*Organizers:* Peter Russell (McGill)

The workshop will focus on recent developments in automorphisms of affine

spaces and related algebraic varieties with simple topology, in particular exotic affine spaces (algebraic varieties homeomorphic to an affine space).

April 8-19, 2002

#### Invariants Theory

*Organizers:* David Wehlau (Queen's), Eddy Campbell (Queen's) (the meeting will be held at Queen's University in Kingston)

The first week will be devoted to introductory lectures aimed at graduate students. During this first week, Professors H. Derksen (Michigan), P. Fleischmann (Kent), Hanspeter Kraft (Basel), and G. W. Schwarz (Brandeis), will give the introductory survey lectures.

The second week will be devoted to a workshop on Invariant Theory. Our expectation is that the younger mathematicians would stay to listen. There will be a number of talks given during this second week, approximately 50 minutes in duration, given by experts in the field. In this second week, lectures will concentrate on current problems in keeping with the workshop nature. During the second week, Bram Broer (UdeM), Loek Helminck (North Carolina), Marcus Hunziker (Georgia), Nondas Kechagias (Ioannina), Wilberd van der Kallen (Utrecht), Gregor Kemper (Heidelberg), Frederich Knop (Rutgers), Peter Littelmann (Wuppertal), Lucy Moser-Jauslin (UFR des Sciences et Techniques - Dijon), Mara Neusel, Vladimir Popov, Yasmine Sanderson (Rutgers), R James Shank (Kent), Nicolas Thiery (Lyons I), Ernest Vinberg, Reg Wood (Manchester).

For more details, consult the web page: [www.mast.queensu.ca/~cit02/index.html](http://www.mast.queensu.ca/~cit02/index.html)

**April - May 2002**

## The Langlands Programme for Functional Fields

**Organizers:** Henri Darmon (McGill), Jacques Hurtubise (CRM)

In April and May 2002, the CRM will host a five week series of lectures on subjects pertaining to the Langlands programme, with a particular emphasis on the case of function fields. One of the goals of the workshop is to introduce researchers from different areas of mathematics to recent major developments in the state of the Geometric Langlands Programme over function fields, both in the arithmetic and complex setting. A particular emphasis is placed on accessibility for advanced graduate students, post-doctoral fellows, and researchers who are interested in the area but who are not specialists. The period will comprise a three week long series of introductory lectures, to be followed by a more concentrated two week period of lectures by some of the most eminent specialists in the area.

**April 8 - April 26, 2002**

**Introductory series of lectures by:**

- Abraham Broer (Montréal) on D-modules
- Jacques Hurtubise (CRM) on Hitchin systems
- Jason Levy (Ottawa) on trace formulae
- Ram Murty (Queen's) "*A survey of the Langlands programme for number fields*"
- Ambrus Pal (CRM) on chtoucas
- Amritanshu Prasad (CRM) on automorphic representations over function fields
- David Savitt (McGill) on étale cohomology.

**April 29 - May 6, 2002:**

**Four three-hour series of lectures by :**

- David Ben-Zvi (Chicago) "*Open's*"
- David Goss (Ohio State) "*Recent advances in char. p arithmetic*"
- Alexander Polishchuk (Boston) "*Introduction to perverse sheaves*"
- Christoph Sorger (Nantes) "*Modulis*

*stacks of G-Bundles*"

- Kari Vilonen (Brandeis) "*TBA*".

**May 7 - May 14, 2002:**

**Two eight-hour series of Aisenstadt lectures by :**

- Edward Frenkel (UC Berkeley) "*Recent developments in the geometric Langlands Program*"
- Laurent Lafforgue (IHES), "*Chtoucas de Drinfeld et correspondance de Langlands*".

**April 29, May 2, May 7, May 10, 2002:**

**A special series of 8 lectures by :**

- Robert Langlands (IAS) "*Au-delà de l'endoscopie*"

**May 15, 2002:**

**On May 15, there will be a special one-day workshop in honour of Robert Langlands, with lectures by:**

Laurent Clozel (Paris), Dennis Gaitsgory (Chicago) & Yvan Saint-Aubin (Montréal).

Support is available for graduate students and post-doctoral fellows. A request for funds must be accompanied by a reference letter from the student's research director and a C.V.

**May 27 - June 10, 2002**

## Computational Lie theory

**Organizers:** William Casselman (UBC), Friedrich Knop (Rutgers)

This extended workshop is aimed at researchers interested in explicit computations in Lie theory, in particular Coxeter groups. In addition to the usual talks, there will also be several series of survey lectures, suitable for graduate students, by M. Brion (Grenoble), M. Geck (Lyon), F. Knop (Rutgers), P. Littelmann (Wuppertal), G. Olshanskii (IITP), J. Stembridge (Michigan). Professor G. Lusztig (MIT) will be delivering some of his Aisenstadt lectures during the period of the conference.

**June 10-15, 2002**

## Algebraic Transformation Groups

**Organizers:** Abraham Broer (Montréal), Jim Carrell (UBC)

The purpose of the meeting is to bring together experts in Algebraic Groups, Algebraic Geometry, Representation Theory and related areas, especially those touching on: geometric methods in representation theory using tools like equivariant cohomology and perverse sheaves; the Hilbert scheme of points on a surface and its connection with the  $n!$ -conjecture in algebraic combinatorics; equivariant versions of cohomology and Chow groups related to flag manifolds and Schubert varieties; quantum cohomology and Schubert calculus.

## ORGANIZING COMMITTEE

A. Broer (Montréal),  
S. Boyer (UQAM),  
J. Carrell (UBC),  
W. Casselman (UBC),  
H. Darmon (McGill),  
I. Hambleton (McMaster),  
J. Hurtubise (CRM),  
N. Kamran (McGill),  
B. Khesin (Toronto),  
F. Knop (Rutgers),  
R. Lee (Yale),  
D. Wise (Brandeis & McGill).