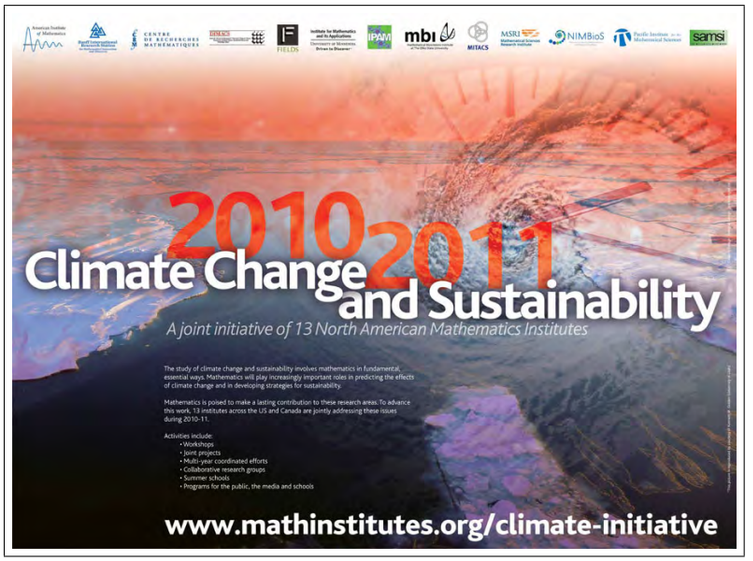
Le Bulletin du CRM
crm.math.ca
Automne/Fall 2010 | Volume 16 – Nº 2 | Le Centre de recherches mathématiques

2010–2011 Climate Change and Sustainability Program

by Odile Marcotte (UQÀM) and Christiane Rousseau (Université de Montréal)



The North-American Institutes in Mathematical Sciences meet at least once a year in January when they co-organise the Open House of the Institutes at the joint Mathematics Meeting of the American Mathematical Society (AMS) and the Mathematical Association of America (MAA). Moreover, the worldwide major research institutes in mathematical sciences circulate regularly among themselves the list of their planned thematic activities for the coming years, in order to minimize duplications and make sure that all major developments are covered. In parallel, in the US, the National Science Foundation (NSF) has initiated a major new initiative on sustainability that involves all directorates in the Foundation.

While in general part of the cooperation between the institutes consists in avoiding repetitions of programs at different institutes, it has appeared that joining the efforts on the SAME research theme was likely to produce an impact. The chosen theme for 2010–2011 is *Climate Change and Sustainability* (CSSP). This theme recognizes the crucial challenges to life on our planet. Up to now, the mathematical sciences have been involved in this theme only in a limited way, despite the large number of mathematical problems of great complexity, interest, and importance in a wide variety of related areas. Hence, this unprecedented collaboration is an invitation to the North-American mathematical sciences community to learn more about the underlying mathematical challenges and augment its research activity in these areas. It is also an opportunity to increase the local collaborations. Meanwhile, activities for the public are also being developed.

The implication of CRM in CCSP will lead to collaborations between CRM and NICDS (National Institute for Complex Data Structures), MITACS (Mathematics of Information Technology and Complex Systems) and the Canadian Forest Service at Natural Resources Canada in Canada, the Statistical and Applied Mathematical Sciences Institute (SAMSI) in the US, and GERAD (Groupe d'étude et de recherche en analyse des décisions) and OURANOS (consortium on Regional Climatology and Adaptation to Climate Change) in Québec.

As part of the CCSP, Jean-Pierre Aubin gave a 15-hour course entitled *Micromacroscopic Systems : A Viability Approach* during the week of September 20–24. The viability theory designs and develops mathematical algorithms for investigating the adaptation to viability constraints of (non-necessarily deterministic) develops mathematical algorithms for investigating the adaptation to viability constraints of (non-necessarily deterministic) evolutions governed by complex systems under uncertainty. It is well adapted to a variety of evolutions including ordinary

(*continued on page* 6)

Mathematics of Planet Earth 2013

The collaboration between the North American Institutes will not stop with the 2010–2011 Climate Change and Sustainability Program (CCSP). CRM and the other North American Institutes are planning a thematic year on "Mathematics of Planet Earth" in 2013.

`www.mpe2013.org` (`www.mpt2013.org` in French)

This project is more ambitious than CSSP, since *Mathematics of Planet Earth* is a much broader theme than Climate Change and Sustainability. The longer planning horizon will allow groups of institutes to organise joint thematic programs on some of the subthemes. An invitation has been sent to the planet to join and several institutes from other continents have become partners, while others are considering the invitation. The learned societies from around the world have also been invited to join. Their presence will allow the development of a large number of activities for the general public, the media, and the schools.

CRM–ISM Postdoctoral Fellows 2010–2011

The CRM–ISM postdoctoral fellowships are awarded on merit to promising researchers from around the world who have recently obtained their Ph.D. in the mathematical sciences. Fellowships are awarded for a two-year period and are co-funded by the CRM, the ISM, and the CRM laboratories. In addition, the CRM funds up to 50% of postdoctoral research fellowships associated with its thematic semesters. These fellowships last between six months and two years.

The members of the CRM are hosting nine new CRM–ISM postdoctoral fellows this year, including four which are associated with the two thematic programs in "Geometric, Combinatorial and Computational Group Theory" and "Statistics."

CRM–ISM Postdoctoral Fellows

Tiago Fonseca (Université Pierre et Marie Curie, 2010)
Advisors : Marco Bertola & John Harnad (Concordia), Jacques Hurtubise (McGill)

Tiago Fonseca has been been studying Alternating Sign Matrices, Completely Packed Loops and Plane Partitions (more precisely TSSCPP). Indeed, all these models, surprisingly, share the famous sequence 1, 2, 7, 42, 429,.... This involves quantum algebra, combinatorics, Hecke algebra, and Macdonald polynomials among others.

Nabil Kahouadji (Université Paris-Diderot, 2009)
Advisor : Niky Kamran (McGill)

The principal interest of Nabil Kahouadji is the study of the generalized isometric embedding problem of vector bundles, whose solutions lead, among other things, to show the existence of conservation laws when there are no symmetries for partial differential equations. The main motivations are the classical isometric embedding problem of Riemannian manifolds, and the problem of the compactness of weakly harmonic maps in Sobolev spaces. During his postdoctoral stay in Montréal, his main goal will be to obtain a global result of his local generalized isometric embedding theorem in the conservation law case, investigating the possibility of the existence of the same generalized isometric embedding in the smooth category, studying the rigidity of such generalized isometric immersions, exploring the problem for the codimension 2 and higher and looking for possible obstructions, and finally, investigating the existence of other embeddings that respect the action of a structural group G other than the orthogonal group.

Dimitris Koukoulopoulos (University of Illinois at Urbana-Champaign, 2010)
Advisor : Andrew Granville (Montréal)

Dimitris Koukoulopoulos works in analytic number theory. He is interested in questions regarding the multiplicative structure of integers and sieve methods as well as the theory of L-functions and its applications to prime number theory. In his thesis, he worked on problems about the distribution of divisors of integers. More precisely, for any fixed $k > 2$, he determined the number of distinct integers that can be written as product of k integers each less than N. During his stay at CRM, Dimitris Koukoulopoulos is planning to study generalizations of this problem as well as investigate other problems in multiplicative number theory such as under what circumstances is the average of a multiplicative function close to the prediction of the classical sieve.

Guyslain Naves (Université de Grenoble, 2010)
Advisor : Bruce Shepherd (McGill)

Guyslain Naves' interests are in graph theory and combinatorial optimization. More specifically, he works on integral multicommodity flow problems in graphs. These problems model transportation issues in networks. They are too complicated to be solved by usual techniques, hence one only tries to find approximation algorithms that can route without violating too much the capacities of the networks, if possible by only a constant factor called the congestion. These algorithms could be useful for the development of the Internet, as packet routing is a typical application of multicommodity flows.

Vivien Ripoll (Université Paris-Diderot, 2010)
Advisor : François Bergeron (UQÀM)

Vivien Ripoll studied at the École normale supérieure (ENS) in Paris, and completed his Ph.D. at ENS and Université Paris Paris-Diderot under the supervision of David Bessis on some properties of complex reflection groups. He is currently working at LaCIM (Laboratoire de Combinatoire et d'Informatique Mathématique), in collaboration with professors François Bergeron and Christophe Hohlweg. His research interests include combinatorics and the geometry of Coxeter groups and complex reflection groups.

Thematic CRM–ISM Postdoctoral Fellows

Mahmood Sohrabi (Carleton University, 2009)
Advisor : Olga Kharlampovich (McGill)

Mahmood Sohrabi works on different aspects of infinite finitely generated nilpotent groups. One specific project that he has been working on is understanding the structure of a model of the complete first order theory of an infinite finitely generated nilpotent group. Some other related topics of interest are Gromov–Hausdorff limits of nilpotent groups and large scale geometry of these groups.

Diane Vavrichek (University of Michigan, 2008)
Advisors : Olga Kharlampovich & Alexei Miasnikov (McGill)

Diane Vavrichek works in the field of Geometric Group Theory. She has done research on quasi-isometry invariants and Bass–Serre theory, and is interested in investigating coarse geometric aspects of limit groups while visiting the CRM.

Cornelius Reinfeldt (Heriot-Watt University)
Advisor : Olga Kharlampovich (McGill)

Elif Acar (University of Toronto)
Advisor : Christian Genest (McGill)

Lectures at the Leading Edge : Efim Zelmanov and Alex Lubotzky

by Olga Kharlampovich and Nicolas Touikan (McGill University)

The goal of the *Lectures at the Leading Edge* was to present pioneering work in group theory and other fields that is the outgrowth of important ideas in combinatorial and geometric group theory. These lectures were given by Efim Zelmanov and Alex Lubotzky during the workshop on "Geometric, Asymptotic, Combinatorial Group Theory with Applications" held at the CRM on August 15–19, 2010.

Efim Zelmanov

Efim Zelmanov is famous for his work in non-associative algebra and group theory, including his solution of the restricted Burnside problem. He was awarded a Fields Medal at the International Congress of Mathematicians in Zürich in 1994. He obtained his doctoral degree at Novosibirsk State University in 1980, and a higher degree at Leningrad State University in 1985. He is a professor at the University of California, San Diego. Efim gave lectures in Montréal on several occasions, and he was the CRM Aisenstadt Chair in 1996.

Efim Zelmanov's leading edge lecture was entitled *On Geometric Theory of Algebras* and presented some new efforts to apply ideas of growth, expanders and self-similarity to problems in the theory of algebras.

A group can be considered as a geometric object because it has a Cayley graph which is a metric space. Lie algebras do not have Cayley graphs. Zelmanov discussed recent efforts to apply geometric methods to infinite dimensional Lie algebras and their representations. He discussed growth functions for groups and their analog for algebras, the Gelfand–Kirillov (GK) dimension. The GK dimension measures the rate at which an algebra is generated by a generating set.

Gromov proved that a group has polynomial growth if and only if it has a nilpotent subgroup of finite index. In particular, this implies that a torsion group having a polynomial growth is finite. The fact that an algebra has a finite GK dimension is considered as the analog of having a polynomial growth.

The GK dimension is zero for algebras which are finite dimensional, and an elementary counting argument shows that the next possible dimension is one. However, Borho and Kraft showed that any real number value greater than or equal to two is possible. Bergman's famous Gap Theorem establishes that there is no algebra with GK dimension strictly between one and two. A theorem of Small and Warfield asserts that an affine prime algebra R over a field F of GK dimension 1 is a finite module over its center, and that its center is a finitely generated F-algebra of GK dimension 1. In the special case when R is a finitely generated domain over an algebraically closed field with GK dimension 1, it follows by Small-Warfield's and Tsen's theorems that R is in fact commutative. A theorem of Small, Stafford and Warfield shows that a finitely generated algebra with GK dimension 1 is close to being commutative in the sense that it must satisfy a polynomial identity. Recently, Lenagan and Swoktunowicz constructed infinite dimensional nil algebras of finite GK dimensions over countable fields answering the question of Small.

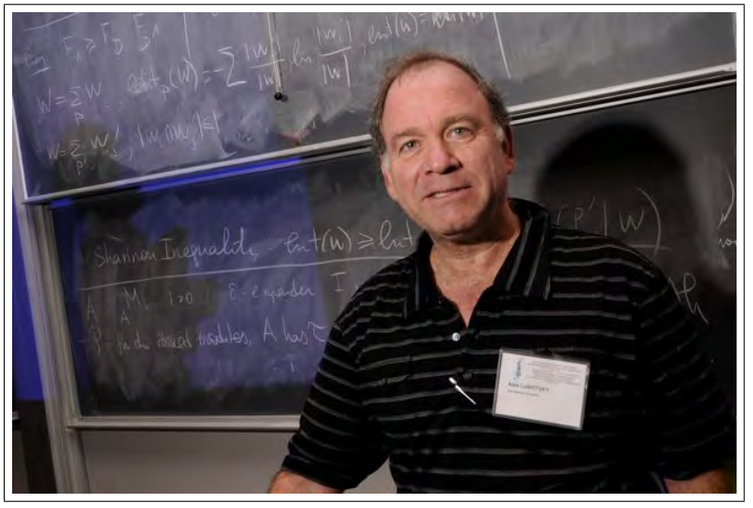
Isoperimetric profile in algebras was first introduced by Gromov in 2008. Zelmanov discussed the behavior of the isoperimetric profile under various ring theoretic constructions and its relation with the Gelfand-Kirillov dimension (in particular, results of Adderio). The isoperimetric profile is an asymptotically weakly sublinear function, and it's linear if and only if the algebra is non-amenable (in the sense of Elek). In this sense it can be viewed as a measure of the amenability of an algebra.

Efim also discussed self-similarity for algebras. After the counterexamples of Golod and Shafarevich new finitely generated infinite torsion groups were constructed by (i) Alyoshin, Grigorchuk, Gupta, Sidki and Sushchansky, and (ii) infinite torsion groups of bounded degree by Novikov and S. I. Adian, and Tarski Monsters by Ol'shansky. The groups (i) are residually finite whereas the groups (ii) are not. The Grigorchuk groups are of particular interest since they are of intermediate growth. Is there an analog for algebras? The Grigorchuk group is a group of automorphisms of a regular rooted tree. It is natural therefore to look for "Grigorchuk algebras" among algebras of differential operators in infinitely many variables (which correspond to infinitely many vertices of a tree). The first such construction was suggested by Petrogradsky for fields of characteristic 2. Shestakov and Zelmanov generalized it and extended to algebras of arbitrary positive characteristics.

Efim also discussed the notion of dimension expanders and property τ suggested by Lubotzky and Zelmanov in characteristic zero.

Alex Lubotzky

Alex Lubotzky is the Maurice and Clara Weil chair in mathematics at the Einstein Institute of Mathematics, which is famous for research in group theory, Lie groups, combinatorics and field arithmetic. Alex is a recipient of Bergman Memorial Prize of the Bi-National Science Foundation, United States-Israel (in cooperation with Professor Hyman Bass of Columbia University.) His other prizes include the 1991 Erdös Prize of the Israeli Mathematical Union (a prize for the best Israeli mathematician/computer scientist under the age of 40), the 1993 Ferran Sunyer i Balaguer Prize from the Institute d'Estudis Catalans in Barcelona for the book Discrete groups, Expanding Graphs and Invariant Measures, *the 2002 The Rothschild Prize, and the 2002 Ferran Sunyer i Balaguer Prize for the book* Subgroup Growth *with Professor Dan Segal. In 2005, he was elected as Foreign Honorary Member of the American Academy of Arts and Sciences, in 2006 he received an honorary doctoral degree from the University of Chicago, and in 2007 he received the Rector's Prize of the Hebrew University (for excellency in research, teaching and service to the university.) He is also the editor of many journals.*



Alex Lubotzky's gave two leading edge lectures. The first one was entitled : *Short Presentations of Finite Simple Groups*.

The starting point of combinatorial group theory is to describe a group in terms of generators and relations. Given a finite set of generators X and a finite set R of relations (words in the alphabet $X \cup X^{-1}$), we can define the length of a group presentation as :

$$\text{length}(\langle X \mid R \rangle) = |X| + \sum_{r \in R} \text{length}(r).$$

Alex presented his joint effort with Guralnick, Kantor and Kassabov to find "short" presentations. Such questions are motivated by conjectures such as the Babai-Smerédi Conjecture which asks whether there is a constant $c \in \mathbb{R}$ such that for any finite group G there is a presentation with length $O(\log(|G|^c)$; or the Mann Conjecture, asking whether every finite group has a presentation with $O\big(\log(|G|)\big)$ relations. These types of questions are of interest to computational group theorists, and are also related to counting the number of finite groups of a given order.

Their first main result is that non abelian finite simple groups (except possibly the Rees groups) of rank n over the field $\mathbb{F}_q$ (viewed as matrix groups) have presentations of length $O\big(\log(n) + \log(q)\big)$. This is optimal by information theoretic considerations.

The second main result is an affirmative solution to a conjecture of Holt's about $\mathbb{F}_p$-cohomology of groups which implies by a previous result of Lubotzky's that there is a constant $0 < c \leq 18$ such that the number of groups of order at most n generated by d elements is at most $n^{cd\log(n)}$, thus settling a conjecture by Mann and Pyber.

Alex's second talk was entitled *Sieve Methods in Group Theory* and presented joint work with Meiri.

The Dirichlet prime number theorem states that for co-prime integers a, d there are infinitely many primes in the set $\{a + nd \mid d \in \mathbb{Z}\}$. There is a dynamical interpretation of this result. Indeed, an arithmetic progression can be thought of in terms of the orbit of a point under the action of $(\mathbb{Z}, +)$ on $\mathbb{Z}$ given by :

$$n \colon z \mapsto z + nd.$$

This result is also a type of regularity condition on the distribution of the images of the primes in the quotient ring $\mathbb{Z}/d\mathbb{Z}$.

There has been a recent non-commutative analogue of this initiated by Peter Sarnak and further developed in works of Bourgain–Gamburd, Helfgott, Breuillard–Tao–Green, Pyber–Szabo, Salehi–Golsefidy–Varju, known as the affine sieve method, which yields results such as : Let $\Gamma \leq \mathrm{GL}_n(\mathbb{Z})$ be a finitely generated infinite subgroup, let G be the Zariski closure of Γ, and let G^0 be the connected component of G. If G^0 is perfect then for some suitable vectors in $v \in \mathbb{Z}^m$ the orbit Γv contains infinitely many almost primes. This result is in a sense a non-commutative analogue of the dynamical interpretation of the Dirichlet prime number theorem.

Alex indicated a key point in this result : that for q a square-free integer, the Cayley graphs of image of Γ in the homomorphisms $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$ form families of *expander graphs* (this is basically the property (τ). Expander graphs enjoy the property that the probability measures (on the vertices) obtained from a random walk converge exponentially fast to the uniform distribution. It turns out that this gives rise to a very powerful method.

When dealing finitely generated infinite groups, finding pertinent quantitative measures for the size of infinite subsets is a subtle activity. Alex presented one such measure and introduced the notion of a subset Y of a finitely generated group Γ being *exponentially small* and presented his main basic theorem,

(*continued on page* 12)

The Canadian Number Theory Association's Eleventh Meeting

Acadia University, July 11–16, 2010

by David McKinnon (Waterloo University)

The Canadian Number Theory Association's biennial meetings are amongst the largest meetings of the world's leading number theorists. The eleventh meeting was no exception, attracting 130 participants from Europe, North America, and Australia. The meeting began on Sunday, July 11, with a plenary talk by Zeev Rudnick entitled *Eigenfunctions and Sums of Squares*, and proceeded through the week with 82 other lectures on a variety of topics in number theory, including o-minimal structures, vanishing of L-functions, rational points on algebraic varieties, and Diophantine approximation.

One of these lectures, on Wednesday, July 14, was given by Valentin Blomer, recipient of the 2010 Ribenboim Prize for distinguished research in number theory by a mathematician who is Canadian or who has close connections to Canadian mathematics. His prize lecture was entitled *On the Ramanujan Conjecture*, and described Dr. Blomer's impressive work on generalizations of the conjecture and their proofs. The conjecture, which was proven in 1973 by Deligne, states that if p is prime, then the Fourier coefficient $\tau(p)$ of the cusp form $\Delta(z)$ of weight 12 satisfies $|\tau(p)| \leq 2p^{11/2}$. In his talk, Dr. Blomer described his joint work with Farrell Brumley in proving a natural generalization of the conjecture to the groups GL_n over arbitrary number fields.

Valentin Blomer, the recipient of the 2010 *Ribenboim Prize, with the president of the Prize Committee, Chantal David.*

Most of the plenary lectures were, of course, not prize lectures. Michael Bennett's lecture featured a novel approach to solving an infinite family of Thue–Mahler equations, extending work of Darmon and Granville. Jan-Hendrik Bruinier gave an impressive algebraic talk, in which he described the calculation of special values of modular functions associated to Shimura curves. Kevin Buzzard gave an overview of the p-adic Langlands program and recent progress towards some proofs. Hershy Kisilevsky's talk dealt with the variation in the rank of the Mordell–Weil group of an elliptic curve as the number field of definition varies. Kristin Lauter discussed the problem of how to count certain kinds of simultaneous embeddings of certain number rings into quaternion algebras over totally real fields, which relates to a famous formula of Gross and Zagier and the intersection pairing on a Hilbert modular surface.

An application of model theory to number theory was the main theme of Jonathan Pila's plenary lecture. He described a novel idea of Umberto Zannier to use o-minimal structures to solve Diophantine equations, and uses it to prove the Andre-Oort conjecture for products of modular curves. Zeev Rudnick, on the other side of number theory, probed the boundary with mathematical physics by using diophantine techniques to describe the set of eigenfunctions of the Laplacian operator on flat tori. In a similar vein, K. Soundararajan's talk described applications of number theory to quantum chaos, including problems that lie in the intersection of the two fields. In particular, Soundararajan discussed the proof of a conjecture of Rudnick and Sarnak that the high-energy eigenfunctions of the Laplacian on the quotient of the complex upper half-plane by an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$ are equidistributed.

In all, the meeting featured ten plenary lectures, in addition to Valentin Blomer's prize lecture and Ken Ono's public lecture on Ramanujan and his discovery of mock theta functions. This sounds fairly technical for a public audience, but Dr. Ono's talk was very accessible, featuring photographs of his research trips to India, and a very down-to-earth description of Ramanujan's mathematics. Dr. Ono also gave a plenary lecture aimed at professional number theorists, in which he described the uses of Ramanujan's mock theta functions in the study of special values of L-functions.

There were also 22 invited lectures, each roughly 35 minutes in length, and 49 lectures contributed by other participants, each of roughly 15–20 minutes in length. The pace of the meeting was very pleasant, with plenty of mathematical energy generated by the talks, and yet plenty of time before, after, and between talks to allow for the interesting mathematical discussions that are some of the greatest fruits of mathematical conferences.

There was also a brief meeting in the middle of the conference to decide the future of CNTA. It was already known that the Twelfth Meeting, in 2012, would be held in Lethbridge, but during the week it was also agreed that for its Thirteenth Meeting

in 2014, the Association would return to Ottawa, at Carleton University.

The CNTA Eleventh Meeting was generously funded by the Atlantic Association for Research in the Mathematical Sciences (AARMS), and also by the Centre de recherches mathématiques (CRM), the National Security Agency (NSA), the University of Acadia and the Number Theory Foundation (NTF).

Climate Change and Sustainability Program

(*continued from page* 1)

differential equations and control systems. The course has focused both on the theoretical and algorithmic aspects of this theory. The basic objects studied by the theory are sets. In particular, basic notions of viability theory include viability kernels and capture basins (the latter notion being useful when there is a target to reach). The topological properties of these sets are studied under the hypothesis that the evolutionary systems are upper semicompact and/or lower semicontinuous. Jean-Pierre Aubin specialized its discussions of applications to the ones interesting the audience, in particular finance and dynamical systems.

The CRM is also organising (or co-organising) five research workshops. The first workshop *Statistical Methods for Geographic and Spatial Data in the Management of Natural Resources* jointly organised with NICDS, took place on March 3–5 2010. The organisers were DongMei Chen (Queen's), Thierry Duchesne (Laval), Anne-Catherine Favre (Laval) and Subbash R. Lele (Alberta). The 13 lectures of the first day of the workshop (March 3) were all on topics related to the theme "Hydrology, Climatology, Meteorology." In particular there were lectures on spatial models of ozone dispersion (Zidek), spatial interpolation methods for measuring precipitations (V. Fortin, Carreau, Tapsoba, Fortier-Filion), modelling of extreme climatic phenomena (Naveau, Garçon), as well as on other methodological problems in the analysis or modelling of spatial data. The 7 lectures of the next half-day dealt with the analysis and modelling of zoonotic diseases. The 6 lectures that took place on the afternoon of March 4 dealt with problems from ecology, especially methods used to construct resource selection functions (Lele, Merrill, Keim) and spatial models for varied problems (M.-J. Fortin, Smith, Gralewicz). The last day of the workshop consisted of a discussion on research financing and meetings of small groups of researchers with common interests.

CRM belongs to a Montréal area network of research centres in mathematical sciences, the Network for Computing and Mathematical Modeling (ncm_2, or rcm_2 in French). The first activity for the public within CSSP is a panel organised by the ncm_2 network, which took place on September 28. The panel, entitled *Le développement durable et le rôle des scientifiques* was chaired by the Radio-Canada journalist Sophie-Andrée Blondin. The invited panelists were Jean-Pierre Aubin, Graciela Chichilnisky and Jean-Pierre Blanchet. The associations of mathematics teachers and/or cegep professors in Québec will be invited to hold their annual congresses on themes related to CCSP. The theme of the 2010 congress of the Association mathématique du Québec (AMQ) is *Mathématiques et environnement*. The first issue of the Accromath magazine in 2011 will also be related to climate change and sustainability.

The joint CRM–GERAD workshop, *Decision analysis and sustainable development* took place on September 27–28, just before the aforementioned panel. It was organised by Michèle Breton (HEC), Odile Marcotte (CRM and UQÀM), Christiane Rousseau (Université de Montréal), and Georges Zaccour (HEC). The invited speakers were Jean-Pierre Aubin, who spoke on a dynamical allocation method of emission rights of pollutants ; Graciela Chichilnisky, who spoke on the foundations of probability and statistics with black swans (i.e., very rare events that may entail catastrophic risk) ; Alain Haurie, who presented a meta-modelling game-theoretic analysis of international emissions trading schemes with full banking and borrowing ; and Gerhard Sorger, who spoke on the implications of intergenerational equity for the study of quasi-orderings of infinite utility streams satisfying the strong Pareto axioms. The workshop featured economic models that take into account sustainable developement, and the contributions drew upon varied decision analysis tools and methods (e.g., optimization, operations research, game theory, dynamical systems, and risk analysis).

Two more workshops will take place in 2011. The first one, *Statistical Methods for meteorology and climate change* (January 12–14, 2011), is a joint venture with SAMSI. It is part of the CRM thematic winter semester 2011 in statistics. The organisers of this workshop are Jean-François Angers (Montréal), Anne-Catherine Favre (Laval), Luc Perreault (IREQ) and Richard L. Smith (SAMSI). The workshop will bring statisticians and climatologists together to talk about new statistical methodologies devoted to the study of climate change. The themes that will be addressed during the workshop include assessment of uncertainty in climate change projections, spatial patterns of climate, climate reconstruction, climate extremes, climate trend assessment, downscaling, data assimilation, and stochastic weather generators.

The last workshop, *Balance, Boundaries and Mixing in the Climate Problem* will take place in the fall of 2011. The organisers are Peter Bartello and David Straub from McGill, and Shafer Smith from the Courant Institute. It will focus on turbulent mixing in the atmosphere and oceans. Although crucial to coarse-resolution numerical modelling efforts, much of it really occurs below typical grid scales. Recent progress in geophysical fluid dynamics will be presented to the community, which could then use it to improve the integrated studies of complex environmental systems. The workshop will span the range from canonical flows in their most theoretically accessible form, to more realistic flows with a full range of complications, both physical and numerical.

Theme Semester W2010

Organisers : Henri Darmon and Eyal Goren (McGill University),
Andrew Granville (Université de Montréal), Michael Rubinstein (University of Waterloo)

The CRM 2010 Winter Thematic Semester "Number Theory as Experimental and Applied Science" was devoted to recent developments in number theory with a specific focus on significant practical applications, as well as on the many ways in which the field stands to be affected by the emergence of new software and technologies. The numerous scientific activities included five one-week workshops and several courses.

A graduate course "Computational Aspects of Quaternion Algebras and Shimura Curves" was given by John Voight (University of Vermont) who visited the CRM for the whole semester. The course covered a variety of subjects in four months, including the basic theory of quaternion algebras over fields and the relationship to quadratic forms, the structure theory of quaternion algebras and orders over local and global fields, graphs, adelic methods (Eichler's theorem of norms, strong approximation, and the mass formula), quaternion unit groups, Shimura curves, and the relationship to supersingular elliptic curves and theta functions. These topics fit well with the five week-long workshops that were held during this period. There were about 8 graduate students registered in the course, which was also attended by additional graduate students and postdoctoral fellows.

A mini-course on "Expander graphs" was given by Eyal Goren (McGill University) and consisted of 10 hours of lectures giving an overview of some of the main topics in this area (Ramanujan graphs and complexes, the Alon–Boppana theorem and the spectrum of infinite trees, known constructions of Ramanujan graphs, the zig-zag product, Cayley graphs and expansion), and a report on some very recent breakthroughs concerning expansion in finite simple groups. In addition, certain applications of expander graphs were presented. The program was organised so as to serve as preparation and motivation for the CRM workshop on "Graphs and Arithmetic." The participants included about 10 graduate students and 5 postdoctoral fellows.

A mini-course on "Point Counting and Cohomology," organised by Henri Darmon (McGill University) consisted of 10 hours of lectures given by 4 lecturers (Henri Darmon, Aurel Page, Francesco Castella and Adam Logan). The mini-course discussed point counting algorithms for varieties over finite fields arising from cohomology (etale and p-adic) and was an introduction to the workshop "Counting Points : Theory, Algorithms and Practice." The basic principle used by all those algorithms is that the zeta function of a variety over a finite field is the characteristic polynomial of the Frobenius endomorphism acting on the cohomology of the variety. The first point counting method is based on the l-adic cohomology ; it is due to Schoof, and works well only for elliptic curves. This method was presented by Aurel Page. The methods based on p-adic cohomology (which is closely related to the de Rham cohomology of the variety computed with differential forms, and seems better for explicit computations) were presented by the other lecturers. Darmon talked about the AGM method of Satoh based on the arithmetic-geometric mean, and Logan talked about the approach of Lauder which exploits the differential equation associated to the Gauss–Manin connection to compute the zeta functions of the varieties as a whole.

Magma Workshop on p-adic L-Functions
Organisers : M. Greenberg (Calgary), X.-F. Roblot (Lyon 1), M. Watkins (Sydney), C. Wüthrich (Nottingham)

To kick off the thematic semester, the CRM played host to the 2010 Magma workshop on p-adic L-functions. This workshop brought together forty participants, both students and researches, from Australia, Canada, China, England, France, Japan and the United States with the goal of developing applications of computer algebra and "p-adic numerical analysis" to fundamental problems of number theory.

The workshop opened with a wide-ranging lecture by Henri Darmon (McGill) on the application of p-adic L-functions to the explicit construction of many gems of arithmetic, from units in rings of algebraic integers to rational points on abelian varieties. This theme was expanded upon in several other lectures. Other major themes of the workshop were the interplay between theoretical insight and advances in explicit computation, Iwasawa theory and p-adic automorphic forms and p-adic Hodge theory. The workshop was capped off by a wonderful colloquium lecture by John Coates (Cambridge) on the past, present and future of Iwasawa theory and p-adic L-functions. The hospitality and excellent environment for scientific exchange provided by the CRM was appreciated by all and facilitated a productive, highly successful workshop.

Workshop on Graphs and Arithmetic
Organisers : E. Goren (McGill), A. Granville (Montréal), W. Li (Penn State)

The connections between graphs and arithmetic emerged from several directions, via explicit constructions, uniformization, and arithmetic properties of subgroups of Lie groups. Ultimately, all these results rest on spectral or structural properties of algebraic groups, where the crucial input is often supplied by number theory (in the wide sense) and algebraic geometry. The theory of expander graphs has fertilized number theory, geometry and theoretical computer science. The workshop on "Graphs and Arithmetic" had several focal points. (i) Ramanujan complexes (ii) Expansion in finite simple groups and in Lie groups (iii) Connection between expanders and geometry and (iv) The affine sieve, in addition to lectures on related topics that do not fall under these classifications, notably the lecture by Tamar Ziegler who reported on the spectacular result of

Green–Tao–Ziegler concerning primes in linear forms, and the lecture by the Aisenstadt prize winner, Omer Angel, concerning limits of graphs and local versus global phenomena in graphs.

The workshop was attended by 52 participants coming from Canada, US, England, Hungary, China, Spain, Australia, Mexico, France, Japan and Israel. It was an exciting event, where many important results that have not yet appeared in print, or for which a preprint doesn't even exist yet, were reported. It gave a panorama of the subject, as well as important emerging directions.

Workshop on Computer Methods for *L*-Functions and Automorphic Forms
Organisers : B. Edixhoven (Leiden), C. Citro (Washington), M. Rubinstein (Waterloo), W. Stein (Washington)

The purpose of this gathering, funded by the CRM and also by an NSF Focused Research Group grant, was to give researchers an opportunity to collaborate on research related to *L*-functions and automorphic forms. Afternoons were reserved for work, while mornings were devoted to talks. Ten morning lectures were held, with talks on various computational aspects of *L*-functions and automorphic forms given by : Amod Agashe, Salman Baig, David Farmer, William Hart, Nathan Ryan, Michael Rubinstein, John Voight, William Stein, and Mark Watkins. In addition, Akshay Venkatesh gave three Aisenstadt Chair lectures, one of which was a talk for the general public. Several working groups were formed during the workshop, on the topics of : classical modular forms, Siegel modular forms, ranks of elliptic curves in families of twists, Maass forms, Hilbert modular forms, analytic algorithms and elliptic curves over function fields. The workshop also gave an opportunity to several postdoctoral fellows and graduate students to discuss their ideas with the attending researchers.

Workshop on Computer Security and Cryptography
Organisers : T. Lange (TU Eindhoven), K. Lauter (Microsoft), J. Silverman (Brown)

This workshop featured a plethora of distinguished lecturers speaking on a variety of current research topics. These included lectures on integer factorization algorithms and implications for the security of RSA, analysis of elliptic and hyperelliptic curve cryptography, including security analyses and applications to pairing-based cryptography, a new proposal for fully homomorphic encryption, and hash function attacks.

The 27 presentations covered major areas of cryptography and security and provided a good balance between survey talks and presentations of recent results. The talks can be grouped into the following areas : Factoring large integers ; ECC and DLP attacks ; Pairing-based cryptosystems ; Code and lattice-based cryptosystems (post-quantum cryptography) ; Fully homomorphic encryption ; Hash function attacks ; Computational resources ; Recent new cryptographic applications.

There were more than 70 participants attending the workshop, and the organisers received extremely positive feedback from the participants, both about the quality of the presentations and about the opportunities to interact and to discuss outside the talks. Several participants pointed out that they made new contacts and that they have started new collaborations.

Workshoop on Counting Points : Theory, Algorithms and Practice
Organisers : K. Kedlaya (MIT), J.-F. Mestre (Paris 7)

The activities of this workshop were disrupted by the eruption of the Eyjafjallajökull volcano that closed the European airspace for several days. As a result, the organisers recruited some graduate students and postdoctoral fellows which were attending the activities and who graciously agreed to give last minute talks, as Nick Alexander (University of California, Irvine), Christiane Peters (Technische Universiteit Eindhoven), Adriana Salerno (Bates College) and Benjamin Smith (INRIA Saclay–Ile-de-France). This turned out to provide a very nice mix of talks by senior and junior participants during the workshop.

There were also some productive discussions about large-scale computing after the lecture of Dan Bernstein, and some useful back-and-forth discussions between people using different flavors of *p*-adic cohomology for computations (e.g., David Harvey and John Voight).

André D. Bandrauk, lauréat du prix Marie-Victorin 2010

Le gouvernement du Québec a décerné cette année le prix Marie-Victorin a André D. Bandrauk, professeur titulaire au Département de chimie de l'Université de Sherbrooke, titulaire de la Chaire de recherche du Canada en chimie computationnelle et photonique moléculaire, et membre du CRM depuis 2001.

Le prix Marie-Victorin est la plus haute distinction attribuée par le gouvernement du Québec dans le domaine des sciences de la nature et du génie.

Le professeur André D. Bandrauk est un pionnier et un leader mondial dans le contrôle et la transformation de la matière par la technologie du laser ultrarapide. Ses travaux sur le comportement des molécules en interaction avec les champs lasers ont eu un impact majeur, ici comme ailleurs, sur les développements expérimentaux et théoriques en chimie et en physique. La qualité et l'envergure de ses travaux de recherche ont été largement reconnues par la communauté scientifique. Il a, entre autres, reçu le prix John C. Polanyi du Conseil de recherches en sciences naturelles et en génie du Canada, le prix Herzberg de la Société canadienne de spectroscopie et un doctorat honoris causa de l'Université libre de Berlin. Il est aussi membre titulaire de la Société royale du Canada et Fellow de l'American Association for Advancement of Science.

Thematic Semester in Group Theory

Organisers : Olga Kharlampovich (McGill University), Alexei G. Miasnikov (Stevens Institute of Technology), Benson Farb (University of Chicago), Luis Ribes (Carleton University), Mark Sapir (Vanderbilt University), and Efim Zelmanov (University of California, San Diego)

Workshop on Geometric, Asymptotic, Combinatorial Group Theory with Applications (GAGTA)
August 15–19, 2010
Organisers : O. Kharlampovich (McGill), M. Sapir (Vanderbilt), N. Touikan (McGill), E. Ventura (UPC)

The first workshop of the special semester on "Geometric, Combinatorial and Computational Group Theory" also happened to be the fourth in the GAGTA sequence of conferences (the previous ones were held in Manresa, Spain ; Dortmund, Germany ; and New Jersey, USA.) Because some of the participants of this workshop were also planning on attending the ICM in Goa, this workshop exceptionally started on a Sunday. This gathering was a big success : there 64 participants and many beautiful new results were given.

David Fisher and Mark Sapir gave mini-courses for this workshop. David Fisher, in his mini-course "Quasi-isometric rigidity," presented some of his joint work with Alex Eskin and Kevin Whyte and that of Irine Peng which gives a quasi-isometric classification of certain classes of virtually polycyclic groups. This result is one of the major recent breakthroughs in geometric group theory and has generated a lot of excitement. He sketched the proof and also indicated some of the obstacles to be overcome in order to make further generalizations.

Mark Sapir gave the second mini-course, which was called "Asymptotic cones of groups." Although the first application of asymptotic cones to geometric group theory was is Mikhail Gromov's celebrated theorem of groups of polynomial growth, Mark's treatment was geared towards the study of "non-positively curved" groups. He discussed their applications to Dehn Functions, divergence of geodesics, and to equations over groups. He also described the asymptotic cones of relatively hyperbolic groups and mapping class groups.

There were some very nice algorithmic results. Vincent Guirardel announced a proof of the isomorphism problem for rigid residually hyperbolic groups. Alexander Olshanskii presented a result which connected the space complexity of a group's word problem with some very natural and and well known group invariants. Enric Ventura gave some conditions which enable one to construct recursive presentations of Mihailova's subgroups, these are subgroups of the direct product of two free groups which are known to have undecidable membership problem, and as an application enabled the construction of new examples of groups with pathological properties.

There were also many new results in asymptotic group theory. Jason Behrstock discussed the quasi-isometric classification of 3-manifold groups, in particular we were shown a very simple description of the quasi-isometry classes of graph manifolds. Alexander Dranishnikov gave a presentation on dimension growth of groups, a notion related to asymptotic dimension and growth, and showed how it could be computed in some instances. He ended with an intriguing open question relating sub-exponential dimension growth and amenability. Daniel Groves showed some his recent work on understanding the sets of homomorphisms to mapping class groups, which ultimately should lead to an understanding of surface bundles. Gilbert Levitt presented a proof of finiteness properties of stabilizers of conjugacy classes of free groups and of point stabilizers of points on the boundary of Culler–Vogtmann outer space. Lewis Bowen exposed his remarkable result that a (finitely generated) free subgroup of a Lie group is, up to some small perturbations and passing to finite index subgroups, a subgroup of *any* co-compact lattice. Diane Vavrichek talked about some conditions for a subgroup to be essentially mapped to another subgroup via a quasi-isometry.

The lectures of Alex Lubotzky (Hebrew University) which took place during the workshop on Geometric, Asymptotic, Combinatorial Group Theory with Applications..

On the more combinatorial side of things we had a presentation by Tim Riley on his hydra groups, which are hugely distorted subgroups of surprisingly nice CAT(0), one relator, free-by-cyclic groups. Anton Klyatchko elaborated on some properties of groups obtained by adding one generator and a special types of relations to the presentation of a non-trivial group. Pascal Weil showed another very natural model of a "random subgroup" of a free group, this model is remarkable in how different the arising algebraic properties are compared to the standard random model. Mikhail Ershov introduced positive weighted deficiency and showed how this could be used to construct examples of residually finite groups whose every finitely generated subgroup is either finite index or finite.

Alexei Miasnikov gave a talk on large scale first order logic, a very general idea that applies to a multitude of structures, and discussed the large scale first order properties of Cayley graphs and of hyperbolic groups. Elena Aladova presented the notion of logical separability and presented an ambitious effort to give geometric interpretations to fundamental notions of model theory.

Alex Lubotzky wasn't the only person to discuss finite groups. Eugene Plotkin surveyed new characterizations of finite solvable groups, and Alina Vdovina presented a new family of expander graphs which come from finite groups with a very small number of generators and relations.

The cultural content of this workshop was also greatly enhanced by Marina Popova's presentation : "Abstract art and mathematics : at the crossroads." In her talk, Marina discussed abstract art, her work, and how mathematical imagery has been inspiring to her as of late. Four of her beautiful paintings were on display on the fifth floor of the CRM, and all the participants agreed that they added a special touch to the workshop.

Workshop on Topics in Algorithmic and Geometric Group and Semigroup Theory
August 23–27, 2010
Organisers : O. Kharlampovich (McGill), R. Gilman and A. Miasnikov (Stevens), B. Steinberg (Carleton), N. Touikan (McGill)

The second workshop of the thematic semester was a natural continuation of the first. There were two mini-courses. The first, given by Benjamin Steinberg, was called "Automata theory and algorithmic problems in groups." In this mini-course, Ben discussed the membership problems for subgroups, submonoids and rational subsets of groups. Ben taught us that automata are powerful tools that can also be used to simplify certain proofs in group theory.

The second mini-course called "Subgroup Membership Problem in limit groups" was given by Denis Serbin. He described infinite words, how they could be applied to the study of limit groups, and showed the Stallings foldings techniques used to solve many important algorithmic problems in limit groups.

Although there was on obvious overlap of interests between the first and second workshops of the thematic semester, the second one had a definitely different, perhaps more multi-dimensional, feel.

For example, there were many interesting talks about semigroups and inverse monoids, not-so-distant yet wildly different cousins of groups. Lev Shneerson, John Meakin and Mark Kambites gave talks that involved techniques of combinatorial and geometric group theory applied to monoids and semigroups, which showed the similarities between the fields, but also made plain the fact that some things are just a lot harder (but still fun) to do without inversions. Jorge Almeida and Alfredo Costa discussed the symbolic dynamics aspect of semigroups.

Another "group" of people that were under represented in the previous workshop were the pro-p group theorists. Luis Ribes gave a very nice survey of virtually free pro-p groups, and Pavel Zalesski presented an ongoing effort to develop a theory of pro-p limit groups that parallels the theory of limit groups over free groups. Said Sidki also gave two lectures on the automorphism groups of rooted trees, a topic which is deeply connected to profinite group theory.

There was also an interesting pair of talks. The first one, given by Gilbert Baumslag, discussed how limited our knowledge of one relator groups still is and quite eloquently decried the tyranny of geometry in contemporary infinite group theory. The other, by Dani Wise, discussed his recent work (which uses geometric methods) on quasiconvex hierarchies that gives a positive solutions to a conjecture of Baumslag's about one relator groups. The two of them had memorable exchanges.

Algebraists were also represented, Helen Bunina spoke about isomorphisms and elementary equivalence of Chevalley groups, Ekaterina Blagoveshchenskaya discussed recent advances in the theory of torsion free abelian groups, and Alexanders A. and V. Mikhalevs discussed general problems about algebras. Alexei Miasnikov also gave a talk on how a more algebraic/model theoretic approach could be used to solve the problem of Krull dimensions for limits of groups.

Olga Kharlampovich, Nicholas Touikan, Andrei Nikolaev and Elizaveta Frenkel gave presentations about various algorithmic properties of certain classes of non-positively curved and free groups, whereas Alexandre V. Borovik discussed black box groups.

There was also more to this workshop than merely mathematics presentations. At the end of the second day, there was a philosophical debate proposed by Alexander Borovik entitled : "Can we save mathematics from mathematicians ?" Unfortunately, no clear consensus was formed on this question.... There was a consensus, however, that the picnic on Wednesday evening by Lac des Castors was a lot of fun.

To close the workshop, we were treated to another presentation by the artist Marina Popova, which was followed by a very interesting discussion on the role of aesthetics in mathematics and an exploration of the strange connection between kitsch and the notion of infinity.

Workshop on Complexity and Group-Based Cryptography
August 30–September 3, 2010
Organisers : R. Gilman & A. Miasnikov (Stevens), V. Shpilrain (CCNY), A. Ushakov (Stevens)

Building a solid mathematical foundation for the use of infinite groups in cryptography inevitably involves operating with various asymptotic and statistical aspects of infinite groups, and this is where modern group theory finds its important applica-

tions. In this workshop we explored "non-commutative ideas" in cryptography We payed particular attention to what can be called group-based cryptography, i.e., cryptography that uses non-commutative group theory one way or another.

There is a remarkable feedback from cryptography to combinatorial group theory because some of the problems motivated by cryptography appear to be new to group theory, and they open many interesting research avenues within group theory. We employ complexity theory, notably generic-case complexity of algorithms, for cryptanalysis of various cryptographic protocols based on infinite groups. We also use the ideas and machinery from the theory of generic-case complexity to study asymptotically dominant properties of some infinite groups that have been used in public key cryptography so far. It turns out that for a relevant cryptographic scheme to be secure, it is essential that keys are selected from a "very small" (relative to the whole group, say) subset rather than from the whole group. Detecting these subsets ("black holes") for a particular cryptographic scheme is usually a very challenging problem, but it holds the key to creating secure cryptographic primitives based on infinite non-commutative groups.

Our workshop gathered together about 40 mathematicians from Australia, Canada, France, Germany, Israel, UK, USA, Russia and Spain. It featured two mini-courses : one by Bob Gilman and Alexei Miasnikov on algorithmic group theory and the other by Vladimir Shpilrain and Alexander Ushakov on group-based cryptography.

Workshop on Group Actions and Dynamics
October 4–8, 2010
Organisers : O. Kharlampovich (McGill), A. Miasnikov (Stevens), D. Serbin (Genève)

The main goal of the workshop was, first of all, to introduce major directions in Geometric Group Theory, which is now all about group actions on various spaces, in a manner accessible to graduate students working in the field, and to show some recent advancements in these directions. In our opinion, this goal was successfully reached and we would like to thank all the participants for their contributions to the unique atmosphere of the meeting.

One of the major topics discussed in the workshop was self-similar and branch groups. An introduction to the topic was given by Volodymyr Nekrashevych in his mini-course, where he defined self-similar and branch groups as groups of automorphisms of rooted trees (first lecture). The second and third lectures were devoted to iterated monodromy groups which can be viewed as a subclass of self-similar groups, their connections with complex dynamics, and recent results on their properties.

Besides the mini-course, there were several talks on groups of automorphisms of rooted trees given by recognized specialists in this field. First of all, the talk of Rostislav Grigorchuk about actions of self-similar groups on the boundaries of the corresponding rooted trees and dynamics related to Schreier graphs of level stabilizers. As a continuation of Grigorchuk's talk, one can consider the presentation of Tatiana Smirnova–Nagnibeda about asymptotical properties of group actions on rooted trees, and the talk by Zoran Sunic about Hanoi Tower group, which is a particular example of a group acting on a rooted tree.

Another mini-course of the workshop was given by Mladen Bestvina on the topology and geometry of outer space, which can be defined as a space of marked metric graphs modulo equivalence of markings by graph isometries. This space naturally arises in the study of automorphisms of free groups and now this is a classical topic in Geometric Group Theory.

The third mini-course given by Denis Osin was devoted to a generalization of relative hyperbolicity based on the notion of hyperbolically embedded subgroups. In the course of lectures, it became obvious that this generalization is proper in the sense that it makes it possible to prove results using hyperbolic techniques in many groups which are not relatively hyperbolic to any reasonable subgroups and it was stressed by the speaker that a substantial part of the theory of relatively hyperbolic groups can now be generalized in the new context.

Actions on various "nice" spaces was always an effective way to study structural properties of the underlying groups. From this perspective one can consider, for example, the talk by Olga Kharlampovich on the structure of Λ-free groups and the talk of Montserrat Casals-Ruiz about limit groups of partially commutative groups. In the former case the underlying group acts freely on a Λ-tree, while in the latter case there is a faithful action on an asymptotic cone of a partially commutative group. Other talks implicitly incorporating the approach to the structure by means of actions include the presentations of François Dahmani on interval-exchange groups and of Indira Chatterji on groups acting on median spaces.

Some results on ergodic properties of groups were presented in the talk of Vadim Kaimanovich on the Hopf decomposition of the boundary action of a discrete group and the talk of Denis Serbin on the description of Poisson boundaries of $\mathbb{Z}^n$-free groups.

The diversity of the talks given in the workshop was not restricted by the directions outlined above, as the theory of group actions in its current state is extremely rich. For example, the talks by Lisa Carbone on symmetries of infinite dimensional Lie groups, of Tullia Dymarz on bilipschitz vs. quasi-isometric equivalence for finitely generated groups, of Vladimir Trofimov on vertex-transitive groups of automorphisms of graphs, and of Pedro Silva on fixed points of endomorphisms made it possible to not only get familiar with the topics discussed but to see various faces of the field.

(*continued on page* 16)

Advanced School in Quantum Information Processing and Quantum Cryptography

by Alain Tapp (Université de Montréal)

The 2010 Séminaire de mathématiques supérieures NATO Advanced School in Quantum Information Processing and Quantum Cryptography took place at the CRM from June 21 to July 2, 2010. It was organised by Alain Tapp (Université de Montréal) in collaboration with Julia Kempe (Tel Aviv University), Daniel Gottesman (Perimeter Institute for Theoretical Physics) and Christiane Rousseau (Université de Montréal). The SMS was made possible by generous contribution of NATO, INstitute for Transdisciplinary Research In Quantum computing (INTRIQ) and CRM.

Quantum information processing (QIP), including quantum cryptography, quantum information, quantum computation and aspect of foundations of quantum mechanics, is a relatively new interdisciplinary science that mostly studies the impact of quantum mechanics on our ability to process information and vice versa. The influence of QIP on physics and computer science is important and growing. In cryptography, QIP seeded a revolution. Cryptography deals primarily with secure interaction between entities, including, for example, private communications, message authentication, electronic signature, secure electronic voting and many other tasks. In that field two world-changing breakthroughs have been obtained. The first major result, obtained by Bennett and Brassard (one of the speakers) in 1984, was a protocol for secure communications known as BB84 quantum key distribution.The security of the protocol is based only on the correctness of the laws of physics ! Quantum cryptography has been tested in dozens of laboratories around the world and four companies actually offer products. Another potentially life-changing discovery in the field was obtained by Shor in 1995. He discovered an efficient technique for factoring very large numbers and another one for computing the discrete logarithm. These algorithms, when successfully implemented on a quantum computer, will render useless nearly all techniques currently used to provide private communication, electronic signatures and secure transactions on the Internet (RSA, Diffi Hellman, etc.). Until recently, practical implementation seemed out of reach. The recent progress on the experimental side make it a priority to be ready with alternative techniques in a near future. With that objective in mind, a new field called post quantum cryptography was born in 2006 that focuses on that problem.

Today, hundreds of scientists in mathematics, computer science, physics and engineering are contributing to research in the field and have interests that range from experimental physics, algorithms, information theory, complexity theory, communication theory, error correction, simulations and foundation of physics. The two-week advanced school has covered a variety of topics that were presented by major international researchers at the heart of those fields : Scott Aaronson (MIT) lectured on “Quantum complexity theory" ; Gilles Brassard (Montréal) lectured on “Non QKD cryptography" ; Richard Cleve (Waterloo) lectured on “Quantum non-locality and communication complexity" ; Daniel Gottesman (Perimeter Institute) lectured on “Proving the threshold theorem for fault-tolerant quantum computation" ; Patrick Hayden (McGill) lectured on “Decoupling : a building block for quantum information theory" ; Raymond Laflamme (Perimter Institute and Waterloo) lectured on “NMR quantum computer" ; Renato Renner (ETH Zürich) lectured on “Security proofs in quantum cryptography" ; Barry Sanders (Calgary) lectured on “Implementations of quantum information" ; Miklos Santha (Paris-Sud) lectured on “Quantum walks and algorithms" ; Alain Tapp (Montréal) lectured on “Quantum algorithms and the mathematics of quantum information processing" ; Barbara Terhal (IBM) lectured on “Hamiltonian problems in quantum complexity" ; John Watrous (Waterloo) lectured on “Zero-knowledge proofs" ; Ronald de Wolf (CWI) lectured on “Quantum computing as a proof tool" ; Stefan Wolf (ETH Zurich) lectured on “Device independent cryptography.”

More than 60 people attended the 2010 edition of the SMS and its great success was mostly due to the outstanding quality of the speakers.

Lectures at the Leading Edge

(*continued from page* 4)

which under the assumption that a certain infinite family of finite quotients of Γ being expanders gives sufficient conditions for $Y \subset \Gamma$ to exponentially small.

This basic theorem is then applied to the problem of powers in linear groups, where Lubotzky announced the following remarkable theorem (a joint result with Meiri) : if Γ is a finitely generated subgroup of $GL_d(\mathbb{C})$ that is not virtually solvable, then the set

$$Y = \{g \in \Gamma \mid \exists m \geq 2, x \in \Gamma \text{ s.t. } g = x^m\}$$

of all proper powers of Γ is exponentially small. In particular, Y does not contain any subgroup of finite order. This result contrasts with Malcev’s 1960s result that for any finitely generated nilpotent group, for all m, the set of mth powers contains finite index subgroup.

Other applications of this basic theorem were the exponential growth of the number of conjugacy classes in linear finitely generated non-virtually-solvable groups and the exponential smallness of the set of non-pseudo-Anosov mapping classes in the Torelli subgroups of mapping class groups.

La table ronde du rcm$_2$ sur le thème « Le développement durable et le rôle des scientifiques »

par Christiane Rousseau (Université de Montréal)

Cette table ronde fait partie du volet grand public du programme nord-américain sur les changements climatiques et le développement durable en 2010-2011 :

`http://www.crm.umontreal.ca/Climat2010/index.php`

Elle clôturait l'atelier « Théorie de la décision et développement durable », organisé conjointement par le CRM et le GERAD, l'organisateur principal étant Georges Zaccour du GERAD.

En effet, d'une part, les changements climatiques et le développement durable sont des enjeux qui interpellent les scientifiques. D'autre part, ces enjeux sont la source de problématiques de recherche dans lesquelles les mathématiques sont appelées à jouer un rôle essentiel.

Au niveau nord-américain, le CRM fait partie du regroupement d'instituts qui a initié ce programme. Au niveau québécois, le CRM travaille en partenariat avec d'autres centres de recherche en sciences mathématiques regroupés en réseau : le *réseau rcm$_2$ de calcul et modélisation mathématique* (`www.rcm2.ca`). Ce réseau regroupe le CIRANO (centre interuniversitaire de recherche en analyse des organisations, `www.cirano.ca`), le CIRRELT (Centre interuniversitaire de recherche sur les réseaux d'entreprise, la logistique et le transport, `www.cirrelt.ca`), le CRM, le GERAD (Groupe d'études et de recherche en analyse des décisions, `ww.gerad.ca`) et l'INRS-ÉMT (Institut national de la recherche scientifique, énergie, matériaux, technologie, `www.emt.inrs.ca`)

Les panélistes invités étaient Jean-Pierre Aubin, le fondateur de la théorie de la viabilité, Jean-Pierre Blanchet, professeur en sciences de la Terre et de l'atmosphère à l'UQÀM et chercheur au centre ESCER pour l'étude et la modélisation du climat à l'échelle régionale, et Graciela Chichilnisky de l'Université Columbia, qui a, entre autres, créé la théorie formelle du développement durable et est l'auteure de la bourse du carbone du protocole de Kyoto. La table ronde était animée par Sophie-Andrée Blondin de Radio-Canada. La discussion a été animée et haute en couleurs. Les deux panélistes de formation mathématique, Jean-Pierre Aubin et Graciela Chichilnisky, ont fortement critiqué la passivité des mathématiques qui ne s'adaptent pas suffisamment aux problèmes d'aujourd'hui et de demain.

Graciela Chichilnisky a expliqué que les mathématiques sont en train de mourir parce qu'elles ont divorcé des applications. La survie de la race humaine est liée au développement durable. Les mathématiques actuelles n'ont pas les outils pour traiter les problèmes de décision dans ce contexte. En effet, les outils probabilistes et statistiques actuels ne sont pas adéquats pour gérer le risque relié aux phénomènes extrêmes, mais de petite probabilité : ils leur accordent systématiquement une probabilité trop faible, introduisant ainsi un biais contre le futur. Les mathématiques se développent parce qu'on pose de nouvelles questions — les questions sont plus importantes que les réponses — et pourtant nous, mathématiciens, semblons plus répondre aux questions du passé qu'en poser de nouvelles.

Jean-Pierre Aubin a renchéri. Il a insisté sur le fait que les mathématiques doivent se renouveler pour pouvoir espérer traiter adéquatement des enjeux du développement durable. Entre les mathématiques pures et les mathématiques appliquées il manque les mathématiques « motivées ». Mais ce processus de renouvellement prend du temps, et il est dangereux de donner une caution mathématique à des études qui auraient mal évalué les risques. Ceci se produit lorsqu'on prend une théorie mathématique et qu'on l'applique dans un autre champ plutôt que de développer la théorie dont ce champ a besoin. Il est beaucoup plus long de forger de nouveaux outils que de les utiliser, et rien n'est fait pour encourager cette démarche de fond.

Jean-Pierre Blanchet a insisté sur la nécesité de changer de paradigme. Il faut recentrer la société et son mode de fonctionnement sur la conservation de l'environnement et, au niveau scientifique, rapprocher les sciences et mettre l'emphase sur la recherche inter-disciplinaire. Il a insisté sur le défi du dialogue et de l'intégration pour pouvoir agir.

Dans la même veine, Graciela Chichilnisky a fait remarquer que ce sont les physiciens qui mesurent les changements climatiques dont les causes sont sociales…, ce sur quoi Jean-Pierre Aubin a renchéri en parlant de la boîte noire entre les causes et les effets. Jean-Pierre Blanchet a insisté sur la nécessité, pour les scientifiques, de maintenir une intuition physique lorsqu'ils travaillent avec des modèles mathématiques très abstraits qui doivent représenter le plus fidèlement possible le comportement des fluides atmosphériques et océaniques.

Graciela Chichilnisky a insisté sur l'urgence d'agir par une comparaison choc. Nous avons tous une assurance maison ou une assurance auto, même si nous sommes dans l'incertitude, et qu'il est fort probable que cette assurance soit inutile. Nous sommes dans la quasi-certitude que des changements climatiques sont en cours, et seulement dans l'incertitude sur l'ampleur et leurs effets. Pourquoi attendons-nous d'avoir des certitudes avant de nous munir d'une « police d'assurance » contre ces changements ? Attendons-nous de rejoindre les 99,9% des espèces qui sont déjà éteintes ? Elle a terminé son intervention en lançant une invitation aux personnes dans la salle à s'impliquer dans la défense du développement durable.

(*suite à la page* 16)

Latest CRM Publications

Monoidal Functors, Species and Hopf Algebras
M. Aguiar (TAMU), S. Mahajan (IIT Bombay)
CRM Monograph Series, volume 29

This research monograph integrates ideas from category theory, algebra and combinatorics. It is organised in three parts.

Part I belongs to the realm of category theory. It reviews some of the foundational work of Bénabou, Eilenberg, Kelly and Mac Lane on monoidal categories and of Joyal and Street on braided monoidal categories, and proceeds to study higher monoidal categories and higher monoidal functors. Special attention is devoted to the notion of a bilax monoidal functor which plays a central role in this work.

Combinatorics and geometry are the theme of Part II. Joyal's species constitute a good framework for the study of algebraic structures associated to combinatorial objects. This part discusses the category of species focusing particularly on the Hopf monoids therein. The notion of a Hopf monoid in species parallels that of a Hopf algebra and reflects the manner in which combinatorial structures compose and decompose. Numerous examples of Hopf monoids are given in the text. These are constructed from combinatorial and geometric data and inspired by ideas of Rota and Tits' theory of Coxeter complexes.

Part III is of an algebraic nature and shows how ideas in Parts I and II lead to a unified approach to Hopf algebras. The main step is the construction of Fock functors from species to graded vector spaces. These functors are bilax monoidal and thus translate Hopf monoids in species to graded Hopf algebras. This functorial construction of Hopf algebras encompasses both quantum groups and the Hopf algebras of recent prominence in the combinatorics literature.

The monograph opens a vast new area of research. It is written with clarity and sufficient detail to make it accessible to advanced graduate students.

Hilbert Spaces of Analytic Functions
J. Mashreghi & T. Ransford (Laval), K. Seip (NTNU), editors
CRM Proceedings & Lecture Notes, volume 51

Hilbert spaces of analytic functions are currently a very active field of complex analysis. The Hardy space is the most senior member of this family. However, other classes of analytic functions such as the classical Bergman space, the Dirichlet space, the de Branges–Rovnyak spaces, and various spaces of entire functions, have been extensively studied. These spaces have been exploited in different fields of mathematics and also in physics and engineering. For example, de Branges used them to solve the Bieberbach conjecture. Modern control theory is another place that heavily exploits the techniques of analytic function theory. This book grew out of a workshop held in December 2008 at the CRM in Montréal and provides an account of the latest developments in the field of analytic function theory.

Spectrum and Dynamics
D. Jakobson (McGill), S. Nonnenmacher (CEA-Saclay),
I. Polterovich (Montréal), editors
CRM Proceedings & Lecture Notes, volume 52

This volume contains a collection of papers presented at the workshop on Spectrum and Dynamics held at the CRM in April 2008. In recent years, many new exciting connections have been established between the spectral theory of elliptic operators and the theory of dynamical systems. A number of articles in the proceedings highlight these discoveries. The volume features a diversity of topics, such as quantum chaos, spectral geometry, semiclassical analysis, number theory and ergodic theory. Apart from the research papers aimed at the experts, this book includes several survey articles accessible to a broad mathematical audience.

Christiane Rousseau élue vice-présidente de l'IMU

M^{me} Christiane Rousseau a été élue vice-présidente de l'International Mathematical Union (IMU) pour la période de 2011 à 2014 lors de la réunion annuelle récente de leur assemblée générale. C'est la première fois qu'un chercheur du Canada occupe ce poste.

Christiane Rousseau est une chercheuse mondialement reconnue dans le domaine des systèmes dynamiques. En 1977, elle a obtenu son doctorat de l'Université de Montréal où elle est professeure de mathématiques. Elle a assumé la direction du Département de mathématiques et statistiques de 1993 à 1997. Elle devient vice-présidente de la Société mathématique du Canada (SMC) de 1995 à 1997, puis présidente de 2002 à 2004.

Elle a organisé ou coorganisé plusieurs événements majeurs sur la scène mathématique canadienne, dont le forum canadien en enseignement des mathématiques en 2003, les congrès Canada-France de 2004 (Toulouse) et 2008 (Montréal) et à 2 reprises, la candidature (infructueuse) du Canada pour le Congrès International des mathématiciens. Elle a été invitée à donner une conférence régulière au Congrès international de l'enseignement mathématique en juillet 2008.

Christiane a assumé la direction du Centre de recherches mathématiques en 2008-2009. Elle siège présentement à la direction d'un comité international qui coordonne les activités d'une liste grandissante d'instituts mathématiques à travers le monde pour une année « Mathématiques de la planète terre 2013 ».

Finalement, en guise de reconnaissance pour ses contributions importantes et soutenues à la communauté mathématique canadienne, en 2009, la SMC a remis le prix Graham Wright à Christiane pour service méritoire.

News from the CRM Laboratories

CICMA Laboratory in Algebra and Number Theory

For CICMA, the 2010-11 academic year will be one of renewal and growth, with the permanent arrival of three new members (Matilde Lalin at Université de Montréal, and Jayce Getz and Heekyoung Hahn at McGill). CICMA will also be hosting three postdoctoral fellows for the year (Fritz Hoermann, Dimitris Koukoulopoulos, and Ethan Smith) and two other postdocs for shorter periods: Shabnam Akhtari (NSERC fellowship) from March to August, and Xavier Guitart (supported by his home institution in Barcelona) from September to January. In addition, CICMA will be hosting numerous visitors for periods of at least a month, such as Fabrizio Andreatta, Adam Logan, and Victor Rotger. The Quebec-Vermont Number Theory Seminar will enter its 26th consecutive year of uninterrupted running, making it one of the oldest seminars of its kind in North America. Speakers this year include Manjul Bhargava, Chandrasekhar Khare, and Joseph Silverman. In addition to the biweekly seminar, CICMA is organising the first of what will become a biannual weekend conference run jointly by Montréal and Toronto and alternating between these two cities. Other activities will include the annual Québec-Maine conference to be held this year in Québec City, and the annual Bellairs Conference that will take place in the first week of May in Barbados.

Laboratoire de statistique

En 2010-2011, les membres du laboratoire de statistique du CRM seront activement impliqués dans l'organisation du semestre thématique en statistique qui aura lieu au CRM de janvier à mai 2011, voir `http://www.crm.umontreal.ca/Stat2011/`. Les activités principales seront les six ateliers suivants : en janvier 2011, « Méthodes statistiques en météorologie et changement climatique », organisé par Jean-François Angers (Montréal), Anne-Catherine Favre (Laval), Reinhard Furrer (Zürich), Philippe Naveau (Laboratoire des sciences du climat et de l'environnement, France), Doug Nychka (NCAR), Luc Perreault (Institut de recherche d'Hydro-Québec), Richard L. Smith (North Carolina), Claudia Tebaldi (UBC), Han von Storch (Hamburg), et Francis Zwiers (Environnement Canada) ; en avril 2011, « Méthodes statistiques computationnelles en génomique et en biologie systémique » organisé par Sandrine Dudoit (UC Berkeley), Raphael Gottardo (IRCM), Jinko Graham (SFU), Aurélie Labbe (McGill) et Francis Larribe (UQÀM) ; en mai 2011, "Problèmes statistiques en gestion forestiére," organisé par Pierre Bernier (Service canadien des forêts, Ressources Naturelles Canada), Valerie LeMay (UBC), Eliot McIntire (Laval), Ron McRoberts (USDA Forest Service), Jean Opsomer (Colorado State), Frédéric Raulier (Laval), Louis-Paul Rivest (Laval), Erkki O. Tomppo (Finish Forest Research Institute), Chhun-Huor Ung (Service canadien des forêts, Ressources Naturelles Canada) ; en mai 2011, « L'inférence causale en recherche sur la santé », organisé par Jennifer Hill (New York), Jay S. Kaufman (McGill), Lawrence McCandless (Simon Fraser), Erica E. M. Moodie (McGill), Robert Platt (McGill) et Bryan E. Shepherd (Vanderbilt) ; en mai 2011, « Analyse des durées de vie et données historiques d'événements » organisé par Richard Cook (Waterloo) et Jerry Lawless (Waterloo) ; et en juin 2011, "Modélisation de la dépendance et les copules" organisé par Debbie Dupuis (HEC), Christian Genest (Laval), Johanna Neslehová (McGill), Jean-François Plante (HEC), Jean-François Quessy (UQTR) et Bruno Rémillard (HEC).

Un autre atelier sur le traitement des données manquantes organisé par R. Steele (McGill) aura lieu en octobre 2010, et la 5^{e} Conference Canadienne en Statistique Appliquée, organiseée par Yogendra Chaubey (Concordia) aura lieu a l'université Concordia en juillet 2011.

Le laboratoire de statistique accueillera en 2010-2011 six nouveaux chercheurs post-doctoraux, soient Elif Fidan Acar (McGill), supervisé par C. Genest ; Vahid Partovi Nia (McGill) supervisé par D. Stephens ; Olli Saarela (McGill) supervisé par E. Moodie et D. Stephens ; Eric Ngoussou (HEC) supervisé par D. Dupuis ; Vahid Partovi Nia (McGill) supervisé par M. Asgarian et D. Stephens, et finalement André Caron (Laval) supervisé par T. Duchesne et Vincent Fradette.

CIRGET–Centre interuniversitaire de recherches en géometrie et topologie

CIRGET welcomes seven new postdoctoral fellows this year: Adam Clay (Ph.D. 2010, UBC), Roman Golovko (Ph.D. 2009, University of Southern California), Clément Hyvrier (Ph.D. 2008, Université de Montréal), Nabil Kahouadji (Ph.D. 2009, Paris VII), Sungmo Kang (Ph.D. 2009, University of Texas at Austin), Frédéric Palési (Ph.D. 2009, Université Joseph Fourier) and Eric Harper (Ph.D. 2010, University of Miami). Scientifically, it shall be a busy year for CIRGET. In addition to the three weekly seminar series and several working groups, CIRGET members are involved in the organisation of two workshops. The first, organised by Virginie Charette and others, is entitled the Colloquium on Surfaces and Representations. It shall be held at the Université de Sherbrooke October 6–9 as part of the Rencontres universitaires Sherbrooke-Montpellier. The main theme of the Colloquium is the interaction between the geometry and the topology of surfaces and the representation theory of algebras, particularly in the area of cluster algebras. In June 2011, a five-day workshop on Moving Frames in Geometry shall be held at the CRM, organised by Niky Kamran and postdoctoral fellows Abraham Smith and Francis Valiquette. In the recent past, relatively few specialized conferences or workshops have been dedicated to this subject, but there is now a larger community of young researchers using moving frames and related techniques to make significant progress on a wide variety of problems in differential geometry and the geometry of differential equations.

INTRIQ—INstitute for Transdisciplinary Research In Quantum computing

The INstitute for Transdisciplinary Research In Quantum computing (INTRIQ) regroups researchers in quantum information processing coming from physics, computer science and engineering. The institute has 23 members coming for McGill, Université de Montréal, École Polytechnique Montréal and Université de Sherbrooke. The year 2009-2010 was excellent for INTRIQ. Firstly, University of Sherbrooke received a NSERC–CERC chair in quantum information and we are now very pleased to count Bertrand Reulet amongst our members. Also, Gilles Brassard won the Gerhard Herzberg Canada Gold Medal for Science and Engineering and Alexandre Blais won the NSERC E.W.R. Steacie Memorial Fellowship. Since June 2010, Alain Tapp has been appointed director and it is in this context that the institute applies for FQRNT regroupement stratégique renewal.

This year, two biannual meetings were held in Saint-Sauveur in June and in Sherbrooke in September. INTRIQ also started in January 2010 a special yearly conference where only the students and postdoc can attend and give a talk. We think that the event was very useful for the students as it helped them to get acquainted with each other, and it was also a good opportunity for them to get experience as a speaker in a less stressful context. It was a successful experiment that should happen again in early 2011 in addition to the biannual meetings. In June 2010, INTRIQ was involved financially and through Alain Tapp (as main organiser) with the SMS Summer School of the CRM. The SMS was sponsored by NATO and was a great success, thanks to the 14 outstanding speakers and the more than 60 participants coming from all around the world.

Thematic Semester in Group Theory

(*continued from page* 11)

Workshop on Equations and First-order Properties in Groups
October 11–15, 2010
Organisers: O. Kharlampovich (McGill), A. Miasnikov (Stevens), I. Kazachkov (McGill), V. Remeslennikov (Omsk)

Hilbert's 10th problem asks if there exists an algorithm to solve a Diophantine problem, i.e., to decide whether or not an equation with integer coefficients has an integer solution. This type of problem can be posed for arbitrary structures (rings, groups, etc.) and in a more general setting from the viewpoint of model theory (decidability of the universal/positive/elementary theory of a structure).

In the case of free groups, a famous problem posed by Tarski around 1945, and recently solved by Kharlampovich–Miasnikov and Sela, is to understand their elementary theory. The theory developed over the years to solve Tarski's problem has uncovered deep connections between model theory, geometry and group theory. The study of first-order theories is closely related to the study of algebraic varieties and their projections. The workshop centered around methods and techniques in algebraic geometry over groups and other algebraic systems, and gathered together about 40 mathematicians from Australia, Canada, France, Germany, Israel, UK, USA, Russia and Spain. It featured two minicourses: one by Olga Kharlampovich and Alexei Miasnikov on algebraic theory of equations in free groups and the other by Nikolai Romanovskii on algebraic geometry over soluble groups. The theme of equations in groups was further expanded in the talks of Volker Diekert, Igor Lysenok and Henry Wilton.

Another major theme of the conference was the so-called universal algebraic geometry. Recent progress in algebraic geometry over groups instigated a body of research aiming to carry over the results and techniques from classical algebraic geometry and algebraic geometry over groups to arbitrary algebraic structures using the language of universal algebra, hence the name—universal algebraic geometry. We had two talks on the subject given by the founders of universal algebraic geometry: Boris Plotkin and Vladimir Remeslennikov. Further, Montserrat Casals-Ruiz presented her results on universal completions of algebraic structures—a construction that plays the role of the ultrapower for the universal theory of a structure.

Finally, we had several talks on first-order properties of groups. In his talk, Mahmood Sohrabi presented a very fine classification of groups elementarily equivalent to a finitely generated nilpotent group. In their talks, Chloé Perin and Abdezerak Ould Houcine presented two independent proofs of the homogeneity of the free group, i.e., they showed that if two tuples of elements from the free group have the same type, then they are conjugate by an automorphism.

The conference was nicely complemented by a series of lectures of the Aisenstadt Chair Alexander Razborov, who among other things is well-known for his work in the theory of equations in free groups.

La table ronde du rcm$_2$

(*suite de la page* 13)

La discussion s'est poursuivi avec la salle sur différentes questions : optimisme versus pessimisme, suivant la manière dont on classe les enjeux climatiques parmi les enjeux planétaires ; nécessité d'alerter le public et les jeunes aux défis des changements climatiques ; comment éviter le dérapage du GIEC et comment expliquer le *Climate gate* ; comment communiquer avec les politiciens ; et surtout comment réformer la recherche scientifique (nouveaux outils, nouvelles problématiques, nouvelle génération de chercheurs inter-disciplinaires) pour qu'elle s'arrime adéquatement à ces nouveaux défis.

Word of the Director

I take this opportunity to say a few words on the highlights of recent and upcoming scientific events at the CRM, and at the same time to discuss a few issues of a more organizational or administrative nature.

As always, the theme semesters or years are the core of the CRM's scientific activities. The semester on Geometric, Combinatorial and Computational Group theory took place in the summer and fall with five workshops and three Aisenstadt lecturers, Yuri Gurevich, Angus MacIntyre and Alexander Razborov. Two previous Aisenstadt lecturers participating in the theme semester, Alex Lubotzky and Efim Zelmanov, were invited to give series of "lectures at the leading edge." In another first a small and well received art exhibition was organized, four large paintings by Marina Popova with mathematical themes were exhibited outside the CRM offices. One of them had provided the background for the colorfull theme semester poster. The next two thematic activities are a semester in Statistics this winter and spring and a semester in Quantum Information next summer and fall. Preliminary proposals for a semester in Analysis (coming out of the Analysis laboratory) for spring and summer 2012 and a year in Geometry-Topology (coming out of CIRGET) for fall 2012/spring 2013 were considerably advanced during the past year and received approval by our International Scientific Advisory Committee at its meeting in October. Other theme proposals for 2013 are expected to develop out the activities of the year of Mathematics of Planet Earth (MPE 2013, `www.mpe2013.org`). Under the leadership of former CRM director Christiane Rousseau this project has become truly planet wide in scope.

The Séminaire de Mathématiques Supérieures (SMS) this year held an advanced summer school in Quantum Information Processing and Quantum Cryptography, for which it was able to secure support by NATO. This prestigious school will celebrate its 50th anniversary next summer with a school on Metric Measure Spaces. (This will also be an early event in the theme semester in Analysis planned for the first half of 2012.) We were fortunate that Octav Cornea from Université de Montréal has agreed to serve as director of SMS for the coming four years. NATO support, on which the school relied heavily in the past, has become more and more difficult to obtain. The new director has succeeded in finding broader sources of financing and in particular to secure the participation of the Fields Institute and of the Pacific Institute of Mathematical Sciences (PIMS). This is a promising development for the SMS.

The Open House of the North American institutes in the mathematical sciences is a recurring event at the winter meetings of the AMS. The CRM and other Canadian institutes are regular participants. Interestingly, the yearly meeting of institute directors taking place there is developing into an informal framework to coordinate collaboration between the institutes. At the San Francisco meeting a year in Climate Change and Sustainable Development (CCSD, `www.mathinstitutes.org/climate-initiative`) was agreed to as a joint activity in 2010/2011. Two activities under these auspices already took place at the CRM, and two more are scheduled in the spring and fall of 2011. (For details see the CRM website.) The CRM also designed the striking poster advertising this joint effort. Another important topic, to come up again at the New Orleans meeting, was plans for MPE 2013.

A Grande Conférence in the CRM series of lectures aimed at a general public was given by recent Fields medalist Cédric Villani in November. Earlier the Grandes Conférences tried out a very interesting new format by organizing a public round table discussion on "Le Développement durable et le rôle des scientifiques" as another contribution to the CCSD initiative.

The Canadian Mathematics Institutes are presently funded by NSERC under the Major Resources Support (MRS) envelope. The future of the MRS program being much under discussion at NSERC, the institute directors were very concerned about having to renew their NSERC grants, all expiring in March 2013, within the present envelope. They had a very productive meeting on this with the President of NSERC which led to the establishment, with the participation and support of NSERC, of a Long Range Planning Committee by the Canadian community in the mathematical sciences (pure mathematics, applied mathematics, statistics). It is, among other tasks, to provide a blueprint for the allocation of NSERC resources in the mathematical sciences in the future. Since these deliberations are expected to take time, NSERC agreed to extend the existing institute grants by one year. For the moment this takes some of the anxiety out of the grant renewal process.

A quite unique feature of the CRM is provided by its affiliated laboratories. These are centres of research of their own (there now are 10) in specialized areas of the mathematical sciences

(*continued on page* 19)

Ateliers / Workshops

Atelier INSDC
Méthodes statistiques pour données géographiques et spatiales dans la gestion des ressources naturelles
CRM, 3 au 5 mars 2010
Organisateurs : DongMei Chen (Université Queen's), Thierry Duchesne et Anne-Catherine Favre (Université Laval) et Subhash R. Lele (Université de l'Alberta)

Cet atelier a été conçu suite à un appel fait par l'Institut national sur les structures de données complexes (INSDC). Il s'agit d'un atelier inaugural dont l'objectif est de réunir des étudiants, stagiaires et chercheurs des milieux académique et industriel ayant des intérêts de recherche liés à l'application de méthodes statistiques pour l'analyse de données géographiques et/ou spatiales aux problèmes liés à la gestion des ressources naturelles. L'atelier a eu lieu au Centre de recherches mathématiques (CRM) et a attiré 67 participants. Le support financier de l'INSDC a permis d'attirer plusieurs conférenciers de l'extérieur du Québec, incluant en outre une forte délégation de conférenciers français ainsi que plusieurs participants des Etats-Unis et de l'ouest canadien. L'atelier était divisé en deux parties : les exposés scientifiques (jours 1 et 2) et une période de discussion sur les opportunités de financement ainsi que des échanges en petits groupes de chercheurs ayant des intérêts de recherche communs (jour 3). Les 13 exposés du jour 1 (2 de 50 minutes, 6 de 30 minutes et 5 de 20 minutes) portaient tous sur des sujets liés au sous-thème "hydrologie, météorologie, climatologie." On y a discuté de modèles spatiaux de dispersion de l'ozone (Zidek), de méthodes d'interpolation spatiale des mesures de précipitations (Fortin, Carreau, Tapsoba, Fortier-Filion), de modélisation d'événements climatiques extrêmes (Naveau, Garçon) ainsi que d'autres problèmes méthodologiques spécifiques en analyse ou en modélisation de données spatiales. Les 7 exposés de la matinée du jour 2 traitaient de méthodes employées dans l'analyse et la modélisation de la propagation de maladies zoonotiques. On y a présenté une revue des méthodes utilisées pour modéliser la distribution spatiale des espèces (Klinkenberg) ainsi que des approches particulières à des maladies précises ou en présence de difficultés statistiques particulières. Finalement, les 6 exposés de l'après-midi du jour 2 étaient dédiés à des problèmes en écologie. On a discuté des méthodes et approches utilisées pour construire des fonctions de sélection des ressources (Lele, Merrill, Keim) ainsi que des modèles spatiaux pour divers problèmes en écologie (M-J Fortin, Smith, Gralewicz). Les participants à l'atelier se sont révélés très heureux du programme, même s'il était très varié et très chargé. Les exposés des jours 1 et 2 ont tous généré beaucoup d'intérêt parmi l'auditoire. Les nombreuses questions et discussions qu'ont suscitées les exposés ont fait que ces deux journées se sont terminées beaucoup plus tard que l'horaire prévu malgré la bonne discipline des conférenciers ! Qui plus est, à la demande générale, les aides visuelles que les conférenciers ont utilisées lors de leurs présentations ont été ajoutées au site web de l'atelier. Les discussions du jour 3 ont été tout particulièrement appréciées. Plusieurs idées de financement (programmes spéciaux du CRSNG, idées d'ateliers pour chacun des sous-thèmes, problèmes de recherche susceptible de générer du financement pour de la recherche en équipe, possibilités de stages MITACS) ont été identifiées. Les discussions en petits groupes de recherche ont déjà mené à de nouvelles collaborations. En outre, Lele et Forester prévoient travailler sur la modélisation des habitats disponibles et leur prise en considération dans les méthodes d'estimation pondérées, et leur discussion a permis à Lele de terminer un article passant en revue les méthodes d'ajustement de fonctions de sélection des ressources. Chen et Deardon ont entrepris une collaboration sur la modélisation de la propagation de la grippe A(H1N1) en Ontario. Il semblerait que les chercheurs d'Hydro-Québec et d'électricité de France ont échangé de nombreuses idées sur des problèmes communs.

Workshop on Analysis of Multiphase Biomembranes
McGill University, April 24 to 26, 2010
Organiser: Eliot Fried (McGill University)

The workshop was devoted primarily to tutorial lectures given by Professors Qiang Du (Pennsylvania State University), James Jenkins (Cornell University) and David Steigmann (University of California at Berkeley). In addition, hour-long research presentations were given by Professors Deseri (University of Trento), Genin (Washington University in St. Louis), Kartunnen (University of Western Ontario) and and a Ph.D. student, Ms. Zhang (McGill University).

Professors Jenkins and Steigmann provided in-depth derivations of the partial differential equations governing equilibrium configurations of single- and multi-component biomembranes. They also presented analytical and numerical results concerning solutions to these equations. Professor Du provided a comprehensive overview of numerical methods for solving both static and dynamic problems for single- and multi-component biomembranes, with a strong focus on phase-field based methods. It is perhaps not particularly surprising he many students who attended the workshop benefited from these lectures. In addition, faculty members with knowledge of the field also found that these lectures provided valuable perspective.

The research talks were also highly informative. Professor Deseri presented a new theory for phase transitions in multicomponent biomembranes derived on the basis of Gamma-convergence. Professor Genin presented an overview of state-of-the-art imaging techniques with the goal of providing theorists and analysts with background needed to connect their results with experimental measurements. Professor Kartun-

nen discussed the latest atomistic simulation techniques for biomembranes. Professor Steigmann presented very exciting results for problems involving biomembranes on surfaces. Finally, Ms. Zhang presented results from her thesis research concerning molecular diffusion on biomembrane surfaces.

Despite occurring over a weekend with unusually fine weather, attendance was consistently high throughout the workshop. All attendees appeared to have considered the time spent to be most worthwhile.

Even more important than the answers arising from the workshop were the questions. The workshop was a one-of-a-kind opportunity to discuss membrane physics across disciplines and length scales. The workshop and its format allowed for a critical, cross-disciplinary discussion of the basic mathematical assumptions underlying analysis in this field, beginning an important re-evaluation of our entire approach. Research in Multiphase Biomembranes represents an area where there are many exciting new discoveries are being made, and where the collaborations of mathematicians, biologists, and mechanicians are crucial. The workshop made important contributions to promoting new research efforts.

Conférence ICISP 2010
International Conference on Image and Signal Processing
Université du Québec à Trois-Rivières, 30 juin au 2 juillet 2010
Organisateurs : A. Chalifour et F. Nouboud (UQTR), A. Elmoataz et O. Lezeray (Université de Caen), D. Mammas (Université Ibn Zohr, Agadir, Maroc) et J. Meunier (Université de Montréal)

Cette conférence a accueilli plus de 80 chercheurs dans le domaine de la vision par ordinateur en provenance de 25 pays de tous les continents. Les actes de la conférence ont été publiés chez Springer (Lecture Notes in Computer Science, LNCS 6134). Les événements forts de la conférence ont été les présentations de nos trois conférenciers invités : le professeur Yann Lecun du Courant Institute et du Centre for Neural Science, NYU, le professeur Theo Gevers de l'Université d'Amsterdam et le professeur Leo Grady de Siemens Corporate Reserch, Princeton. Les différentes sessions de la conférence se répartissaient comme suit : Image filtering and Coding ; Patter Recognition ; Biometry ; Signal Processing ; Video Coding and Processing ; Watermarking and Document Processing ; Computer Vision ; Biomedical Applications. La 5^{e} édition de la conférence ICISP se tiendra à Agadir (Maroc) en 2012.

Conférence MPC 2010
10th International Conference on Mathematics of Program Construction
Lac-Beauport, 21 au 23 juin 2010
Organisateurs : Claude Bolduc, Jules Desharnais et Béchir Ktari (Université Laval)

MPC 2010 a eu lieu au Manoir St-Castin, à Lac-Beauport, en banlieue de la ville de Québec. Le programme a consisté en deux présentations invitées par les professeurs Roland Backhouse (The University of Nottingham, Royaume-Uni) et Stephan Merz (INRIA Nancy et LORIA, France), en 19 présentations d'articles choisis parmi 37 à la suite d'un processus d'évaluation rigoureux et en un banquet suivi d'une visite du Vieux-Québec. Le congrès MPC a précédé le congrès AMAST 2010 (13th International Conference on Algebraic Methodology And Software Technology, 23 au 25 juin 2010). Les deux congrès ont des buts similaires, mais ceux d'AMAST sont plus généraux, alors que MPC se concentre principalement sur la construction des programmes. Parmi les 46 participants, 22 ont participé à MPC et à AMAST. Les congrès MPC visent à promouvoir le développement de principes et de techniques mathématiques utiles pour la construction des logiciels et des systèmes informatiques. Les présentations ont porté sur la construction et la vérification des programmes, le raffinement des spécifications, la sémantique des langages de programmation, les algèbres de processus, les théories de la programmation, les systèmes de types, les structures mathématiques utiles et l'automatisation de certaines démarches. Lors du banquet, une plaque souvenir a été remise à Roland Backhouse, conférencier invité et l'un des deux initiateurs de la série de congrès MPC, pour le remercier et pour commémorer cette 10^{e} édition de MPC.

Word of the director

(*continued from page* 17)

such as Statistics, Geometry and Topology, Quantum Information,.... Some laboratories existed as research centres when they joined the CRM, others were founded directly for the purpose of joining. They are represented in the administrative structure of the CRM by the Committee of Directors of Laboratories, and there is a laboratory director designated to serve as a member of the Conseil d'administration, the highest decision making body of the CRM. There is now a strong symbiosis between the activities of the CRM and those of its laboratories. In particular, many or the thematic semesters of the CRM are initiated and planned with a strong input from the laboratories. A funding formula was agreed upon at the time the laboratories structure was created. In the meantime the laboratories have evolved and it was felt that the "historic formula" needed rethinking. A formula was developed by the committee of laboratory directors that takes account of membership, but with a built in quality control based on existing data. It is easily updated. It bypasses the need for periodic independent review of all laboratories which was more or less unanimously seen as a burden that the laboratories did not want to subject themselves to. To create the possibility of rewarding particularly active laboratories, it was decided to make part of the laboratory financing available as a special fund to which the laboratories can apply for non-recurring "special" activities. Applications received are submitted to the CRM Local Scientific Committee for evaluation and approval. We already went through two rounds of applications and awards, one for 2010/2011 and one for 2011/2012.

Peter Russell

The First Montreal–Toronto Workshop in Number Theory

by Eyal Goren (McGill University) and Steve Kudla (University of Toronto)

The Montreal–Toronto Workshop in Number Theory is a new joint initiative, conceived by us as a way to foster stronger relations between the active groups in number theory and arithmetic geometry in the two cities. The workshop enjoys financial support from both the CRM at Montréal and the Fields Institute at Toronto. The first workshop took place in Montréal on September 4–5, 2010. The program was devoted to recent developments in the theory of orthogonal Shimura varieties. We had 9 participants from Toronto and 20 participants from Montréal, including graduate students, postdoctoral fellows, faculty and visiting faculty.

The program started Saturday morning at 10:00 and ended at 18:30, it consisted of background lectures given by Dylan Attwell-Duval, Andrew Fiori, Patrick Walls, Brian Smithling, Bahareh Mirza, Victoria de Quehen, Jayce Getz and Siddarth Sankaran. The day ended by an hour-long lecture by Fritz Hoermann, a new postdoctoral fellow at McGill, on the results recently obtained in his thesis. This series of lecture was outstanding in its clarity and scope, and that is especially commendable given that many of the speakers are graduate students. Following the day's lectures, we headed for a joint dinner, which allowed fantastic opportunity to follow up on some of the day's topics and to foster connections between the two communities.

The Sunday program started at 9:30 and ended in the early afternoon. It consisted of two 90 minutes lectures, given by Goren and Kudla, who surveyed some of the recent progress in the area to which the workshop was devoted. Goren surveyed the work done in the last years on generalizing the theorem of Gross and Zagier on singular moduli to the setting of multiplicative averages of Borcherds lifts on CM cycles, and, in a different direction, to the study of primes for which two abelian varieties with CM may have isomorphic reduction. Kudla devoted his lecture to explaining the recent breakthrough made by Bruinier in generalizing the Borcherds lift to the context of Hilbert modular varieties and orthogonal groups over totally real fields.

The workshop was a smashing success and its participants are waiting with anticipation to the next workshop to be held at the Fields Institute in April 9–10, 2011. The lectures were available to the participants as pdf files, posted and currently available from `www.math.mcgill.ca/goren/Montreal-Toronto/Montreal-Toronto.html`.

Le Bulletin du CRM

Volume 16, N° 2
Automne 2010

Le *Bulletin du CRM* est une lettre d'information à contenu scientifique, faisant le point sur les actualités du Centre de recherches mathématiques.

ISSN 1492-7659

Le Centre de recherches mathématiques (CRM) a vu le jour en 1969. Actuellement dirigé par M. Peter Russell, il a pour objectif de servir de centre national pour la recherche fondamentale en mathématiques et leurs applications. Le personnel scientifique du CRM regroupe plus d'une centaine de membres réguliers et de boursiers postdoctoraux. De plus, le CRM accueille chaque année entre mille et mille cinq cents chercheurs du monde entier.

Le CRM coordonne des cours de cycles supérieurs et joue un rôle prépondérant (en collaboration avec l'ISM) dans la formation de jeunes chercheurs. On retrouve partout dans le monde de nombreux chercheurs ayant eu l'occasion de parfaire leur formation en recherche au CRM. Le Centre est un lieu privilégié de rencontres où tous les membres bénéficient de nombreux échanges et collaborations scientifiques.

Le CRM tient à remercier ses divers partenaires pour leur appui financier à sa mission : le Conseil de recherches en sciences naturelles et en génie du Canada, le Fonds québécois de la recherche sur la nature et les technologies, la National Science Foundation, le Clay Mathematics Institute, l'Université de Montréal, l'Université du Québec à Montréal, l'Université McGill, l'Université Concordia, l'Université Laval, l'Université d'Ottawa, l'Université de Sherbrooke, le réseau MITACS, ainsi que les fonds de dotation André-Aisenstadt et Serge-Bissonnette.

Directeur : Peter Russell

Directeur d'édition : *Chantal David*
Conception et infographie : *André Montpetit*

Centre de recherches mathématiques
Pavillon André-Aisenstadt
Université de Montréal
C.P. 6128, succ. Centre-Ville
Montréal, QC H3C 3J7

Téléphone : 514.343.7501
Télécopieur : 514.343.2254
Courriel : `CRM@CRM.UMontreal.CA`

Le Bulletin est disponible au
`crm.math.ca/docs/docBul_fr.shtml`.