



CRYPTOGRAPHY: A Retrospective

From June until December of the 2006-2007 academic year, the Fields Institute ran a program in Cryptography, organized by Ian F. Blake (Toronto), Alfred Menezes (Waterloo), Michele Mosca (Waterloo and Perimeter Institute for Theoretical Physics), Kumar Murty (Toronto), Renate Scheidler (Calgary), Andreas Stein (Wyoming), Ramarathnam Venkatesan (Microsoft Research), and Hugh Williams (Calgary). The following is a brief overview of the activities.



Hugh Williams

BACKGROUND

The integrity and security of information and information systems is often overestimated in our electronic age, with increasingly devastating results. The social and economic costs to individuals and organizations due to the lack of reliable and effective security can be measured in the loss of privacy and information, a loss or lack of confidence in electronic commerce, trade and communications systems, time, strategic advantage, and billions of dollars in business opportunity, security measures and downtime. One essential component of any installation in which secure communication is needed is cryptography, the topic of the fall 2006 Thematic Program at the Fields Institute. Briefly put, Cryptography is the study of the design and analysis of mathematical techniques that ensure secure communications in the presence of malicious adversaries.

If a sender and receiver of a message wish to communicate over an insecure channel (e. g. mobile phone, internet) and want to ensure that no other unauthorized party can read their transmission, they can make use of a particular *cryptosystem*. A conventional cryptosystem can be thought of as a large collection of transformations (ciphers), any one of which will render the original message (plaintext) to unintelligible *ciphertext* – but in order for the receiver

continued on page 10

NEW FELLOWS OF THE RSC



Andrew Granville, Mary Thompson, Ming Li and Barbara Keyfitz

THIS YEAR'S SPEAKERS AT THE SYMPOSIUM honouring the new Fellows of the Royal Society of Canada ran the gamut of the mathematical sciences: a mathematician, a statistician, and a computer scientist.

Mary Thompson (Waterloo) gave a “whirlwind tour of sampling theory.” Her talk on the history of sample surveys from the 19th century to the present gave vivid portraits of the founders of statistics, along with fascinating details of the development of the subject. If you find the superiority of random sampling over representative sampling counter-intuitive, you have company: it was not until 1934 that Jerzy Neyman was able to convince the statistics community of this fundamental principle.

Andrew Granville (Montreal) presented a series of analogies between two apparently unrelated mathematical objects: integers less

continued on page 13

WORKSHOP ON HIGHER CATEGORIES AND THEIR APPLICATIONS



Workshop participants

PHOTO: J. BAEZ

THIS WORKSHOP, WHICH TOOK PLACE AT the Fields Institute from January 9 to 13, 2007, was part of the thematic program on *Geometric Applications of Homotopy Theory*. It was organized by John Baez (UC Riverside), Eugenia Cheng (Chicago) and Peter May (Chicago). Higher category theory, roughly speaking, is the study of hierarchical systems of morphisms between morphisms between morphisms. For example, a category has objects and morphisms, but the category of categories has objects (categories), morphisms (functors), and morphisms between morphisms (natural transformations), so it forms what is called a 2-category. There are strict and weak versions of higher categories and the full force and flavor of the subject comes from the weak versions, in which one never insists on equalities where isomorphisms are possible.

One might ask what that subject has to do with homotopy theory, let alone geometry. There are many answers, and the workshop devoted a day to each of five of them. Higher category theorists are a hardworking and sociable group, so the word “day” is a misnomer. There were usually two morning talks, one or more

long afternoon talks, and four evening sessions ending only around 9:00 pm.

One answer, the subject of the first day, a Tuesday, is that low dimensional higher category theory, that is the theory of 2-categories and 3-categories, describes patterns and structures that appear ubiquitously in mathematics. There is still a lot that is not well understood for $n = 2$ and 3. It was shown long ago by Mac Lane that every weak 2-category, or bicategory, is equivalent in a suitable bicategorical sense to a strict 2-category. However, that is only true one object at a time, and it is not true that there is an equivalence of weak 3-categories between strict and weak 2-categories. From the point of view of applications, that means that even in dimension 2, it is not enough to study strict 2-categories. Tom Leinster explained this in the first talk. In dimension 3, it is not even true that every weak 3-category is equivalent to a strict 3-category, but it is equivalent to a semistrict (or Gray) 3-category, as Steve Lack explained in the second morning talk. Actually, it is not even clear how to define weak 3-categories precisely, as Nick Gurski pointed out in the afternoon talk. He wrote his thesis on that topic, where

he gave perhaps the definitive algebraic answer. In his talk, Nick not only explained the definition, which is famously complicated, he also did his best to convince us that we could reinvent this definition ourselves if we tried! Then he went ahead and discussed various proofs that every weak 3-category is equivalent to a semistrict one.

Nothing so far about homotopy theory, but one relevant point is that model category theory, which is an organizing principle for the homotopy theory of all kinds of structures of a homotopical nature, is now playing an important role in understanding higher category theory. Since this theory is not as well-known to category theorists as it should be, Mike Shulman gave a gentle introduction to the subject Tuesday evening. However, there is a more directly relevant point. One of the organizing principles of higher homotopy theory is that weak n -categories in which all morphisms are suitably invertible, the “weak n -groupoids”, should model homotopy n -types, spaces whose homotopy groups above the n^{th} are zero.

The main theme of the second day was the analogy between higher category theory and higher homotopy theory, which can be thought of as the study of homotopies between homotopies between homotopies. John Baez explained the “Homotopy Hypothesis” on the modelling of homotopy types, which is due to Grothendieck, in the first talk. Then Simona Paoli spoke about her work on turning the homotopy hypothesis from a dream into a reality. She has connected earlier algebraic models of homotopy n -types with a higher categorical model, due to Tamsamani, in a strikingly convincing fashion. There are many different ways of defining weak n -categories and thus many different ways one might approach the homotopy hypothesis. Eugenia Cheng spent the afternoon guiding us through another approach, due to Clemens Berger and Denis-Charles Cisinski, which starts from Batanin’s definition of weak higher groupoids.

continued on page 9

2007 CRM-FIELDS-PIMS PRIZE



Joel Feldman

JOEL FELDMAN

UNIVERSITY OF BRITISH COLUMBIA

MY FIRST ENCOUNTER WITH THE WORK OF Joel Feldman came when I was a graduate student in the 1970s. In those days the program to construct quantum field theories (QFT) was in full flight. The construction of two spacetime dimensional QFT had been successful and even the formidable divergences of three dimensional QFT were under siege by a machine invented by Glimm and Jaffe and known as “the phase-cell expansion”. Joel Feldman was one of a very small number of people who clearly understood the principles of this technique and I was reading his papers almost in preference to the papers of the masters because, then as now, his papers were models of clarity. In 1976 Feldman and Osterwalder were finally able to prove that a candidate for three dimensional quantum field theory known as φ^4_3 was indeed a quantum field theory, that is, it satisfied the Wightman axioms. As for four spacetime dimensions, my adviser said to me “it may be 100 years before we understand four dimensions”. Since then I have watched in astonishment as Joel Feldman and his collaborators have gradually extended the scope of

the phase cell expansion to such an extent that their recent work on the Fermi surface problem overcomes a problem that is much more than the equal of the particular difficulties that made my adviser so pessimistic 30 years ago. Unfortunately, he may yet be right in that the original goal of existence of a four dimensional theory remains unsolved. However, the obstruction is no longer the “short distance divergences” that seemed so hard in 1976.

To describe Joel Feldman’s place in all of this and give a sense of the accomplishments that the CRM-Fields-PIMS Prize honours, I will have to give a little background on QFT and the phase cell expansion. If another person were to write this article they might emphasize other parts of Feldman’s work such as his work on infinite genus Riemann surfaces but I take most pleasure in his work in QFT and condensed matter. In one other respect at least this description does a bad job. To keep it short the contributions of theoretical physics are not properly described.

The axioms of quantum field theory (QFT) are surprisingly simple. To each bounded open subset of spacetime is associated an algebra of operators on a Hilbert space. These operators represent quantities one can measure, such as the energy of the field inside the set. The structure of spacetime is encoded functorially by requiring that when two open sets in spacetime are related by a morphism the corresponding algebras of operators must be related by a corresponding morphism. Yet this simplicity conceals one of the most beautiful and difficult structures ever encountered in mathematics. We now hear about it all the time in differential geometry and topology, but for analysts it may offer the greatest challenge of all. All the strange arguments based on the “functional integral” will remain fringe intuition for conjectures proved some other way for as long as this challenge is unmet. Brownian motion, the pride and joy of probability, is a quantum field theory on a one dimensional Euclidean spacetime.

Among the other quantum field theories there will be other treasures. In fact SLE and conformal QFT in two dimensions is an unfolding example.

Phase space is the Cartesian product of space, \mathbb{R}^d , with momentum space \mathbb{R}^d . As in the theory of pseudo-differential operators, a phase-cell is a box which is consistent with Fourier analysis and the uncertainty principle in that the sides Δx in spatial \mathbb{R}^d and Δp in momentum \mathbb{R}^d satisfy $\Delta x \Delta p = 1$. Divergences in quantum field theory arise because the field has fluctuations on all scales. If fluctuations are decomposed into fluctuations localised in phase-cells then there is roughly only one degree of freedom of fluctuation per phase-cell. The divergences of QFT are now lurking in the infinity of phase cells, but this reorganisation uncovers a compensating property of approximate independence. The phase-cell expansion implements the idea that the functional integral of quantum field theory is approximately the product over phase cells of integrations over fluctuations in phase cells. According to the phase cell expansion a quantum field theory functional integral can be understood as a convergent sum of corrections to this oversimplified picture. In this expansion the divergences of QFT appear in combinations where they cancel each other. The term “divergent” means that a parameter is introduced. It is called an “ultraviolet cutoff” and it specifies a small length at which fluctuations are artificially suppressed. The suppression destroys at least one of the axioms of QFT, but the phase cell expansion is uniform in this parameter and so the limit as the ultraviolet cutoff is taken to zero becomes feasible and the axioms are restored in the limit.

The Fermi surface problem arises in condensed matter physics. The object is to understand the collective behaviour of a large number of electrons moving in a crystal. The term collective behaviour is a signal that this is in the same class of problems as

continued on page 7

Workshop on the Representation Theory of *Reductive Algebraic Groups*

THIS ENORMOUSLY SUCCESSFUL WORKSHOP was hosted by the University of Ottawa from January 18 to 21, 2007, attracting approximately forty participants from across Canada, the US, Europe and Israel.

The workshop opened with two days of intense mini-courses on some of the key topics in this field: Julia Gordon (UBC) brought us up-to-date in the emerging field of motivic integration; Ju-Lee Kim (UIC) described her recent exhaustion result for supercuspidal representations of p -adic groups; and Phil Kutzko (Iowa) gave wonderfully entertaining and wide-ranging lectures on the fundamentals of the representation theory of p -adic groups.

Toward the end of this part of the workshop, Anantharam Raghuram (Oklahoma State) kicked off the weekend portion of the workshop with a colloquium talk, widely attended by faculty from both Ottawa universities, on the arithmetic of L -



functions. The subsequent conference talks, which took us through Sunday, covered a wide range of research drawing from the representation theory of reductive algebraic groups: Jeffrey Adler (Akron) spoke on *Multiplicity one upon restriction*, Anne-Marie Aubert (Jussieu) spoke on *Springer correspondence for complex reflection groups*, Cristina Ballantine (Holy Cross) spoke on *Combinatorics and representation theory of p -adic groups*, Lassina Deméle (Calgary) gave a talk in *Explicit Jacquet-Langlands*

for $GSp(4)$, Fiona Murnaghan (Toronto) spoke on *Ordinary characters and spherical characters: the supercuspidal case*, Anantharam Raghuram gave a talk on *Special values of certain automorphic L -functions*, Michael Schein (Hebrew) spoke on *Weights in Serre-type conjectures and the mod p Langlands correspondence*, and Teruyoshi Yoshida (Harvard) spoke on *Non-Abelian Lubin-Tate theory and Deligne-Lusztig theory revisited*.

The great scope of the talks, together with the diverse backgrounds of our attendees, produced a very stimulating atmosphere, with participants grouping together to discuss ideas long after the talks were concluded each day. This event was the second in a sequence of high-profile workshops in this area sponsored by the Fields Institute and the University of Ottawa.

Clifton Cunningham (Calgary)
Monica Nevins (Ottawa)

2007 FIELDS-CARLETON DISTINGUISHED LECTURER

JERROLD E. MARSDEN

Lagrangian Coherent Structures: From Jellyfish to Hurricanes. Discrete Mechanics, Variational Principles, Time Stepping, and Optimization.

THE ANNUAL FIELDS-CARLETON Distinguished Lecture Series was delivered by Jerrold E. Marsden, the Carl F. Braun Professor of Engineering and Control and Dynamical Systems at the California Institute of Technology. Among many other achievements, Marsden was also the founding director of the Fields Institute from its inception (around 1987) to 1994.

As one of the leading authorities in theoretical and numerical mechanics, Jerrold Marsden has done extensive research in the area of geometric mechanics, with applications to rigid body systems, fluid mechanics, elasticity theory, plasma physics, as well as to general field theory. His work in dynamical systems

and control theory emphasizes their relations to mechanical systems and systems with symmetry. He is one of the founders, in the early 1970s, of reduction theory for mechanical systems with symmetry.

“Marsden discussed discrete mechanics and its fascinating spectrum of applications.”

The first lecture focused on Lagrangian Coherent Structures (LCS), which are the time varying generalization of separatrices dividing the space of a dynamical system into trajectories that have different dynami-

cal behavior. The audience was motivated with the LCS analysis of the Hurricane Nabi and other coherent structures which appear in planetary physics and celestial mechanics. Next, more formal discussion of LCS was given in the context of the central developments of dynamical systems theory. Using examples from ocean and atmospheric dynamics, the speaker demonstrated the usefulness of LCS for computing mixing and transport. For example, in a jellyfish, which fluid particles will get entrained into the jellyfish and which will be used for propulsion? Similarly, what fluid particles will get entrained into a hurricane and which will get detrained? What are the dynamics of the Ozone Hole breakup? What exactly do fluid particles do in the process of the aerodynamic boundary layer separation from the surface of an airfoil? Can LCS be of any help in cardiovascular applications?

continued on page 13

Connecting Women in Mathematics across Canada

LAST DECEMBER, THE FIELDS INSTITUTE hosted the third annual meeting of this workshop, attended by more than 40 women, ranging from undergraduate and graduate students to senior and administrative faculty. The organizers were Gerda de Vries (Alberta), Megumi Harada (McMaster), Lisa Jeffrey (Toronto), Laura Scull (UBC), and Ping Zhou (StFX).

They came together with one common aim: to support junior women in developing their mathematical careers.

The evening of day one began with some perspective, provided by freelance writer and journalist Siobhan Roberts. Her presentation, entitled *Mr. Polytope and Sexual Polytics*, examined Donald Coxeter's relationship with the women in his life. Coxeter's views were in many ways ahead of his time, and he was willing to judge mathematicians on their mathematics, not their genders.

Gender roles have, of course, undergone radical changes since Coxeter's early days. Yet, as dinner speaker Margaret Beattie, Dean of Science at Mount Allison University, was quick to point out, mathematics has failed to realize the same levels of growth in female participation as other traditionally male-dominated sciences. Given how far technology and society have come in the last 30 years, asked Beattie, are girls still "too cute" to be good at math, a question sparked in part after spotting a 12-year old girl wearing a pink T-shirt with the slogan "I'm too pretty to be good at math."

One is tempted to answer no, that the problem lies elsewhere. But, then, as mathematicians and, in particular, as women in mathematics, what more should we be doing to encourage women to pursue advanced studies and careers in mathematics? Through informal mentorship pairings and numerous discussion sessions, the remainder of the workshop actively sought to answer precisely this question.

Conversation during dinner provided the first opportunity for junior women to benefit from the experiences of their



Workshop participants

senior mentors. More than just networking opportunities, these pairings gave the younger women insight into the workings of institutions other than their own, and gave the mentors an opportunity to influence their future in mathematics.

Day two of the workshop emphasized the ongoing and prospective research projects of graduate students and postdoctoral fellows in attendance. Six research talks along with a ninety-minute poster session reflected a wide range of interests across the mathematical spectrum.

Right before lunch and the final mentorship pairing, Wendy MacCaull (StFX) provided some food for thought by speaking on the topic of new opportunities for mathematical research. Drawing upon her own experiences, Wendy outlined the steps she took to becoming involved in health research late in her career. She presented alternatives to the model of mathematicians as mysterious Ivory Tower academics, and challenged the participants to look into ways in which their skills can be applied to solving problems in industry and health.

The afternoon featured a discussion panel with Barbara Keyfitz (Fields), Laura Scull (UBC), Susan Tolman (UIUC), Gail Wolkowicz (McMaster),

and moderator Megumi Harada (McMaster). Questions tackled by the panel ensured that the junior women were well prepared to face the challenges of graduate studies, the academic job search, and beyond. Through numerous anecdotes, the panellists addressed many pertinent issues affecting developing academics from a woman's point of view. Among the topics discussed were those of advisor selection, variations on the two-body problem, and the transition from student to independent researcher. While the diversity of experience at times resulted in a lack of consensus, it also reflected the multitude of possible roads to success.

Overall, the workshop was an invaluable opportunity for the participants to play an active role in supporting the development of women in mathematics.

The Third Connecting Women in Mathematics across Canada workshop had support from the Committee for Women in Mathematics of the Canadian Mathematical Society. Financial support was received from the Fields Institute, the Canadian Mathematical Society, and a generous anonymous donor.

Alexandra Chouldechova (Toronto)

Going outside the University: Jeffrey S. Rosenthal

THERE ARE NOT VERY MANY MATHEMATICIANS who cross the border between the culture of mathematics—which is characterized by outsiders as mysterious and caught in a self-constructed web of theoretical language—and that of public culture. Tom Lehrer, who taught statistics at Harvard, did so in the 1960s, writing and singing satirical folksongs:

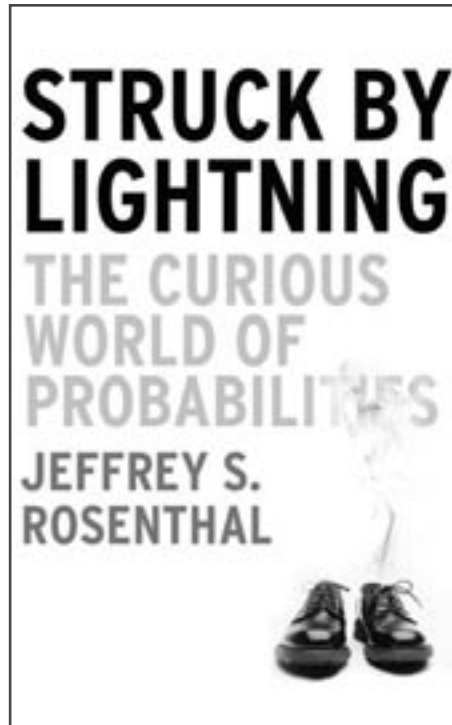
*So join in the folk song army!
Guitars are the weapons we bring
To fight against poverty, war,
and injustice.
Ready, aim, sing! (1965)*

Charles Lutwidge Dodgson, who taught mathematics at Oxford, but is known universally by his pen-name Lewis Carroll, did so spectacularly in 1865 when he published *Alice's Adventures in Wonderland*.

In 2005, Jeffrey S. Rosenthal published a best-selling book entitled *Struck by Lightning: The Curious World of Probabilities*. Rosenthal is a Professor of Statistics at the University of Toronto, and has published two textbooks on probability theory: *A First Look at*

“newspapers only feature rare events, leading to public misconceptions about the quotidian world.”

Rigorous Probability (2000) aimed at graduate students; and *Probability and Statistics: The Science of Uncertainty* (2003), with co-author Michael J. Evans, intended for undergraduates. In addi-



tion, he has written many research papers, and is particularly interested in Markov chain Monte Carlo algorithms, and how they can be used when the complexity of the data overwhelms other methods of analysis.

Struck by Lightning, however, is aimed outside the culture of mathematics at everyone who has ever been struck by the thought that we live in a society in which there is a lot of randomness, variability, and uncertainty. His book speaks of homicide rates: the fact that more homicides are committed by spouses than by strangers suggests to Rosenthal that one should consider one's choice of partner carefully! He juxtaposes the anxiety of air travellers about plane crashes with their casual acceptance of greater risk when they drive. He describes the way in which the law of large numbers ensures that gambling casinos will make huge profits although the odds are only narrowly in their favour. As for lotteries, well, put your money in a piggy-bank instead. He discusses what he calls “headline bias,” namely, that newspapers only feature rare events, leading to public misconceptions

about the quotidian world. Such examples illustrate the usefulness of a probabilistic perspective in one's personal outlook.

In his book, Rosenthal goes on to look at applications of randomness in biology, in considering medical pandemics, in constructing opinion polls, and in analysing election results. And although he has had no direct experience in the environmental sciences, he has no doubt that probability will be a powerful tool in looking at the vast quantities of data and shifting uncertainties in the field of climate change.

Jeffrey Rosenthal grew up in Scarborough, Ontario. As there were many mathematicians in his family, including his mother and father, a grandfather, and an uncle, it seemed perfectly natural to him to pursue mathematics. But he has other strong interests, some of them surprising. He creates wry cartoons using Java applets, which he also uses to provide visual material to illustrate lectures. And he enjoys playing rock, blues, and folk music on a variety of musical instruments—guitar, keyboard, harmonica, trumpet, penny whistle, and bongo

“he has no doubt that probability will be a powerful tool in looking at... climate change.”

drums. Can we look forward to compositions combining the penny whistle and probability?

Elaine Riehm

2007 Nerenberg Lecture: Leslie Woods

Against the Tide: The Fusion Energy Establishment and a Heretic's Challenge

WHEN DR. LESLIE WOODS, FELLOW OF Balliol College at Oxford University, titled his lecture, he hinted at controversy—a hallmark of the Nerenberg Lecture series. The 10th Nerenberg Lecture also celebrated the 40th anniversary of Western's Department of Applied Mathematics.

Early in his talk, Woods proclaimed "I haven't always been against the tide, my first forty-eight years I was with the tide." During those years, Woods realized that something was flawed in the promise of fusion power as the date of production kept on being pushed back. He soon focused on the concept of "Tokamaks and so-called anomalous transport."

According to Woods, the disappointing performance of the huge Tokamak machines that are supposed to generate massive amounts of energy (as well as high energy neutrons) from the fusion of tritium and deuterium is due to an anomaly overlooked by those in the field. "Heat normally goes down temperature gradients, we all know that, but sometimes it goes the other way, heat goes up the temperature gradient," says Woods.

Woods first laid the groundwork for his argument by referring to Thomas Kuhn's proposition of the two kinds of science

research. The paradigm of normal science is "the accepted mode of thinking at any given time and ... an anomaly can be resolved within that paradigm." Woods then added, "If you get a persistent anomaly, that is, if you can't figure how to get rid of it in the ordinary line of science then you have to have a revolution in science." Woods noted that after World War II the development of "big science" was incompatible with the above paradigms since the huge funding involved was made on "a case based on existing science and then suddenly there's an anomaly which surprises you. It's not resolved, it persists, and you've got no way of having a new paradigm."

According to Woods, the failure of tokamaks to retain energy has a simple explanation, which is not "anomalous" transport due to turbulence. Part of the problem is due to shear. "If you take hot electrons spinning around the lines of magnetic force and the colder ones below then at the intersection the net effect along the intended path will be at right angles. You will get heat either going up the temperature gradient or down the temperature gradient." Woods suggests that the mechanism of backward thermal diffusion is not only responsible for internal transport

barriers but it also explains coronal heating with plasma loops as conduits.

Although the thought of heat going up the temperature gradient amounts to scientific heresy, Woods says that heresy is an essential element for the advancement of science which is evolutionary, requiring open minds.

The Nerenberg Lecture is named after the late Morton (Paddy) Nerenberg, a much-loved professor and researcher born on 17 March – hence his nickname. He was a Professor at Western for more than a quarter century, and a founding member of the Department of Applied Mathematics there. Nerenberg was a successful researcher and accomplished teacher; he believed in the unity of knowledge, that scientific and mathematical ideas belong to everyone, and that they are of human importance. He regretted that they had become inaccessible to so many, and anticipated serious consequences from it. The series honours his appreciation for the democracy of ideas. He died in 1993 at the age of 57. He is survived by his children Albert, Ben, and Simone.

Mitchell Zimmer (UWO)

2007 CRM FIELDS PIMS PRIZE

continued from page 3

QFT: the many degrees of freedom of the electrons give rise to new phenomena such as superconductivity that are in the domain of QFT. If interactions between electrons are neglected then we can first focus on a single electron moving in the crystal. According to textbook quantum mechanics, there are allowed energies which are functions of the momentum of the electron. Then the ground state for N noninteracting electrons is such that the lowest single electron energies are fully packed up to a sharp threshold called the Fermi surface and all higher energies are unoccupied. This is because

electrons are Fermions and the antisymmetry of N particle Fermionic states under interchange of particle coordinates forbids multiple occupation of any single particle state so the electrons fill the levels like water in a bath. The surface can be visualised as enclosing a part of momentum space which is fully occupied. What happens to this picture if interactions between electrons are not neglected? Does a jump in the density of occupied states as a function of momentum persist or does it smooth out? The work of Feldman, Knörrer and Trubowitz answers this question, for a certain class of models, in a sequence of papers posted on his homepage. Their work shows that if the

Fermi surface for noninteracting electrons in a two dimensional system satisfy certain conditions then the result of turning on a small interaction is a deformation of the noninteracting surface as opposed to its destruction. Furthermore the renormalised perturbation theory is not merely finite term by term but convergent.

One of the major new ideas in these papers is to generalise the phase cell expansion to allow curvilinear phase cells that follow the geometry of the Fermi surface and refine as the surface is approached. A single electron, not interacting with others,

continued on page 12

KING OF INFINITE SPACE – Book Launch, and Celebration of the Life and Work of Donald Coxeter



The following is an excerpt adapted from Siobhan Roberts' biography on geometer Donald Coxeter, "King of Infinite Space: Donald Coxeter, the Man Who Saved Geometry," published last fall (by House of Anansi in Canada, and Walker & Company in the US.) The Fields Institute hosted a launch party celebrating the book on December 12, 2006 at which Coxeter's PhD student and great friend Willy Moser spoke. The main lecture room was packed with guests, who gamely folded a paper pentagon from a strip of paper (one of Coxeter's favoured tricks), and viewed clips from Coxeter's appearances on CBC television with Lister Sinclair in the 1950s (using as a prop a globe painted black to serve as a chalkboard), as well as a 1960s documentary film "Dihedral Kaleidoscopes," in which Coxeter starred. As a testament to geometry's enduring application in the sciences, guests also experienced a computerized stereoscopic simulation, complete with 3D glasses, of flying in a possible model for the shape of the universe — a 12-sided dodecahedron (the software was created by New York geometer Jeff Weeks.) Coxeter had experienced the same dynamic rendering of a 3D dodecahedral cosmos at the final geometry conference he would attend, in Budapest in 2001.



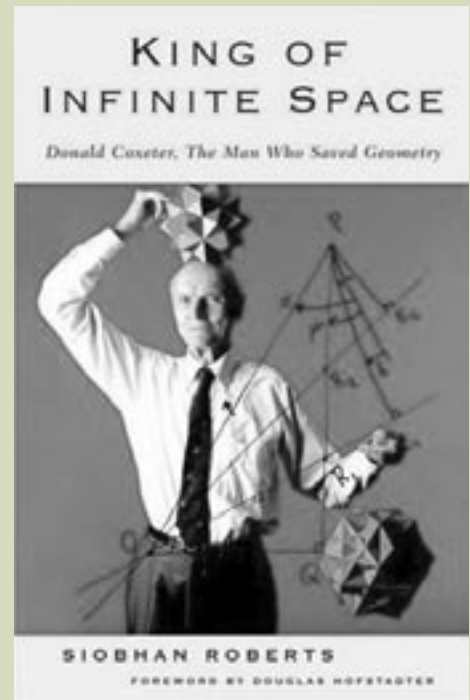
THIS YEAR IS THE CENTENARY OF DONALD Coxeter's birth, which makes it a fitting time to look back at one of a number of special birthday celebrations held in the geometer's honour at the Fields Institute.

At Coxeter's 95th birthday party, after the dedication ceremony for the 120-cell sculptural mobile that hangs in the atrium, John Conway, Coxeter's spiritual successor as a geometer, delivered a touching but humorous ode to his mentor. "My aim is to try to tell Donald Coxeter something about polytopes that he doesn't already know.

I'm not at all confident that I can pull it off. But I am going to try," Conway said, trying to reassure Coxeter that the impact of his oeuvre was enduring.

"But before I do," said Conway, "I want to step back 25 or so years, if I may, to Donald Coxeter's 70th birthday celebration [the Coxeter Symposium at the University of Toronto]. Nearly all the people there were students of Coxeter, or grand-students or great grand-students, and they were all getting up and saying how this man had been such a great inspiration in their lives. Well, I rather brashly thought I'd do something different. I stood up and said I was there to forgive Professor Coxeter for having tried to murder me. I then told a story which actually has a few elements of the truth about it."

"A long time ago Professor Coxeter came to Cambridge to give a lecture when I was a student there in the late fifties. I didn't realize it during the lecture, but that was his attempt to murder me. He chose as his weapon something Agatha Christie never thought of: a mathematical problem — he ended his lecture asking for a solution to a problem he'd been pondering." It was a problem about geometrical groups, the rotational polyhedral groups, and Coxeter groups. "I walked out of the lecture room," Conway recalled, "and crossed Trumpington Street, the main road in town. Just as I was in the middle of the road, the solution to Professor Coxeter's problem hit me. Right when he calculated it would, I figure — he judged its level of difficulty precisely. Because as it turned out, it was not the only thing that hit me. At the same time as the solution hit me, or a few microseconds later, a garbage truck also hit me. Fortunately, it didn't do too much damage; it was an unsuccessful attempt at murder. And after being shouted at for being a damned fool by the men hanging off the back of the truck, I limped back to the room and told Professor Coxeter all this and gave him my solution, which



to this day I refer to as the "The Murder Weapon" — this is a simple statement of Coxeter's murder weapon:

If $A^p = B^q = C^r = ABC = 1$ defines a finite group, then $A^p = B^q = C^r = Z$ implies that $Z^2 = 1$

"I'm one of the greatest Coxeter lovers," said Conway in closing. "He has a certain way with presentation that is elegant and carries the reader along. With mathematics what you're doing is trying to prove something and that can get very complicated and ugly. Coxeter always manages to do it clearly and concisely, with beauty. Coxeter kept a little flame of geometry alive by doing such beautiful works. There is a quotation from Walter Pater's book, *The Renaissance*. Pater was describing art and poetry. He refers to a hard, gem-like flame: "To burn always with this hard, gem-like flame, to maintain this ecstasy, is success in life." Somehow," Conway said, "that always makes me think of Donald Coxeter."

Siobhan Roberts

On Wednesday evening, Peter May spoke about some new applications of bicategories that appear in the just published book *Parametrized Homotopy Theory* that he and Johann Sigurdsson wrote. A suitable bicategory of parametrized spectra plays a central role in the book. There are two different kinds of duality in the parametrized world, one which works fiberwise and another which works like classical Spanier-Whitehead or Poincaré duality. It is virtually impossible to understand these dualities without viewing them in a suitable general context of duality in bicategories.

Thursday was all about $(\infty, 1)$ -categories. These are ∞ -categories in which all n -morphisms for $n > 1$ are invertible. This sounds fancy, but it is really a very simple idea. By the homotopy hypothesis, with $n = \infty$, weak ω -groupoids should model homotopy types. An $(\infty, 1)$ -category should have objects, and between any pair of objects a weak ω -groupoid. So the obvious models for $(\infty, 1)$ -categories are just categories enriched in topological spaces; that is, there should be a space of maps between any two objects. It is more usual to replace spaces by simplicial sets, but the idea is the same. However, there is a much more economical model with which one can actually redo category theory in a nice way. This kind of $(\infty, 1)$ -category is called a quasi-category. It was introduced by Boardman and Vogt around 1973, and it is just a simplicial set with a weaker “horn-filling condition” than the Kan complexes of classical simplicial theory. Mike Shulman started the day with a nice intuitive treatment of quasi-categories. Then Julie Bergner compared different approaches to $(\infty, 1)$ -categories. She is one of the few people who has worked hard on “the homotopy theory of homotopy theories”, and that was very much in evidence in her talk. She first described various different definitions of $(\infty, 1)$ -category, but she then showed that they are not really so different! For each definition, she constructed a model category of all $(\infty, 1)$ -categories of that type. She then sketched the proof that all of these model categories are “Quillen equivalent”.

In the afternoon, Andre Joyal spoke

about quasicategories. He is the prime figure in developing their theory, and he followed up his talk at the workshop with a minicourse on the subject. One can’t possibly summarize this material! It basically amounts to taking the whole of category theory and extending it to quasicategories. (Well, I guess that is a summary, but....). After Joyal’s talk, Joshua Nichols-Barrer spoke about using quasicategories as an approach to understanding “stacks”, which are like sheaves, only categorified.

In the evening, Kathryn Hess spoke about some work she’s doing with Steve Lack on parallel transport in bundles of bicategories. It sounds like physics, but they came to the subject with a completely different motivation. Finally, Dorette Pronk spoke about weak 2-categories and weak 3-categories of fractions. The use of a “calculus of fractions” for describing good localizations obtained by inverting certain morphisms in a category goes back to work of Gabriel and Zisman in the 1960s. With applications to stacks in view, Pronk has been looking at how this generalizes to allow the adjunction of “weak inverses” to some of the morphisms in a weak 2-category or weak 3-category.

Friday’s talks were about higher gauge theory, which is an application of higher category theory to geometry. Alissa Crans explained Lie 2-groups and Lie 2-algebras, and then Danny Stevenson explained his work on connections, 2-connections and Schreier theory. In the afternoon, Urs Schreiber described his ideas on higher-dimensional parallel transport and local trivializations, with a little help from Toby Bartels.

Friday evening, we heard talks from Simon Willerton (on Hopf monads) and Igor Bakovic (on 2-bundles).

Finally, on Saturday morning, Aaron Lauda spoke about Frobenius algebras and their relation to Khovanov homology in knot theory. Urs Schreiber then wrapped things up with a talk about the quantization of strings from a higher category viewpoint.

Altogether, the workshop put on display a broad range of abstract theory and concrete applications in and around higher category theory.

Peter May (Chicago)

THANKS TO OUR SPONSORS

MAJOR SPONSORS

Government of Ontario—Ministry of Training, Colleges, and Universities;
Government of Canada—Natural Sciences and Engineering Research Council (NSERC)

CORPORATE SPONSORS

Algorithmics, General Motors, QWeMA, R2 Financial Technologies Inc., Sigma Analysis and Management

PRINCIPAL SPONSORING UNIVERSITIES

Carleton University, McMaster University, University of Ottawa, University of Toronto, University of Waterloo, University of Western Ontario, York University

AFFILIATED UNIVERSITIES

Nipissing University, University of Guelph, University of Houston, University of Manitoba, University of Maryland, University of Ontario Institute of Technology, University of Saskatchewan, Queen’s University, University of Windsor, Wilfrid Laurier University

The Fields Institute receives and welcomes donations and sponsorships from individuals, corporations or foundations, and is a registered charity.

The Fields Institute is grateful to all its sponsors for their support.

The Fields Institute for Research in Mathematical Sciences publishes *FIELDSNOTES* three times a year (September, January, and May).

Director: Barbara Lee Keyfitz
Deputy Director: Juris Steprans
Managing Editor: Laura Gass
Distribution Co-ordinator: Tanya Nebesna
Scientific Editor: Carl Riehm

to read the message, he or she must know which particular transformation was used by the sender. The information that identifies the transformation used by the sender is called the *key*; this information, together with the ciphertext, can be used by the receiver to recover the original plaintext or *decrypt* the ciphertext. To maintain security, it is essential that the key be kept secret from any possible adversary. It is important to recognize that there are several possible objectives of eavesdroppers. One of these may simply be to read the transmissions, but it is also possible that they may wish to forge messages or send false messages or simply delete trans-

“Authentication systems are particularly useful in electronic funds transfers...”

missions. Thus, we distinguish between a *privacy system* and an *authentication system*. A privacy system protects against the unauthorized extraction of information from a given transmission, whereas an authentication system protects against the unauthorized injection or alteration of information into a transmission or the possibility of impersonation. Authentication systems are particularly useful in electronic funds transfers because secrecy of the transaction is often not nearly as important as the correct identity of the participants. It is important to emphasize that in order to achieve security, any particular cryptosystem must be used in a manner that does not leak information; such an implementation is called a *cryptographic protocol*.

In both privacy and authentication systems it is vital that the key be known to only the sender and receiver of the messages. Of course, this means that at some point the key must be communicated between the sender and receiver in a very secure manner. In one-key or symmetric cryptosystems, this must be done over a different and more secure transmission channel than that used for the transformed (encrypted) messages.

Prior to the mid-seventies all encryption techniques and algorithms were one-key systems and tended to be designed in *ad hoc* ways involving mathematics only peripherally. Two significant events in this period changed this situation. The first was the adoption of a one-key block cipher standard, the *Data Encryption Standard* or DES, by the US government. Although the key length of 56 bits was recognized early as being too short, the algorithm set the precedent of government standards in this area and was very successful. It was recently replaced by AES (*Advanced Encryption Standard*).

As separate key communication channels are expensive and often inconvenient to use, one important objective of modern cryptography has been to try to eliminate them altogether. The other important event of the mid seventies was the landmark contribution of Diffie and Hellman in their paper *New Directions in Cryptography*. In this paper they introduced several important concepts, such as the one way function and a kind of scheme now referred to as a *Diffie-Hellman protocol*. In such a scheme the transmitter and the receiver exchange information over a public channel that they can then assemble into a common communication key. An eavesdropper, however, does not acquire sufficient information to construct this key. They also suggested another method, but provided no example, of avoiding the use of a separate key channel by using a *public-key system*. In such a system each participant has two keys, a private one and a public one. The idea is that knowledge of the public key should not reveal anything about the private key. Thus, anyone who

wants to send a secure message to one of the participants uses that individual's public key, available in an easily accessible directory, for example, to encrypt the message; as only the receiver knows the private key, he or she can use this to decrypt the enciphered message, but no one else can.

PROGRAM DESCRIPTION

Cryptography and cryptographic protocols have now become a key element of information systems, protecting data and communications to ensure confidentiality, integrity and authenticity of data. While most symmetric key systems (block ciphers such as DES and AES and stream ciphers) have relatively modest mathematical requirements, public-key systems, as well as cryptographic protocols, have become increasingly mathematically sophisticated. Such systems rely for their security on the difficulty of specific mathematical problems. Two mathematical problems of particular interest for public-key cryptography are the integer factorization problem and the discrete logarithm problem (DLP). The discrete logarithm problem has been studied in a variety of mathematical structures, such as elliptic curves, hyperelliptic curves, abelian varieties, class groups of algebraic number fields to name a few. Cryptographic protocols have been studied in these structures and the work has opened new aspects of these problems and engaged talented mathematicians.

It is important, however, to emphasize that no rigorous mathematical proof of security has ever been given for any of these systems. The difficulty of these problems is usually established anecdotally through frequent and unsuccessful attempts by specialists to provide computationally efficient solutions to them. Indeed, several problems thought to be very difficult, such as the integer factorization problem, have been shown to be somewhat less to considerably less intractable than previously believed. Furthermore, the possibility of quantum computing becoming practical would change this

picture dramatically. If realized, most of the problems on which the security of public key cryptosystems rely drop from exponential complexity to polynomial, rendering currently deployed cryptographic systems useless. While the likelihood of this occurring in the short term is remote, this is an exciting area of research which may well lead to revolutionary advances in computation and secure information communication.

In view of this, it is certainly prudent to consider alternatives to public-key cryptography. One alternative is to use unconditionally secure cryptographic schemes, which can be proved secure regardless of the computational power of the adversary. Areas of active research in unconditionally secure cryptography include encryption schemes, message authentication, key distribution, broadcast encryption, secret sharing, fingerprinting and tracing. Research in unconditionally secure cryptography often involves elegant applications of diverse mathematics, including combinatorics, coding theory, information theory and probability. This provides a nice complement to the number-theoretic nature of public-key cryptography.

The aim of this program was to engage the cryptographic and mathematical communities in Canada and abroad to increase awareness of recent developments in these fields and to initiate a greater degree of collaboration in attacking the important problems, particularly those on the boundaries. The specific areas of concentration were, *quantum computing and quantum cryptography, algebraic curves and cryptography, computational challenges arising in algorithmic number theory and cryptography, unconditionally secure cryptography, cryptographic protocols, and applied aspects of cryptography.*

The program began with a summer school on *Computational Number Theory and Applications to Cryptography*, June 19–July 7, 2006, organized by the Rocky Mountain Mathematics Consortium at the University of Wyoming in Laramie, Wyoming. The summer school courses both complemented and prepared par-

ticipants for the activities of the Fields cryptography program. The remaining program activities were held at the Fields Institute.

The rest of the program was driven by a series of one-week workshops and supplemented by graduate courses, seminars and talks presented by distinguished lecturers. The scope of the program was ambitious in that it brought together researchers from areas that seldom have the opportunity to interact in an atmosphere where problems at the intersections could be explored. Developments in certain areas of mathematics (for example, number theory, combinatorics, algebraic geometry, non-abelian groups and rings) and in cryptography are both numerous and rapid; however, it is often the case that lack of contact and communication between cryptographers and mathematicians in these related fields, presents obstacles in achieving significant advances on both sides. The aim was to overcome these obstacles and foster new links among all of these areas.

The success of the Cryptography program was much more than the sum of its parts. There was an enormous amount of activity throughout its duration. In particular, there were many distinguished visitors from both academia and industry who interacted with each other and with graduate students and post doctoral fellows. Many new and exciting results were produced and often described at the various workshops. Indeed, there was almost a constant buzz of activity, particularly during the period of the workshops. The graduate courses were on the cutting edge of research and invariably well attended, as were the seminars. The Coxeter Lectures were given by two of the most prominent people in their area today. These lectures never failed to be both informative and stimulating. The objectives of this program were certainly achieved, and much future work will derive from its activities.

Hugh Williams (Calgary)

NOTED

JOHN BAEZ, a co-organizer of the recent Fields thematic workshop *Higher Categories and Their Applications* has written an entertaining summary of his time at the Fields Institute, including some great photos of the event in his online journal. www.math.ucr.edu/home/baez/week245.html

J. RICHARD BOND, university professor and past director of the Canadian Institute for Theoretical Astrophysics, University of Toronto, and member of the Fields Institute's Board of Directors has been awarded the prestigious *Gerhard Herzberg Canada Gold Medal for Science and Engineering*.

JENNIFER CHAYES, a member of the Fields Institute's Scientific Advisory Panel, was featured in the March issue of *Scientific American*.

CORRECTION: The January 2007 Fields Notes article on Nicole Tomczak-Jaegermann's CRM-Fields-PIMS prize lecture omitted the names of S. Artstein-Avidan, V. Milman and S. Szarek who collaborated with her on metric entropy problems. Their recent result solves the duality problem for metric entropy for a large class of Banach spaces. We apologize for the omission.

propagates according to a partial differential equation for which the Fermi surface is characteristic. In the dynamics of many noninteracting electrons, phase cells near this characteristic surface harbour the large fluctuations. However with this geometry in the phase cell decomposition, the interactions between fluctuations have the necessary independence properties as one gets closer to the surface.

As in QFT there are divergences in naive perturbation theory. These arise because the Fermi surface of the noninteracting electron system is not the same as the Fermi surface of the interacting system. Renormalisation means making the expansion about a new noninteracting system whose Fermi surface is the same as the interacting Fermi surface.

A Cooper pair consists of two particles each of whose momenta lie on the Fermi surface and whose total momentum is very small. If the shape of the surface permits such pairs then the interaction between these pairs becomes so huge as their total momentum approaches zero that new divergences appear in the perturbation

theory. This is again a signal that the model is being approximated by the wrong non-interacting model. In these Fermi surface papers this phenomenon is exactly what the hypotheses are ruling out. Conjecturally, if they are not ruled out, the Cooper pairs dominate the long distance structure of the theory, the Fermi surface is destroyed and the system is a superconductor.

In the 1980s, in the work of Balaban and others, it became clear that taking the limit as the ultraviolet cutoff tends to zero is possible, but there is another obstruction to existence of four dimensional QFT in the sense that is specified in the Clay Institute problem. One must also understand the role of fluctuations at very long scales. The phenomenon of superconductivity in the many electron problem is very relevant to what is conjectured to happen in four dimensional gauge QFT: superconductors expel magnetic field by setting up a flow of electrons to create an opposite magnetic field. This is called the Meissner effect. In some versions of this effect instead of complete expulsion, which is energetically costly, a thin tube reverts to the nonsuperconducting phase so as to permit the magnetic field but only in the tube. If two magnetic monopoles were placed in such a system, there would

be a flux tube joining them whose cost in energy grows linearly with length. Therefore the monopoles would be “confined” to stay close to each other by the flux tube. In four dimensional QFT a similar mechanism is expected to confine quarks. A more detailed grip on this type of mechanism is needed to understand four dimensional gauge QFT. The Fermi surface work has built part of the infrastructure for this problem. In fact, to prove existence of the Fermi surface the authors had to build an enormous infrastructure, including definitions, properties and estimates for integration over Grassmann algebras in order to express Fermions in the language of QFT, analysis and estimates of classes of ladder diagrams and the technology of phase cells adapted to the Fermi surface.

When I contemplate the range of phenomena that QFT rules, it seems to me that nature lives on the edge of what is possible, and an extraordinary amount of preparation may be needed for us to follow it there. By gathering in one place complete proofs that end with a very strong control over perturbation theory for condensed matter, the expedition is well under way.

David Brydges (UBC)

JOEL FELDMAN'S CRM-FIELDS-PIMS PRIZE LECTURE

THE SUBJECT OF JOEL FELDMAN'S PRIZE lecture at the Fields Institute on April 27, 2007 was quantum field theory, one of the topics emphasized by David Brydges in his description of Feldman's research career. In particular, Feldman gave a description of his work with Tadeusz Balaban of Rutgers and Horst Knorrer and Eugene Trubowitz, both of ETH-Zurich, on a functional integral representation of systems of many Bosons. Feldman explained that functional integrals have a long history of use as tools to provide intuition about quantum field theories, but in the past few decades it has become possible to use them to rigorously analyze such theories.

Feldman's talk considered a gas of particles with integer spin, such as photons or Helium-4 atoms. The particles themselves have kinetic energy, but any two particles

also interact through a repulsive two-body interaction. The system is imagined to be in thermodynamic equilibrium with a heat bath with which it can exchange both energy and particles. Feldman's talk focussed on how to represent the statistical mechanical partition function for this system as a functional integral. There are several sources of difficulties which are immediately apparent, difficulties such as the infinitely many possible sizes of the family of particles and, even more seriously, the uncountably many points of Euclidean space, each of which contributes to the partition function. However, even the vast simplification obtained by approximating Euclidean space with finitely many points does not surrender easily. This may seem surprising to those familiar with Brownian motion and Wiener measure since it seems that a similar

approach should yield a useful definition of the integral. The key difference in the many boson setting however, is that the exponent in the partition function can take on complex values. This results in wild oscillations that cause difficulties if one tries to define a measure on a space of paths as one does in the setting of Brownian motion. Feldman explained how coherent states, which are families of elements of Hilbert space parametrized by a single continuous variable, can be used to define the desired integral as a limit. The domain of the parameter is approximated by a finite set and the trace of the exponential operator is shown to be approximated arbitrarily closely by a formula involving only this finite set. More details can be found in the notes of the talk at www.fields.utoronto.ca/audio/06-07/crm-fields-pims/feldman/

New Fellows of the RSC
continued from page 1

than a number x and permutations on n letters. In both cases, he studies the relation of fundamental components – primes and cycles respectively – to the whole set. How rare are primes? The ratio of primes to all integers is exactly the ratio of cycles to all permutations. And the analogy continues through as many details of the distributions of these objects as Andrew has so far compared. The reason behind this is as yet undiscovered.

Ming Li (Waterloo) described three ways in which mathematics helps bioinformatics.

“The ratio of primes to all integers is exactly the ratio of cycles to all permutations.”

In a “homology search”, one finds all locally

similar regions in two DNA sequences – a huge task. Li and colleagues developed a method based on replacing a seed – a pattern to search for – by a spaced seed, in which gaps are left in the pattern. By optimizing the gap arrangement, the search is made both faster and more accurate. A second innovation involves the use of multiple seeds, and the third a hidden Markov model, leading to amazing speedup.

The audience was truly inspired by the talks, and offered warm congratulations to all the new Fellows.

Barbara Keyfitz (Fields Institute)

THANKS TO OUR DONORS

The Fields Institute conducts an annual giving campaign each fall to raise funds in support of our scientific and educational programs. For further information about donations, please visit our website <http://www.fields.utoronto.ca/aboutus/fundraising/>

Mayer Alvo
Stephen Berman
Cecily Bradshaw
Hermann Brunner
Inna Bumagin
Alison Conway, in honour of
 Florentia Conway
John Crow
Ronald G. Douglas
Sheila Embleton
Peter Fillmore
Hamid R. Ghaffari
Bradd Hart
Deirdre Haskell
Hillsdale Investment Management Inc.
Ken Jackson
Barbara Keyfitz
Nathan Keyfitz
Cathleen S. Morawetz
Michele Mosca
George O’Brien
J. Paldus

The management and Board of Directors of the Institute wish to express their profound thanks to the following individuals, whose generous donations in the period April 2006 – March 2007 are helping to support the work of the Institute.

Doug Park
Neil Price-Jones
QWEMA Group Inc.
Carl and Elaine Riehm
Chris Robinson, in honour of
 Fred and Fran Robinson
Tom Salisbury
Gerald Schwarz
Sankar Sitaraman
Juris Steprans
Mary E. Thompson
James G. Timourian
Hans Tuenter
Dan-Virgil Voiculescu
Daniel Wevrick
Thomas P. Witelski
Grant Woods
Graham Wright
Noriko Yiu
Xiaowen Zhou
Anonymous (4)

2007 Fields-Carleton Lecturer– J. Marsden
continued from page 4

Marsden illustrated that LCS answers these and other types of questions through the use of recently developed theoretical and computational methods in dynamical systems.

In his second lecture, Marsden discussed discrete mechanics and its fascinating spectrum of applications. With major input from Marsden over the last 5 years, the theory and computation for mechanical systems have been developing based on discrete mechanics and discrete variational principles of mechanics, resulting in algorithms that respect the geometric structure of mechanics and at the same time offer very efficient methods with none of the undesirable effects of the numerical dissipation associated with generic algorithms. These ideas are applicable not only to finite-dimensional mechanical systems, but also to those described by partial differential equations.

As multiple applications—such as six hovercrafts arranging themselves in a hexagon in an optimal way, or a falling cat—provided by the speaker demonstrated, variational methods are excellent not only for large systems, but for long term simulations too. Moreover, for systems with complicated dynamics, the structure of chaotic sets is captured as well. The diverse applications to time stepping—e.g. to nonlinear elasticity and to optimal control—illustrated the power of the discrete mechanics methods.

Rouslan Krechetnikov (Carleton)

Call for Proposals, Nominations, and Applications

For detailed information on making proposals or nominations, please see the website: www.fields.utoronto.ca/proposals

General Scientific Activities*

Proposals for short scientific events in the mathematical sciences should be submitted by October 15 or March 15 of each year, with a lead time of at least one year recommended. Proposals will be considered at other times as funds permit. Activities supported include workshops, conferences, seminars, and summer schools. If you are considering a proposal, we recommend that you contact the Director, Barbara Keyfitz, or Deputy Director, Juris Steprans (proposals@fields.utoronto.ca)

Thematic Programs *

Letters of intent and proposals for semester long programs at the Fields Institute are considered in the spring and fall each year, and should be submitted by March 15 or August 31. Organizers are advised that a lead time of several years is required, and are encouraged to submit a letter of intent prior to preparing a complete proposal. They should consult the directorate about their projects in advance to help structure their proposal.

Postdoctoral Opportunities

Applications are invited for postdoctoral fellowship positions for the 2008-2009 academic year. The thematic program on **Arithmetic Geometry, Hyperbolic Geometry and Related Topics** will run in the fall of 2008, and the program on **o-Minimal Structures and Real Analytic Geometry** in winter/spring 2009. Qualified candidates who have recently completed a PhD in a related area of the mathematical sciences are encouraged to apply. The fellowships provide for a period of engagement in research and participation in the activities of the Institute. They may be offered in conjunction with partner universities, through which a further period of support may be possible. One recipient will be awarded the Institute's prestigious Jerrold E. Marsden Postdoctoral Fellowship. Applicants seeking postdoctoral fellowships funded by other agencies (such as NSERC or international fellowships) are encouraged to request the Fields Institute as their proposed location of tenure, and should apply to the address below for a letter of invitation. Additional support is available from NSF to support junior US visitors to this program. Applications are encouraged from all qualified candidates, particularly aboriginal peoples, persons with disabilities, members of visible minorities and women.

The deadline for postdoctoral applications for the 2008-2009 programs is December 7, 2007, although late applications may be considered. Postdoctoral opportunities also exist at some of the Fields Institute's sponsoring universities. Consult www.fields.utoronto.ca/proposals/#pdf for details.

CRM–Fields–PIMS Prize

Nominations are invited for this joint prize in recognition of exceptional achievement in the mathematical sciences. The candidate's research should have been conducted primarily in Canada or in affiliation with a Canadian university.

Please send nominations to: The Deputy Director, Fields Institute, 222 College Street, Toronto, Ontario, M5T 3J1 Canada

Nominations for the CRM-Fields-PIMS Prize should reach the Fields Institute by November 1, 2007.

Distinguished Lecture Series in Statistical Science (DLSS)

Nominations are being solicited for the eighth Fields Institute Distinguished Lecture Series in Statistical Science, to be given in spring 2008. The awardee will be an internationally prominent statistical scientist, who will give two lectures (one general, one specialized) at the Fields Institute. Nominations for the DLSS should reach the Institute by October 1, 2007.

***A note on diversity. In proposing any activity, applicants are requested to consider the mandate of the Institute to broaden and enlarge the community.** Applicants should explain how they plan to include women and members of visible minority groups in the proposed activity. As well, they should ensure that the proposed participant lists include scientists representing a range of career levels, types of institutions and geographical locations in Canada and abroad.

Fields Activities

Chalk it up to Mathematics



JUNE – SEPTEMBER 2007

FIELDS

at Fields unless otherwise indicated

Detailed information: www.fields.utoronto.ca/programs

Thematic Programs

THEMATIC PROGRAM ON OPERATOR ALGEBRAS

JULY–DECEMBER, 2007

Organizers: George Elliott (chair, Toronto), Dietmar Bisch (Vanderbilt), Joachim Cuntz (Münster), Kenneth Davidson (Waterloo), Thierry Giordano (Ottawa), Roland Speicher (Queen's)

JULY 16–20, 2007

Workshop on Noncommutative Dynamics and Applications

SEPTEMBER 17–21, 2007

Workshop on Free Probability, Random Matrices, and Planar Algebras

This program has obtained support from the National Science Foundation. Post-doctoral students and junior researchers from US universities are encouraged to apply for funding.

General Scientific Activities

JUNE 1–3, 2007

16th International Workshop on Matrices and Statistics
University of Windsor

JUNE 5–8, 2007

Probability and Stochastic Processes Symposium in honour of Donald A. Dawson's work, on the occasion of his 70th birthday
Carleton University

JUNE 5–9, 2007

35th Canadian Operator Symposium (COSy)
University of Guelph

JUNE 18–23, 2007

Conference on Combinatorics and Optimization
University of Waterloo

JUNE 21, 2007

Fields Annual General Meeting

JUNE 27–29, 2007

Randomization of Quantum Systems Workshop
Institute for Quantum Computing,
University of Waterloo

JULY 2007

Combinatorial Pattern Matching Workshop
University of Western Ontario

JULY 7, 2007

Future Directions of Computational and Mathematical Neuroscience

JULY 17–19, 2007

Fields Institute Summer Workshop on Environmetrics
University of Waterloo

JULY 18–21, 2007

CUMC 2007 Canadian Undergraduate Mathematics Conference
Simon Fraser University

JULY 25–28, 2007

Symbolic–Numeric Computation (SNC'07) and Parallel Symbolic Computation '07 (PASCO '07)
University of Western Ontario

JULY 27, 2007

Brain Biomechanics: Mathematical Modelling of Hydrocephalus and Syringomyelia

JULY 29–AUGUST 1, 2007

International Symposium on Symbolic and Algebraic Computation (ISSAC2007)
University of Waterloo

AUGUST 9–13, 2007

Summer School in Iwasawa Theory
McMaster University

AUGUST 13–17, 2007

6th International Conference on Unconventional Computation
Queen's University

AUGUST 12–16, 2007

2nd International Conference on Continuous Optimization ICCOPT – MOPTA07
McMaster University

AUGUST 13–24, 2007

Summer School on Operator Algebras
University of Ottawa

AUGUST 27–29, 2007

Automata 2007, 13th International Workshop on Cellular Automata

SEPTEMBER 4–7, 2007

Data Assimilation Workshop

SEPTEMBER 22–24, 2007

Geometrization of Probability Workshop
University of Ottawa

MESSAGE FROM THE DIRECTOR

A Boon for the Mathematical Community



Barbara Keyfitz

WRITING LAST NOVEMBER, I DESCRIBED the new envelope, *Major Resources Support*, designed by NSERC to give the Mathematics Institutes a stable funding home. At the end of March we received excellent news. The three institutes collectively garnered 60% of the million-dollar increase that NSERC had put into the MRS competition. We were also very impressed with the quality of the site visit team; the fact that such distinguished people agreed to serve is a comment on our reputations, and the fact that such an excellent team was put together indicates NSERC's commitment to giving the institutes a fair hearing. We were able to make our case to a committee consisting mainly of people outside of mathematical sciences. The congratulations go, of course, to the whole community: each institute

had enormous help from many people in putting together the proposals and the site visits.

After a period of nine months in which the three mathematical sciences institutes were placed in direct competition with each other, we are now able to return to the normal state of cooperation. We all, in our proposals, made a commitment to work together to achieve common objectives that will benefit the Canadian community: providing support jointly for important events like the 2008 Canada-France meeting and ICIAM 2011, working with AARMS and NPCDS to help them obtain stable funding, and helping to plan a national network.

Not all NSERC news was good: the increase in funding for the institutes came during a year that Discovery Grants in Mathematical Sciences were severely cut. Even though NSERC announced the budget increase to MRS last summer, long before the Discovery Grants competition of this year, and before it had been decided that the mathematics institutes would even enter the MRS competition this year, there is an unhappy suspicion that one mathematical enterprise might have profited at the expense of the other. We trust this is not the case. NSERC has long supported "individual investigator" or discovery grants as the key support for fundamental research, holding out the image of curiosity-driven creativity. The institutes have made a case for a different picture: mathematics as a group activity, the value of communica-

tion and interaction, and the benefit of an international window for Canadian mathematics. The two modes of research – discovery and communication – coexist in mathematics, as in every field. The very fact that the institutes support different activities from those supported by discovery grants emphasizes the difference. For example, Fields, while offering graduate courses as part of each thematic program, does not run graduate programs, offer degrees, or support graduate students for longer than a semester. Furthermore, the Canadian institutes could not run as efficiently as they do were it not that most Canadian mathematicians are able to pay some of the costs of their participation from their own grants. The two programs complement each other, and although the discovery grants program is much larger (the ratio in mathematical sciences is about 7:1), almost every mathematician in Canada benefits in some way from institute programs. Now that the competition is over, the institutes have resolved to work together to help make the case with NSERC for restoration of funding cuts to the discovery grants program.

In the last Fields Notes we also mentioned that we hoped to gain some new Affiliates. That hope has been realized: Three new Affiliate Members are joining Fields: Nipissing University, University of Ontario Institute of Technology, and Wilfrid Laurier University. We welcome them, thank them for their support, and urge them to take advantage of all our events.

FIELDS INSTITUTE
Research in Mathematical Science
222 COLLEGE STREET, 2ND FLOOR
TORONTO, ONTARIO,
CANADA M5T 3J1
Tel 416 348.9710 Fax 416 348.9714
www.fields.utoronto.ca



FIELDS