Geometric Applications of Homotopy Theory

This winter’s Fields thematic program will study and develop new applications of homotopy theory in algebraic geometry, mathematical physics and related disciplines. There will be three subprograms devoted, respectively, to the study of higher categories, the homotopy theory of schemes, and stacks in geometry and topology. The program organizers are Gunnar Carlsson from Stanford University, and Dan Christensen and Rick Jardine, both from the University of Western Ontario.

The purpose of mathematical technique is to understand the workings of – and to see the patterns behind – complicated phenomena. Mathematics is used throughout Science and Engineering to develop theoretical models for the observed behaviour of physical systems, and then analyze discrepancies between these models and experimental data. These same general methods also apply within Mathematics, to the study of mathematical objects in and of themselves.

Homotopy theory is a suite of tools which has been developed over the past hundred years to distinguish geometric and topological objects through the assignment of algebraic invariants to the objects. These invariants, such as homology and homotopy groups, are among the fundamental objects of modern Mathematics, and the formal theories surrounding them have been studied in great depth. The applications of homotopy theory, however, have always defined the most compelling aspects of the subject.

Traditionally, homotopy is defined to be a variational principle which transforms one map (or space) to another continuously through what is usually thought of as a time variable. Thus, for example, a solid sphere is homotopy equivalent to a point, and the homotopy that shrinks the sphere to the point at its centre can be easily visualized. On the other hand, a hollow sphere has a hole inside, which can be detected by its homology groups: it has a non-trivial higher homology group while a point does not, and since homology is a homotopy invariant the hollow sphere cannot be deformed to a point.

Historically, many of the applications of homotopy theory arose through discrete, purely set-theoretic models of...
in cryptographic problems like computation on encrypted data – e.g. the tallying of electronic votes while preserving secrecy – and delegation of cryptographic ability. Goldwasser showed that the first proposed definition of what constitutes a good obfuscator could be weak in the context of multiple obfuscations. She introduced the concept of an obfuscator that is secure with regard to auxiliary output – extra information available to an attacker, possibly including the result of previous obfuscations. She then proved that there exist large families of natural functions that cannot possibly be obfuscated securely, no matter if the auxiliary input is independent or not of the function we would like to obfuscate (although the functions may be different in the two cases), showing that there are theoretical limits to what can be obfuscated.

In her second lecture, Goldwasser presented an approach that can be used to prove that a function is a hardcore predicate. A predicate \( P \) (a function that returns “true” or “false”) is hard core for a function \( f \) if computing \( P(x) \) better than a random guess is as hard as inverting \( f \). Such a situation is essential for cryptographic one-way functions since they must be functions for which computing \( f(x) \) for a given \( x \) is relatively easy, but obtaining \( x \) only from the value of \( f(x) \) is computationally hard. For these functions, we are interested in segment predicates, i.e. predicates that can be transformed into a predication that changes value only polynomially many times in the bit size of \( x \) – for example “Is the \( k \)-th bit 1?” Using a number of tools, ranging from coding theory to Fourier analysis, Goldwasser showed that any segment predicate is a hardcore predicate for three types of functions, namely those occurring in RSA encryption, finite field exponentiation and scalar multiplication of a point on an elliptic curve. The security of these three functions is essential to many cryptosystems, and this result was of great interest to many of the participants in the thematic program in cryptography.

Nicolas Theriault (Fields Institute)
FOR HOW MANY MATHEMATICIANS WILL A group of Undergraduate students charter a bus and drive over 100 kilometers to hear a lecture at Fields? The Waterloo Math Society organized a busload on October 20, 2006, at four dollars a head, to come to Fields for a talk by James Dickson (JD) Murray. Murray was actually on his way to receive an honorary DMath degree from Waterloo the next day. This was to add to his doctorate in Applied Mathematics at the University of St. Andrews (Scotland), and D.Sc. at Oxford. His citation mentions:

Murray is a pioneer in the field of mathematical biology, including advances in the modeling and analysis of factors behind the spread of rabies. He has identified new areas of research in mathematical biology and his ideas have been applied to a number of pattern formation problems in developmental biology, wound healing and problems in modeling the growth of cancers.

Murray has many other honours. He is also a Fellow of the Royal Society of Edinburgh (FRSE) and a Fellow of the Royal Society (FRS). He stopped at Fields to give a talk entitled On the Virtues of Simple Models in the Biomedical Sciences, organized by the Centre for Mathematical Medicine.

Murray is an author and coauthor of many books including The Mathematics of Marriage: Dynamic Nonlinear Models, but he is especially known for his wonderful mathematical biology books. These introduce a reader with little formal training in biology to the practical application of mathematical models to help unravel the underlying mechanisms of biological processes. Many believe that biology will provide the inspiration for mathematics in this century that physics did a hundred years ago. Murray has helped lead the way. In his mathematical biology books, he introduces topics such as the mechanical theory of vascular network formation, geographic spread and control of epidemics, and wolf-deer interactions and deals with them with real mathematical tools such as differential equations. His models are based on genuine biological problems; his predictions and explanations result directly from a mathematical analysis of the models.

He talked first about the growth of brain tumours, introducing a mathematical model of gliomas based on proliferation and diffusion rates. He showed that one could simulate model tumours and achieve good agreement with clinically observed tumour geometries and suggested paths of tumour invasion not detectable on MRI images. This gives insight into microscopic invasion of the human brain by glioma cells and predicts pathways of glioma cell invasion. Hence one identifies regions of the brain where treatments should be focused.

In predicting marriage stability and divorce he showed how to quantify a 15-minute discussion of a topic of the couple’s choice and then apply the measured results. Based on a longitudinal study of a large number of newlywed couples, it was found that there was a 94 per cent accuracy of prediction of marital stability. The testers score anger and active listening and other factors to build a model whose scores have remarkable social predictive potential.

The best thing about Murray’s talk was that the listeners easily understood the models and examples. He promised to keep the models simple, but not the applications, and he delivered. This listener left with the determination to read at least one of his books.

Irwin Pressman (Carleton)

the introduction and development, in the hands of Hopkins and his collaborators, of elliptic cohomology theories and the theory of topological modular forms.

Higher category theory concerns higher level notions of naturality, which can be expressed as maps between natural transformations, maps between such maps, and so on: that is, “maps between maps between maps ...” The need for a higher categorical language has become apparent, almost simultaneously, in mathematical physics, algebraic geometry, computer science, logic, and, of course, category theory itself. Such a language and a relevant body of results are already implicit throughout algebraic topology, where analogous higher homotopies have been in use since the 1950s in the definition and analysis of homotopy coherence problems. Many of these developments have connections to physics, and to conformal and topological quantum field theory in particular.

Similar ideas are present in new applications of homotopy theory in computer science, in models for concurrent behaviour of parallel processing systems, computational geometry, and complexity. Homotopy theory also has subtle applications in combinatorics – for example in analysis of hyperplane arrangements, and in problems related to graph colouring.

The algebraic, combinatorial nature of modern homotopy theory is the basis of its applications, and the subject and its techniques have become ubiquitous. It is also increasingly apparent that the full scale of the utility of homotopy theoretic ideas has yet to be discovered.

Rick Jardine (Western)
The series of Grad Day events has been organized by the Fields Institute for the past several years to provide local (and sometimes not so local) universities the opportunity to tell undergraduates planning to go to graduate school about their programs. This year’s event, held on Saturday, November 18, 2006, attracted over thirty students, the largest contingent being from Waterloo, but with Western, York and Toronto also being well represented. The list of departments that set up booths included the Mathematics departments from Carleton, Ottawa, Waterloo, Western, Manitoba, Guelph, OUIT as well as York’s Computer Science department. There were booths from both McMaster’s Computational Engineering department and its Mathematics and Statistics departments while the University of Toronto had representatives from Mathematics, Statistics and Computer Science.

The booths were all set up by just after noon and students had plenty of time to talk to representatives. An interesting phenomenon observed was that students seemed reluctant to approach the representative tables individually, preferring, rather, to move from stand to stand collectively. A satisfactory explanation for this behaviour remains to be found.

At 1:00 Renate Scheidler gave an interesting and accessible talk about the history of cryptography – as we learned, the more accurate way to refer to the subject is cryptology, which combines the encryption of data (cryptography) and its decryption (cryptanalysis).

The most common type of encryption historically was the “shift cipher”, where each letter is replaced by the letter which appears K letters later in the alphabet. As an example she mentioned that HAL of 2001: A Space Odyssey fame, when encrypted with K = 1, is IBM. K = 3 was used by Julius Caesar and became known as the “Caesar Cipher”.

Another kind of encryption widely used historically was the “transposition cipher”, in which the letters are scrambled. Both this and the shift cipher can be broken easily by a computer using statistical methods. In order to make these historical ciphers more secure, the two methods were at one time used in succession many times.

Perhaps one of the best known encryption systems was Enigma, invented in Poland by A. Scherbius in the 1920s, and widely used by Germany in World War II. It had actually been broken in the 1930s by 3 Poles, M. Rejewski, H. Zygalski, J. Rózyski, and then once more by British mathematicians during the war – among them W.T. Tutte and Alan Turing.

Another of the difficulties with encryption/decryption is the safe transmission of the “key”. There are two solutions to this problem – Public Key Cryptography and Key Establishment Protocols.

In Public Key Cryptography, the fictional sender, Alice, has both a public and a private key. The public key can be used by anyone to send her an encrypted message which can only be easily deciphered with the private key. This is accomplished by basing the keys on a mathematical problem which is (at least perceived to be) very difficult to solve. This method was invented by two Americans W. Diffie and M. Hellman in 1976 – but then it was later discovered that they had been anticipated a few years earlier by J. Ellis in the U.K. The most widely used system based on this idea is RSA – introduced by 3 MIT students Rivest, Shamir and Adleman in 1978, and relies on the difficulty of finding the prime factors of large integers.

The RSA method is rather slow and is now more often used to exchange cryptographic keys for the more traditional methods of encryption, such as AES.

More recently elliptic curve cryptography (ECC) has come into widespread use, using the group law on elliptic curves. And other sophisticated methods involving number theory and such things as algebraic geometry and cohomology are also coming into use.

Another important application of cryptography is the digital signature, which makes authentication possible within electronic communication. In this case, in order to “sign” a message “m”, Alice sends both “m” and an encrypted version “s” obtained by using her private key. Then Bob can verify that “m” really came from Alice by using her public key to decrypt s. In algebraic terms, this means that decryption must be a right inverse as well as a left inverse to encryption (if we think of the operations being written on the left).

Scheidler finished by talking about more futuristic methods, namely quantum cryptography and quantum information science. The former is based on the laws of physics, rather than mathematical problems, and is already in use. The latter – quantum information science – designs techniques for breaking public key cryptosystems and would break any public key cryptosystem currently in use. But its practical implementation is apparently not in sight.

After the talk there was pizza and a chance for students to talk further with the graduate department representatives. It was close to 4:00 by the time the last booth was packed up and Grad Day 2006 came to an end – a successful end, we believe.

Carl Riehm and Juris Steprans
(Fields Institute)
The first recipient of the CRM-Fields-PIMS Prize, Nicole Tomczak-Jaegermann, gave her prize lecture at the Institute on November 20. The prize is the successor to the CRM-Fields Prize and is now supported by all three institutes. Several of those honoured by the earlier prize were in attendance to listen to Tomczak-Jaegermann’s lecture entitled, High dimensional convex bodies: phenomena, intuitions and results.

The starting point of the talk was the concentration of measure phenomenon which is familiar from instances such as the law of large numbers or the concentration of the uniform measure of the large dimensional sphere near the equator. This sort of phenomenon presents a more sophisticated sphere near the equator. This sort of the uniform measure of the large dimension has a central section of reasonably large dimension. A variation due to V. Milman gives bounds on the numbers involved:

“each centered convex body of sufficiently high dimension has a central section of reasonably large dimension.”

Every normed space of dimension \( n \) has an almost Euclidean subspace of dimension \( k > c \log(n) \) for some constant \( c \). The notion of almost Euclidean depends on the Banach-Mazur distance between two subsets of a linear space: Roughly speaking \( A \) and \( B \) are a distance \( \lambda \) apart if \( A \) can be moved so that it is sandwiched between \( B \) and \( \lambda B \).

The general nature of the questions considered by Tomczak-Jaegermann is whether a given property is ubiquitous in sufficiently high dimensions. A space may fail to have the property for trivial reasons, but it may still be the case that many subspaces do have the property. For example, a property may be destroyed by multiplying with a small factor but the product will still have a large subspace with the desired property. In this context the notion of saturation is introduced: A space \( V \) is said to saturate the space \( X \) (with respect to a given integer \( n \)) if every subspace of \( X \) of dimension at least \( n \) contains a copy of \( V \). Work of Tomczak-Jaegermann and Szarek shows that any space can saturate some space with respect to a suitable \( n \).

In the same circle of ideas is the problem of reconstruction of a vector from random measurements. Given a subset \( T \) of \( n \)-dimensional Euclidean space and \( k \) random vectors \( X_i \) where \( k \) is much smaller than \( n \), if one knows the inner product of a vector \( t \) from \( T \) with each \( X_i \) can one determine \( t \)? Earlier work of Candes and Tao on \( T \) being the unit ball in powers of \( l_1 \) inspired Tomczak-Jaegermann, Mendelson and Pajor to extend these results to other geometric structures and different probability distributions. The concentration of measure phenomenon plays a central role in their analysis of this class of problems. A related question that yields to this sort of analysis is that of exactly reconstructing a sparse matrix from random measurements. The surprising result is that this can be done if \( k > C \log(n/r) \) where \( n \) is the length of the vector, \( r \) the number of non-zero coordinates, \( k \) the number of random measurements and \( C \) is a suitable constant.

A polytope is called \( m \)-neighbourly if any \( m \) of its vertices is the vertex set of some face. If \( n \) vectors consisting of 1’s and -1’s are chosen at random in \( k \)-dimensional Euclidean space then they are almost certain to be \( m \)-neighbourly provided that \( m \log(Cn/k) < c k \) for constants \( C \) and \( c \).

The last part of the talk dealt with metric entropy. This concept deals with the packing and covering number familiar from geometric measure theory. The covering number \( N(K,B) \) is the least number of translations of \( B \) required to cover \( K \) while the packing number \( M(K,B) \) is largest number of disjoint translations of \( B \) by elements in \( K \). These numbers can be used to associate to each operator on a linear space a sequence of entropy numbers and, in the case of a compact operator \( U \), the limiting behaviour of the entropy sequence of \( U \) is the same as that for \( U^* \). The Duality Conjecture of Pietsch asks whether the rates of convergence of the two sequences of entropy numbers are similar. Tomczak-Jaegermann introduced a convexified version of these numbers that, unlike the classical case, is sensitive to the ordering. These ideas were used to amplify earlier results on the Duality Conjecture.

The selection of results provided a fascinating insight into the problems and methods, as well as the potential applications, of the study of asymptotic geometric analysis.

Juris Steprans (Fields Institute)
First Canadian-Ukrainian Summer School

The participants in this Summer School, that took place from August 14-26, 2006, were eight Ukrainian undergraduate students selected from the two largest mathematical centres in Ukraine, Kyiv and Kharkiv, Canadian students from local universities, and several postdocs and visitors to the Institute. All of the instructors were from the University of Toronto.

We were very pleased with the results of the School and excited by the mathematical level of the participants. The School centered on dynamical systems: two mini-courses were given by the organizers, complemented by two beautiful lectures by G. Forni, Y. Karshon and B. Khesin introduced the students to symplectic geometry, motivating it by Hamiltonian dynamics. D.Bar Natan taught the students to tie some very sophisticated knots, as a motivation for the introduction of the polynomial knot invariants. I. Binder and J. Quastel described a probabilistic approach to dynamics in their lectures, and introduced the students to such hot subjects as SLE, and stochastic PDEs. K. Murty gave an excursion into the mind of Pierre Fermat, at the time that he made the famous note on the margins which became known as the Fermat’s Last Theorem. He also described several fascinating open questions related to the theory of elliptic curves, and tempted the students with a Clay one million dollar problem – the Birch and Swinnerton-Dyer Conjecture.

On a lighter note, there was a pizza party at the Institute at which the students mingled with the lecturers, and a trip to Niagara Falls was, of course, included in the program.

We see the School as a promising start, and hope that it will become a regular event at the Institute.

It is a pleasure to acknowledge the generosity of the sponsors who made the Summer School possible: the Fields Institute; the Department of Mathematics at the University of Toronto; the Department of Mathematics and Computational Sciences at the University of Toronto at Mississauga; and Aerosvit Ukrainian Airlines. The School was also partially supported by contributions from several individual NSERC grants.

Konstantin Khanin and Michael Yampolsky (Toronto)

Workshop on Computational Challenges Arising in Algorithmic Number Theory and Cryptography

This was the third in a series of four workshops representing part of the activities of the Thematic Program in Cryptography held at the Fields Institute during the fall of 2006 and it took place from October 30-November 3, 2006.

Number theoretic problems lie at the heart of most public key cryptosystems in use today. The underlying idea is to base the security of such a cryptographic technique on a problem from number theory or arithmetic geometry that is widely believed (though generally not proved) to be extremely difficult. The only way an adversary knows how to break such a scheme is to solve an instance of this hard problem. The challenges faced by researchers who design and analyze such systems are both mathematical and computational in nature.

Twenty-six speakers from institutions spanning eight different countries presented state of the art research on a wide variety of subjects in computational number theory and cryptography. Not surprisingly, elliptic curves and other algebraic curves of low genus featured prominently, since curve-based cryptography is a very active area of research that also has commercial applications. Other topics included constructive questions in algebraic number fields and function fields, prime generating sequences, efficient matrix computations, factoring sparse polynomials, signature schemes, provable security, and public key cryptosystems based on lattices, tori and multivariate polynomials.

The workshop schedule left ample time for informal meetings and research discussions. Social activities included a reception for all participants at Fields as well as a conference banquet.

A special feature of the event was an informal presentation by Hugh Williams entitled My reminiscences of Emma Lehmer. Together with her late husband Dick Lehmer as well as Dick’s late father (and Emma’s supervisor) Derrick Lehmer, Emma was one of the early pioneers in the field of computational number theory. Still in good health, she celebrated her 100th birthday on November 6 in Berkeley, California.

Renate Scheidler (Calgary)
Workshop on How I Became a Quant: Financial Engineers Give a Personal View of their Careers in Quantitative Finance

IN THE EVENING OF OCTOBER 17, 2006, the Fields Institute hosted over 120 students and industry participants for the successful event How I Became a Quant, organized by the International Association of Financial Engineers (IAFE) and sponsored by Numerix, a leading software provider in cross asset derivatives pricing.

Financial engineering is a relatively new discipline dedicated to providing and implementing practical solutions to economic and financial problems, which result from the social interactions of humans, rather than problems that originate in physics, chemistry or biology. Essentially, financial engineering can be seen as a cross-disciplinary field which relies on mathematical finance, numerical methods and computer simulations to make trading, hedging, investment and business decisions, as well as to facilitate the risk management of those decisions. Its application today extends well beyond traditional trading and financial markets into commercial and retail banking, commodities, portfolio management, insurance, and environmental problems, as well as corporate investment decisions and project planning in general.

The recent explosive growth in quantitative finance has led mathematics, physics, computer science and engineering students of all levels to wonder whether a career or an advanced degree in quantitative finance is right for them. With the rapid increase in sophisticated quantitative and computational techniques employed in financial firms there has been increasing demand for students with highly quantitative backgrounds to work in the financial field and an increase in advanced degree programs covering these topics.

Organized by the IAFE Education Committee and the Fischer Black Memorial Foundation, the “How I became a Quant” series are panel discussions for students interested in a career in quantitative finance. These events have been previously held in New York, London, Berkeley and Boston. The Toronto event was moderated by John Hull, the Maple Financial Group Professor of Derivatives and Risk Management at the University of Toronto and IAFE Senior Fellow. Featured panelists included Barry Schachter, Chief Risk officer of Moore Capital Research, Jonathan Schachter, Vice President Financial Engineering at Numerix (both from NY) and Michael Zerbs, President and COO of Algorithmics in Toronto.

This type of forum is designed to give a personal view of the world of quantitative finance from the point of view of professionals with varying specialties. Without formulas or Power Point presentations, the panelists shared their own experiences and engaged in a moderated discussion with plenty of student questions. Finally, as part of the event, a reception for students and panelists was held after the panel. The Fields Institute is now well established as an important catalyst for bringing together academics, practitioners and students in quantitative finance with events such as the prestigious Quantitative Finance seminar series now running for over a decade, as well as the PRMIA Risk Management Seminars and courses. The great attendance and success of “How I became a Quant” further demonstrate the growth and interest in this field as well as the vital role that the institute continues to play.

Dan Rosen (R2 Financial Technologies Inc.)

WORKSHOP ON ELLIPTIC CURVE CRYPTOGRAPHY (ECC 2006)

HELD AT THE INSTITUTE ON SEPTEMBER 18–20, 2006, was the 10th Workshop on Elliptic Curve Cryptography, an annual event that has been held since 1997. This year’s event was organized by Mark Bauer (Calgary), Tanja Lange (Eindhoven), Alfred Menezes (Waterloo), Kumar Murty (Toronto), Christof Paar (Bochum), and Scott Vanstone (Waterloo). The purpose of the first workshop was to encourage the study of the elliptic curve discrete logarithm problem, whose hardness is the basis for the security of elliptic curve public-key cryptosystems.

Over the years, the workshop has broadened its scope to cover all issues related to curve-based cryptography including the discrete logarithm problem, efficient curve arithmetic, efficient parameter generation, protocols, side-channel attacks, and deployment.

At ECC 2006 there were lectures on three topics that are actively being researched: algorithms for the discrete logarithm problem, the security and efficiency of hyperelliptic curve cryptosystems, and pairing-based cryptography. For the first time, L(1/3) subexponential-time algorithms were presented for the discrete logarithm problem in the Jacobians of certain classes of algebraic curves. State-of-the-art implementations of the arithmetic on genus-two hyperelliptic curves were described, showing that low-genus hyperelliptic curve cryptosystems are indeed competitive (and in some cases better than) their elliptic curve counterparts. Attendees were kept abreast of the latest techniques for generating low-embedding elliptic curves that are crucial for pairing-based cryptosystems, and the fastest method for implementing the Tate pairing. Several new research directions were considered, including the use of generalized Jacobians in cryptography, and the use of isogenies between supersingular elliptic curves to design provably-secure hash functions.

ECC 2006 was attended by 107 researchers and graduate students. There were 18 invited lectures, and a rump session consisting of short (and humourous) presentations about recent results and work in progress.

ECC 2007 will be held from September 5-7 2007 at University College Dublin.

Alfred Menezes (Waterloo)
The unexpected and sometimes surprising behaviour of conditional probabilities was demonstrated by a personal example from Rosenthal’s own experience with medical tests. He recounted his reaction at learning that a test for an unpleasant disease had returned positive. His initial anxiety was tempered with the statistician’s analysis of the information provided him. Even though the possibility of a false positive was distressingly low, Rosenthal explained why this, coupled with the known chances of any one individual having the disease in question, comforted him. The reader will be pleased to learn that a subsequent test did return negative and that Rosenthal was apparently in very good health. The technique of relating questions in statistics to his own experience, such as his misgivings about flying and how his knowledge of statistics mitigated them, was warmly accepted by the audience.

The lecture was punctuated with interesting graphics illustrating concepts from probability at an elementary level. Rosenthal opted to emphasize the content underlying the graphics rather than relying on cute special effects. For example, a simple moving dot recording the current wealth of a gambler was used to illustrate the gambler’s ruin phenomenon and the audience was clearly fascinated watching the progress of the animation.

Another example along these lines was his illustration of an answer to the question: What does randomness look like? The audience was asked to guess which of two distributions of dots on the plane was random, the seemingly uniformly distributed example or the one which seemed to display clumping.

The usual request for questions at the end of the talk produced a sea of hands and it was impossible to answer all of them. It was clear though that the general public has a much higher level of interest in mathematics than is often assumed, especially when delivered with such verve and clarity.

The audience was clearly fascinated watching the progress of the animation.

At the summit? Why didn’t they install escalators again?

Another example along these lines was his illustration of an answer to the question: What does randomness look like? The audience was asked to guess which of two distributions of dots on the plane was random, the seemingly uniformly distributed example or the one which seemed to display clumping.

The usual request for questions at the end of the talk produced a sea of hands and it was impossible to answer all of them. It was clear though that the general public has a much higher level of interest in mathematics than is often assumed, especially when delivered with such verve and clarity.
Workshop on Quantum Cryptography and Computing

FROM OCTOBER 2–6, 2006, FIELDS HOSTED the Quantum Cryptography and Computing workshop, organized by Richard Cleve (Calgary), Claude Crépeau (McGill) and Michele Mosca (Waterloo). The main theme of this workshop was information security in a quantum setting. The event brought together classical (or “non-quantum”, as one speaker preferred) and quantum cryptographers in an effort to bridge the gap between the two worlds.

The week’s talks could be roughly divided into three subjects.

1) One group of talks addressed protecting classical information using quantum techniques such as quantum key distribution (QKD); here, talks addressed a variety of topics, including security definitions for QKD, experimental and commercial projects, and the relationship between key distribution and quantum communication. Some speakers also talked about the protection of classical information in the context of quantum computation, addressing the security of classical cryptography.

2) Another set of speakers discussed protecting quantum information, focusing on encryption of quantum states using perfect or approximate quantum encryption schemes.

3) A large number of talks were concerned with foundations for secure quantum computation. These talks addressed quantum versions of many classical secure computation problems, such as zero-knowledge, string commitment, coin flipping, and secure distributed or multi-party computation, but also addressed some topics only relevant to quantum computation, such as ensuring that a quantum circuit performs the intended operation.

In addition to a range of theoretical computer scientists and mathematicians, attendees heard from experimental physicists on implementations of quantum key distribution (QKD) and from industrial researchers on deployments of QKD in a real-world environment. Most talks included a vigorous question-and-answer session, demonstrating the intensity of ongoing research in the field.

The highlight of the week was the panel discussion featuring cryptographers of all backgrounds addressing two questions: “What are the killer apps for quantum key distribution?” and “What are the main obstacles to widespread QKD use?” While quantum cryptographers argued that the long-lasting security of QKD (both in terms of the security of transmitted information as well as the long-lasting utility of a QKD infrastructure, once installed) might be the killer app for QKD, the non-quantum cryptographers noted that killer apps are rare in practice and that getting well-known backers (such as government agencies) to support the technology might itself be a killer app. Panelists noted that current limitations on distance and the present lack of quantum repeaters are certainly obstacles to widespread adoption, but so too is the lack of standardization, certification, and verification of devices.

The panel, and indeed the workshop, concluded with a sentiment of cautious, but realistic, optimism for the future applicability of quantum key distribution, emphasizing the need for continued theoretical and experimental research in the area.

Douglas Stebila (IQC, Waterloo)
Summer School and Conference in Valuation Theory and Integral Closures in Commutative Algebra

The Summer School and Conference in Valuation Theory and Integral Closures in Commutative Algebra was held from July 2 to July 22, 2006 at the University of Ottawa. About 30 graduate students and young researchers from Canada, the U.S., Europe and the Middle East attended the summer school, and stayed on for the conference.

The first week was dedicated to morning lectures on valuation theory by Franz-Viktor Kuhlmann and Hagen Knaf, and afternoon lectures on integral closures given by Irena Swanson. The goal was to introduce students to the two areas simultaneously, and to demonstrate how these subjects interact.

The second week consisted of more advanced lectures about recent applications of valuation theory to resolution of singularities and related topics by Cutkosky, Kuhlmann, Knaf, Vaquie and Teissier. Teissier as well as Kuhlmann and Knaf gave an introduction to their approaches to local uniformization, which is a local form of resolution of singularities.

The afternoons focused on practical aspects of computing integral closures using various computer algebra programs. Winfried Bruns, Amelia Taylor and Irena Swanson led the lab sessions.

In the evenings the students gathered in the lounges at the University of Ottawa housing center to discuss problems assigned during the day. The students did a great job working on the problems, most of the time without additional support from the professors during these discussion sessions. (But when it came to playing the immensely successful “Mafia” game afterwards, they were heavily supported by the professors!)

The third week was dedicated to a conference on valuation theory and integral closures with about 50 participants, and 20 invited and 5 contributed lectures. The summer school students were prepared for the conference lectures after two weeks of introductory work. We also had the opportunity to celebrate the 76th birthday of Shreeram Abhyankar at the end of the conference.

The city of Ottawa with its nice restaurants, events and attractions provided a wonderful background for great interaction between the lecturers and the students.

The event was supported by the Fields Institute, the US National Science Foundation, and the University of Ottawa.

Sara Faridi (Dalhousie/Ottawa) and Franz-Viktor Kuhlmann (Saskatchewan)
Conference on Nonparametric Statistics and Related Topics

This conference, held at Carleton University on September 15-17, 2006, attracted over 55 participants for three days in a friendly and informal atmosphere. The conference began with opening remarks by Jean-Guy Godin, the Dean of the Faculty of Science, and Don Fraser (Toronto), author of the classical monograph Nonparametric Methods of Statistics (1957). Then Ehsanes Saleh (Carleton), one of the organizers, gave a brief overview of the history of nonparametric statistics. The opening ceremony ended with a short impromptu speech of Madan Puri (Indiana) who paid tribute to Ehsanes Saleh’s scholastic achievements and his activity in organizing conferences over the years.

The goal of the conference was to bring together researchers from different countries and scientific schools to survey the changes in the rapidly growing field of modern Statistics. The conference featured prominent statisticians and junior researchers from Canada, United States, Europe, and Asia. There were present many distinguished speakers who contributed significantly to Nonparametric Statistics and related areas; among them were Don Fraser (Toronto), Marc Hallin (Bruxelles), Jana Jureckova (Prague), Hira Koul (Michigan), Boris Levit (Queen’s), Madan Puri (Indiana), Jon Rao (Carleton), Pranab Sen (North Carolina), Robert Serfling (Texas), Muni Srivastava (Toronto), and Winfried Stute (Giessen).

The conference program was both diverse and intense. It included 22 forty-minute invited talks and 8 fifteen-minute contributed talks, which covered the development of several central themes in nonparametric statistics, including non-parametric multivariate outlier detection, estimation in univariate and multivariate non-parametric regression, estimation in linear and generalized linear mixed models, nonparametric goodness-of-fit, and multivariate rank-based tests.

There were also several review talks. Most notably, Boris Levit discussed applications of splines in functional estimation; Jon Rao spoke on some recent advances in linear and generalized linear mixed models; Robert Serfling presented a talk on nonparametric multivariate outlier detection via depth and quantile functions; and Muni Srivastava gave a review of multivariate theory for high dimensional data with fewer observations. These provided an excellent brief introduction to the area for the graduate students attending the conference. The results reported at the conference were both theoretically and practically oriented, and some had applications to medical and epidemiological studies.

The conference, funded by the Fields Institute and the University of Toronto, was organized and partly financed by Ehsanes Saleh (Carleton), Majid Mojirsheibani (Carleton), and Natalia Stepanova (Carleton).

“The results reported at the conference were both theoretically and practically oriented…”

Natalia Stepanova (Carleton)
Summer School on Computational Number Theory and Applications to Cryptography

This three week summer school, hosted by the University of Wyoming Mathematics Department from June 19 to July 7, 2006, followed the successful style of earlier summer schools at the Fields Institute and those that have been running for twenty-four years at the Rocky Mountain Mathematics Consortium in Laramie. The event was organized by Michael Jacobson (Calgary), Duane Porter, Bryan Shader, and Andreas Stein (Wyoming).

The objective of the summer school was to acquaint graduate students and faculty with the most recent developments in computational number theory and mathematical cryptography. The summer school provided participants with a cutting-edge survey of computational number theory and the consequences in modern day cryptography. Topics included: \textit{Primality and integer factorization, Arithmetic of algebraic number fields and algebraic function fields, The discrete logarithm problem and related algorithms, Public key cryptography, Elliptic and hyper-elliptic curve cryptography, Pairings, and multivariate cryptography.}

A very original public lecture entitled \textit{Cryptography – the art of secret writing – from old to new} was given by Renate Scheidler from the Centre for Information Security and Cryptography (CiSAC) at the University of Calgary.

The school was officially opened on the first day by Tom Buchanan, the President of the University of Wyoming. The itinerary was as follows: Each week two plenary speakers gave an 80-minute lecture in the morning, and there were an additional 1–2 hours of talks from invited lecturers in the afternoons, filling up the conference schedule tightly. The conference also included student projects for the remainder of the each afternoon, as well as group discussions, and question and answer sessions. The student projects turned out to be a big success and many research groups continued working on their problems or even expanding on the topics they had learned. The research projects were managed by Michael Jacobson from the University of Calgary. Ten research projects were suggested by the speakers, and groups of five to eight students and one or two supervisors met in late afternoon or evening to work on them.

The funding from external agencies was used to support over 75 selected participants and 12 invited speakers from around the world – in fact, there were more than 140 applicants for funding. About 20 of the participants and speakers came from Canadian universities – their talks were outstanding and the organizers received very positive feedback from participants about their high quality. This is probably due to the expertise Canadian universities have developed in this area of mathematics.

Besides the very successful academic program, the participants also enjoyed a lively social program. Many people contributed to this success. Duane Porter organized a picnic in Washington Park and an excellent banquet in the University of Wyoming Union, followed by a very interesting after dinner speech by Myron Allen, Vice President for Academic Affairs. Several weekend hikes were organized by Diane Wagner, a regular participant in the summer school, and by Mikal Grant, an undergraduate student. Mikal and his Math Club also organized various other evening activities including frisbee, soccer, movies, and skating. Finally, Derrick Cerwinsky, a graduate student in the mathematics department, volunteered as the conference photographer and Eric Moorhouse designed an excellent conference T-shirt.

The Summer School was funded by the Rocky Mountain Mathematics Consortium (RMMC), the National Science Foundation (NSF), the Fields Institute, the Institute for Mathematics and its Applications (IMA), the Alberta Informatics Circle of Research Excellence (iCORE), and the Number Theory Foundation.

More information can be found on the summer school website math.uwyo.edu/RMMC/2006/rmmc06.html where lecture notes and slides of most contributed talks appear, including a video of the public lecture.

Andreas Stein (Wyoming)

NOTED

CARL RIEHM has been appointed chair of the selection committee for the Levi L. Conant Prize. The prize was established by the American Mathematical Society in 2000 in honour of Levi L. Conant to recognize the best expository paper published in either the \textit{Notices of the AMS} or the \textit{Bulletin of the AMS} in the preceding five years.
Workshop on Lorenz-Gini Type
Asymptotic Methods in Probability
and Statistics, and their Applications

The aim of the workshop, held at Carleton University on September 14-16, 2006, was to provide a platform for the exchange of recent findings and new ideas inspired by the path-breaking contributions of Max Otto Lorenz (1876-1959) and Corrado Gini (1884-1965), which have also influenced the development of quantile methods in Probability and Statistics in general. This workshop in part was devoted to introducing their ideas and to reviewing later developments along the lines of Lorenz-type curves and Gini-type indices, and their applications. Other talks were on new advances in the area and related fields.

Due to the intensive workshop nature of this event, this was a relatively small gathering of significant contributors to the area in hand and its related fields. Nevertheless, we were very happy to welcome 11 speakers from Canada and abroad.

The talks were summaries of leading edge research in the areas involved, and resulted in many stimulating discussions. In order to have some evidence of our Workshop for the future, we intend to collect all presentations in one of the volumes of the Technical Report Series of LRSP.

The first, introductory talk was given by Charles M. Goldie (Sussex), one of the major contributors to the area of Lorenz-Gini type methods. It was followed by two talks: Youri Davydov (Université de Lille I) talked about Gini index, Lorenz curves and convex rearrangements, and Murray Burke (Calgary) gave a talk on reducing the total time on test in the context of progressive type I multistage censoring.

The second day we had two talks in the morning session. Edit Gombay (Alberta) gave a talk on strong approximations of dependent sequences, while Sandor Csorgo (Bolyai Institute, University of Szeged) discussed weighted quantile correlation tests for location-scale families. The afternoon session started with a talk by Wei-Biao Wu (Chicago) on asymptotics for Gini indices and Lorenz Curves under dependence. The next speaker Rafał Kulik (Sydney and University of Wrocław), talked on quantile processes and extremal behaviour of long range dependent sequences.

On the last day we had four talks. The first speaker was Ricardas Zitikis (Western). His talk on testing hypotheses about absolute concentration curves and marginal conditional stochastic dominance was followed by the talk of his (jointly with Lajos Horvath, Utah) Ph.D. student Nao Mimoto (Western) on testing for exponentiality using the Atkinson index and its modification. In the afternoon, the first talk was given by Emad-Eldin Aly (Kuwait) on some measures of income inequality. Finally, we concluded our workshop with the talk by Hao Yu (Western) on total time on test process and its application to testing for exponentiality.

Gill Murray, the Coordinator of LRSP, was instrumental in helping to organize the workshop and took care of the logistics of this meeting. Mohamedou Ould Haye initiated and took up the main load of organizing the workshop.

This workshop was co-sponsored by the Laboratory for Research in Statistics and Probability (LRSP) at Carleton University, the Fields Institute for Research in Mathematical Sciences in Toronto, and the School of Mathematics and Statistics at Carleton University.

Miklós Csörgő, Mohamedou Ould Haye, and Barbara Szyszkowicz (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 (bkeyfitz@fields.utoronto.ca) or Deputy Director, Juris Steprans (deputydirector@fields.utoronto.ca).

Thematic Programs*

Deadlines for letters of intent and proposals for semester or year-long programs at the Fields Institute are March 15 and August 31 each year. 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 may consult the directorate about their projects in advance to help structure their proposal.

Postdoctoral Opportunities

Applications are invited for postdoctoral fellowship positions for the 2007-2008 academic year. The thematic program on Operator Algebras will take place at the Institute from July-December 2007, while the thematic program on New Trends in Harmonic Analysis will run from January-June 2008. 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 2007-2008 programs is December 7, 2006.

Postdoctoral opportunities also exist at some of the Fields Institute’s sponsoring universities. Consult http://www.fields.utoronto.ca/proposals/#pdf for details.

*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.

Please send applications, nominations, and proposals to:

The Director, Fields Institute
222 College Street, Toronto, Ontario, M5T 3J1 Canada
Message from the Director
continued from page 16

as long as they have demonstrated a commitment to research in mathematics. The intent of this change is to recognize that Fields can offer its stamp of approval more broadly to mathematical research, and thus benefit (and enlarge) the group of institutions and researchers that see themselves as part of our “community”. Furthermore, the benefit goes both ways. By communicating with more different kinds of universities, Fields gets to participate even more broadly in the mathematical life of the province, to learn from the research, educational, and cultural activities on different campuses, and to enrich everyone’s knowledge of the mathematical life of Ontario. We hope to introduce a new cohort of Affiliate Members at next year’s Annual General Meeting.

Barbara Lee Keyfitz (Fields Institute)
A recent decision by NSERC has established a funding envelope for the Canadian Mathematics Research Institutes. After a period of uncertainty following the cancellation of NSERC’s Reallocations exercise, which had established a federal funding level for the three institutes (CRM, Fields and PIMS), NSERC has established a new program, “Major Resources Support”, or “MRS”, which includes also BIRS, several research institutes in other disciplines (such as CITA, the Canadian Institute for Theoretical Astrophysics), and a number of large experimental facilities (the best known may be the Canadian Light Source) and field stations. By rewriting the guidelines and enlarging the set of projects that used to be known by the name “Major Facilities Access”, NSERC has set up what may prove to be a more stable funding paradigm for the institutes. This action shows recognition of how much mathematics research institutes have matured following the first NSERC involvement with mathematic institutes, which began with CRM in the 1980s. The first NSERC funding that helped establish Fields was in a program called “Collaborative Special Projects”. From there, the institutes entered the Discovery Grants envelope, in a special sub-envelope called “Institutes and Initiatives”. The new arrangement – for MFA to be redesigned as MRS and for the mathematics institutes support to be transferred to this program – has had its challenges for all three institutes. Among the strains has been the time-pressure for all three mathematics institutes to enter proposals in the current competition so as to provide enough lead time that we can plan our programs based on funding known a year in advance. However, thanks to NSERC’s willingness to extend the deadline until mid-November, all of us have submitted proposals in the competition.

NSERC has further requested that all three institutes submit their proposals during the same year. This has advantages for NSERC – they can arrange a single site-visit committee for all three institutes – and for us, as it insulates us from the variations in our funding that might be caused by NSERC's variations in the amount available in the MRS envelope from competition to competition. However, it does emphasize that, however much the three institutes work together to achieve common goals, we are inevitably competing for the same federal money.

Unlike the US NSF-funded mathematics institutes, whose funding is part of the DMS (Division of Mathematical Sciences) budget, the Canadian institutes’ envelope is multi-disciplinary, and contains enterprises of very different scope and with very different missions – the unifying theme being that these are resources that are used by and benefit an entire community (regional, national or international) rather than lying within the structure of a single institution. The explicit recognition of this role (which has been perceived by all stakeholders in mathematics institutes) has been one outcome of the extensive discussions with NSERC and within the mathematics community that led up to the formation of MRS.

The extraordinary role of mathematics research institutes worldwide in stimulating mathematics, both in fundamental and interdisciplinary research, has been one of the strongest motivators of NSERC’s current efforts, which we see as aimed at ensuring that the institutes have a secure home, as well as keeping us at the cutting edge. Here I would like to quote Doug Arnold, Director of IMA, who has said that the mathematics institutes have changed the culture of mathematics “from inward and isolated to central and connected”.

The reputation of Fields, as of all mathematics institutes worldwide, rests on the uncompromising pursuit of excellence in its thematic research programs. But there is more to it than that. The best in the world can be anywhere in the world, but bringing this activity to Toronto, Ontario is a part of our mission as well, and is the basis for Fields’ warm relationship with universities in the area. The stamp of approval, both approval of our activities by the universities that support us, and support for research at those universities, is captured by the concepts of a Principal Sponsoring University, and an Affiliate University.

This year, at the Fields Annual General Meeting, a change in the by-laws of the Institute was made that will allow Fields, for the first time, to admit as Affiliates some universities that do not offer a doctorate in any mathematical science,