Lecture Abstracts

Lecture Abstracts

(sorted by date and time)

Monday, September 22

Sir Michael Francis Atiyah

"Beauty in Mathematics"
(Monday, September 22, 9:00 a.m.)

Many famous mathematicians have highlighted the importance of beauty in mathematics. I will discuss what we mean by beauty and why it is so important. I will compare beauty in mathematics with beauty in the arts and report on recent experiments that show the underlying neurological similarities.

Manuel Blum

"Towards a Theory of Humanly Computable Protocols"
(Monday, September 22, 9:45 a.m.)

ALGORITHMS are instructions for single agents. PROTOCOLS are instructions for multiple agents. Agents may be specified to be humans or computers.

Our GOAL is to know which cryptographic problems can be solved by protocols that specify certain agents to be human. We are especially interested in the case in which each human does all computations entirely in his/her head (in all dealings with the other agents).

QUESTION: Can a human compute something/anything PRIVATELY -- entirely in his head -- that NO ADVERSARY -- BE IT HUMAN, COMPUTER, OR COMBINATION OF THE TWO -- can reasonably get hold of? In particular, can a human compute a private hash function $h(x_1)$, $h(x_2)$,...

- with just a few (3?) hours of preprocessing to learn h, and just 1 minute of processing per input x_i to compute $h(x_i)$, so that
- a human/computer combo that observes a small number of pairs $(x_1, h(x_1))$, $(x_2, h(x_2))$, ... but does not otherwise know h (because it is private and hard to infer) cannot compute h(x) on a new x.

EXAMPLE 1: PRIVATE KEY ENCRYPTION with n randomly chosen n-bit strings (ONE-TIME PADS) for small n.

EXAMPLE 2: PASSWORDS.
Definition: A PASSWORD SCHEME is an algorithm for producing passwords in response to given challenges (typically domain names).

THEOREM: there exists a PASSWORD SCHEME that is
1. WELL DEFINED (a mathematical concept),
2. HUMANLY USABLE by a normal dedicated human being, namely me (an experimentally demonstrable concept),
3. MACHINE UNCRACKABLE to a small well-defined extent (as determined by the password game).

Wendelin Werner

"Randomness, continuum, and complex analysis"
(Monday, September 22, 11:30 a.m.)

The fact that space and time can be continuous is rather intuitive. But when one thinks of random phenomena, the natural examples that first come to mind are of discrete nature, such as coin tossing.
The conceptual question on how randomness can be split up into and reassembled from infinitesimal little pieces turns out to be quite tricky and related to several different fields of mathematics, as well as mathematical physics (in particular for the study of phase transitions, sometimes referred to as critical phenomena) or theoretical computer science. It is related to contemporary research in mathematics that we shall illustrate via some concrete examples.

William Morton Kahan

"Desperately Needed Remedies for the Undebuggability of Large Floating-Point Computations in Science and Engineering"
(Monday, September 22, 12:15 p.m.)

How long does it take to either allay or confirm suspicions, should they arise, about the accuracy of a computed result? Often diagnosis has been overtaken by the end

of a computing platform's service life. Diagnosis could be sped up by at least an order of magnitude if more users and developers of numerical software knew enough to demand the needed software tools. Almost all these have existed though not all of them together in one place at one time. These tools cope with vulnerabilities peculiar to Floating-Point, namely roundoff and arithmetic exceptions. Programming languages tend to turn exceptions into branches which are prone to error. In particular, unanticipated events deemed ERRORs are handled in obsolete ways inherited from the era of batch computing. There are better ways. They would have prevented the crash of Air France #447 in June 2009, among other things.

Tuesday, September 23

Joseph Sifakis

"Is Computing a Science?"
(Tuesday, September 23, 9:00 a.m.)

Initially considered rather as applied technology, over the years computing resisted absorption back into the fields of its roots and developed an impressive body of knowledge. We discuss how computing is related to other domains of scientific knowledge and draw conclusions about the very nature of the discipline.
Computing deals with the study of phenomena of transformation of information defined as a relationship that involves the syntax and the semantics of a language. Information is an entity independent from matter and energy. It is not subject to space-time constraints. It is non material, although it needs media for its representation.
Computing has developed as a scientific discipline started from prior knowledge about computation based on mathematics and logic. In contrast to physical sciences, it focuses on the design of artefacts. The dominant paradigm is synthesis rather than analysis to understand and predict phenomena. Nonetheless, both computing and physical sciences share a common objective: the study of dynamic systems. Physical phenomena can be understood not only through the study of immutable laws, but also as computational processes. Physical systems are inherently synchronous and driven by uniform laws. Computational systems ignore physical time and are driven by specific laws defined by their designers. Despite these differences, computing and physical sciences are rooted in two common paradigms that characterize any scientific approach. The first is the application of modularity principles to cope with the inherent complexity of phenomena. The second is the use of abstraction hierarchies of models that describe phenomena at different levels of detail. We discuss similarities and differences in the application of

these paradigms.
Computing pursues the study of design as a formal process leading from requirements to correct artefacts. Providing design with scientific foundations raises sev-eral deep theoretical problems including the conceptualization of needs using declarative languages, their proceduralization and implementation. Additionally, design "scientization" seeks the purposeful and coherent integration of methods through the study of general semantic models, of expressive component frameworks and most importantly, of theory for achieving correctness-by-construction. This endeavor and its overarching goal are both intellectually challenging and culturally enlightening. It is at least as important the quest for scientific discovery in physical sciences and nicely complements the effort for scientific progress and its fruition.

Martin Hairer

"Taming infinities"
(Tuesday, September 23, 9:45 a.m.)

Some physical and mathematical theories have the unfortunate feature that if one takes them at face value, many quantities of interest appear to be infinite! Various techniques, usually going under the common name of "renormalization" have been developed over the years to address this, allowing mathematicians and physicists to tame these infinities. We will tip our toes into some of the mathematical aspects of these techniques and we will see how they have recently been used to make precise analytical statements about the solutions of some equations whose meaning was not even clear until now.

Vinton Gray Cerf

"On Digital Preservation"
(Tuesday, September 23, 11:30 a.m.)

We are creating and depending upon digital content and processing to an unprecedented degree. How will we assure that this massive amount of information will be accessible in the distant future? Digital preservation has many facets but among them will be the discovery and resolution of references to content created in the distant past but in need for current rendering. We need Digital Vellum!

Ngô Bảo Châu

"Number theory and the Langlands program"
(Tuesday, September 23, 12:00 noon)

My talk would depict in impressionistic manner the deep transformation that number theory has been undergoing under the influences of ideas of Robert Langlands.

Leslie Lamport

"How to write a 21st Century Proof"
(Tuesday, September 23, 12:30 p.m.)

Mathematicians have made a lot of progress in the last 350 years, but not in writing proofs. The proofs they write today are just like the ones written by Newton. This makes it all too easy to prove things that aren't true. I'll describe a better way that I've been using for about 25 years.

Thursday, September 25

Manjul Bhargava

"Rational points on elliptic and hyperelliptic curves"
(Thursday, September 25, 9:00 a.m.)

Understanding whether (and how often) a mathematical expression takes a square value is a problem that has fascinated mathematicians since antiquity. In this talk I will give a survey of this problem, and will then concentrate on the case where the mathematical expression in question is simply a polynomial in one variable. The main result in this case---proved just recently---is that if the degree of the polynomial is at least 6, then it is not very likely to take even a single square value!
I'll explain how this was proved, and how the question relates to the very active and exciting area of mathematics today known as "arithmetic geometry".

Robert Endre Tarjan

"Data Structures"
(Thursday, September 25, 10:00 a.m.)

Algorithms are at the core of computing, and choosing a good data structure is often key in producing an efficient algorithm. This talk will review the development of data structures over the last 65 years, and how the speaker came to play a role in it.

Shigefumi Mori

"Algebraic geometry vs. impressionism paintings"
(Thursday, September 25, 11:30 a.m.)

Mathematics is beautiful as well as useful, though many people do not recognize it. The main topic of my talk is the beauty of algebraic geometry.

The research in mathematics is considered to be quite unique and different from those in other academic disciplines. However a mathematician's attitude toward the object of his/her interest often has something common to those in other disciplines or even an artist's. In my experience, I found certain similarities between my field of research, algebraic geometry, and impressionism paintings, some of which I would like to explain and illustrate.

In this context, I will also explain the idea of the Minimal Model Program (MMP).

Jean-Christophe Yoccoz

"Regularity versus chaos in area preserving maps"
(Thursday, September 25, 12:15 p.m.)

I will present what is perhaps the most important open question in the theory of dynamical systems: do typical area-preserving maps have positive measure-theoretic entropy ? The so-called «standard map family» offers a very concrete instance of this problem.

Friday, September 26

Gerd Faltings

"Diophantine equations"
(Friday, September 26, 9:00 a.m.)

Diophantine equation are a classical subject. Progress in modern times has been possible because of modern algebraic geometry. I review what is known for curves and the techniques of proof involved. In addition I explain open problems like the "abc-conjecture", a seemingly simple problem for which new attempts have been made recently.

John Hopcroft

"Computer Science in the Information Age"
(Friday, September 26, 9:45 a.m.)

Computer science has changed significantly in the last few years. In the early years computer science was focused on making computers useful and was concerned with programing language, compilers, operating systems, and algorithms. Today the focus has shifted to what computers are used for. Several of the derivers of this change are the amount of data that is available and the information in this data, the world-wide-web, and social networks. This talk will focus on some of the basic theory need to support this change. It will consist of a few simple ideas concerning high dimensional data, random projections, deep learning and sparse vectors.

Efim Zelmanov

"Infinite Groups"
(Friday, September 26, 11:30 a.m.)

I will discuss the subject of Infinite Groups from the very beginning (1900 + ε) to our time.

Daniel Spielman

"The path from Laplacian matrices to the Kadison-Singer problem"
(Friday, September 26, 12:15 p.m.)

Linear algebra in computer science and mathematics:
The path from Laplacian matrices to the Kadison-Singer problem.

I will tell the story of some remarkable interactions between Mathematics and Computer Science, showing how progress in each area built on developments in the other.

The main plot line begins with my work on designing algorithms for solving systems of linear equations in the Laplacian matrices of graphs and ends with the solution of the Kadison-Singer problem. Along the way we will encounter mathematical results in combinatorics, random matrix theory, and the geometry of polynomials. These were inspired by other algorithmic problems, such as those of estimating the volumes and mixed volumes of convex bodies, of estimating the permanents and mixed discriminants of matrices, of computing partition functions of mathematical physics, and of accelerating algorithms by subsampling their inputs.