
5th Heidelberg Laureate Forum

Lecture Abstracts

Lecture Abstracts

(sorted by date and time)

Monday, September 25

Martin Hellman

"The Evolution of Public Key Cryptography"
(Monday, September 25, 9:00 a.m.)

While I love that public key cryptography is seen as revolutionary, after this talk you might wonder why it took Whit Diffie, Ralph Merkle and me so long to discover it. For example, Whit and I had been talking about trap door cryptosystems and it is a small step from that concept to public key cryptography. This talk will also highlight the contributions of some unsung (or "under-sung") heroes: Ralph Merkle, John Gill, Stephen Pohlig, Richard Schroeppel, Loren Kohnfelder, and researchers at GCHQ (Ellis, Cocks, and Williamson).

Aaron Ciechanover

"The Personalized Medicine Revolution: Are We Going to Cure all Diseases and at What Price?"
(Monday, September 25, 9:45 a.m.)

Many important drugs such as penicillin were discovered by serendipity. Other major drugs like the cholesterol-reducing statins were discovered using more advanced technologies, such as screening of large chemical libraries. In all these cases, the mechanism of action of the drug were largely unknown at the time of their discovery and was unraveled later. With the realization that patients with apparently similar diseases – breast or prostate cancer, for example – respond differently to similar treatments, we have begun to understand that the molecular bases of what we thought is the same disease entity, are different. Thus, breast or prostate cancers appear to be sub-divided to smaller distinct classes according to their molecular characteristics. As a result, we are exiting the era where the treatment of many diseases is "one size fits all", and enter a new era of "personalized medicine" where the treatment is tailored according to the patient's molecular/mutational profile. Here, the understanding of the mechanism will drive the development of new drugs. This era will be characterized initially by the development of technologies

to sequence individual genomes, transcriptomes, proteomes and metabolomes, followed by identification and characterization of new disease-specific molecular markers and drug targets, and by design of novel, mechanism-based drugs to these targets. This era will be also accompanied by complex bioethical problems, where genetic information of large populations will become available, and protection of privacy will become an important issue.

Daniel Spielman

"Approximate Elimination"
(Monday, September 25, 11:30 a.m.)

We provide context for and explain the recent Approximate Gaussian Elimination algorithm of Kyng and Sachdeva.
Gaussian Elimination is the first algorithm most of us learn for solving systems of linear equations. While it is simple and elegant, it can also be impractically slow. Kyng and Sachdeva show that, after carefully modifying elimination to randomly drop and rescale entries, it can provide very fast approximate solutions to systems of equations in Laplacian matrices. Our implementation of a refinement of this algorithm is now among the best Laplacian solvers in practice.
We will explain what Laplacian matrices are, what it means to approximately solve a system of linear equations over the reals, and how one analyzes this algorithm using recent results in Random Matrix Theory. We will also discuss what is means for an algorithm to be the "best in practice."

Martin Hairer

"The mathematics of randomness"
(Monday, September 25, 12:00 noon)

From the gambling machines in a Casino to the predictions of next week's weather, the world that surrounds us is governed by seemingly random events. How do mathematicians make sense of this and what does it even mean to "predict" something inherently random? We will explore these questions and see what are the main guiding principles of our modern understanding of randomness. Along the way, we will see how the works of an 18th century egyptologist and a 19th century biologist allow today's banks to model the stock market.

Piergiorgio Odifreddi

"Ménage à trois: art, math and computer science"
(Monday, September 25, 12:45 p.m.)

On the occasion of the Computer Art Exhibition organized for this meeting, I will give a short general overview of the relationships between Art, Mathematics and Computer Science, to place into a wider context the specific works exhibited.
I will tell a story in three acts, illustrated by many pictures. The first act deals with a superficial level of interaction beween art and mathematics, in which mathematical objects (solids, knots, surfaces...) are used as subjects of the works of art. The second act deals with a deeper level of penetration, in which mathematical concepts (tessellations, perspective, hyperbolic geometry ...) are used as structures for the works of art. And the third act deals with an even deeper level of integration, in which computers and programs are used as tools by the artist, to achieve infinitary extensions of the finitary procedures used in the previous two acts.

Tuesday, September 26

John E. Hopcroft

"Deep Learning Research"
(Tuesday, September 26, 9:00 a.m.)

This talk will cover the basics of machine learning and then talk about interesting directions in deep learning. Deep learning has become an important aspect of machine learning since it has been applied very successfully to many applied problems. The focus of the talk will be on directions related to understanding why deep learning works so well rather than applications.

Alexei Efros

"Self-Supervised Visual Learning and Synthesis"
(Tuesday, September 26, 9:30 a.m.)

Computer vision has made impressive gains through the use of deep learning models, trained with large-scale labeled data. However, labels require expertise and

curation and are expensive to collect. Can one discover useful visual representations without the use of explicitly curated labels? In this talk, I will present several case studies exploring the paradigm of self-supervised learning – using raw data as its own supervision. Several ways of defining objective functions in high-dimensional spaces will be discussed, including the use of General Adversarial Networks (GANs) to learn the objective function directly from the data. Applications in image synthesis will be shown, including automatic colorization, paired and unpaired image-to-image translation (aka pix2pix and cycleGAN), and, terrifyingly, #edges2cats.

Leslie Lamport

"How to Write a 21st Century Proof"
(Tuesday, September 26, 10:00 a.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 more than 25 years.

Joseph Sifakis

"How Much Hard is System Design?"
(Tuesday, September 26, 11:30 a.m.)

The ICT revolution is dominated by the IoT vision which promises increasingly interconnected smart objects providing autonomous services for the optimal management of resources and enhanced quality of life. These include smart grids, smart transport systems, smart health care services, automated banking services, smart factories, etc. Their coordination will be achieved using a unified network infrastructure, in particular to collect data and send them to the cloud which in return will provide using data analytics, intelligent services to ensure global trustworthiness and performance.

This vision raises a lot of expectations and in my opinion some over-optimism about its short-term impact.

The purpose of this talk is to discuss to what extent the IoT vision is reachable under the current state of the art, identify technical obstacles and point out work directions for overcoming them.

It is well understood that the current network infrastructure is neither safe nor secure enough. Furthermore, it is hard to guarantee time predictability for critical events. All these make problematic the development and coordination of critical autonomous systems and services. Additional problems come from the need to integrate critical and best-effort systems and deal with heterogeneous technical requirements.

We need to work in two complementary directions.

The first is to make progress in overcoming long-standing obstacles. These include limitations stemming from the lack of effective solutions to well-defined algorithmic problems e.g. verification and synthesis, but also from hard problems of different nature, such as faithful modeling of complex cyber-physical systems and requirement capturing and formalization in an unambiguous technical language.

The second is to develop design flows for mixed criticality systems and so to bridge the gap between critical and best effort system design. Existing design flows for critical systems are not any more affordable in the IoT context for both technical and economic reasons. Guaranteeing statically at design time correctness of critical systems such as self-driving cars becomes impossible due to unmanaged uncertainty of their execution and external environment. We need effective design flows seeking an appropriate balance between properties guaranteed at design time and properties enforced at run time. This implies in particular that we break with the deterministic concept of correctness adopted by some critical application standards.

The key issue is to design adaptive systems that can change dynamically their behavior to cope timely and effectively with hazards of any kind caused by design errors, failures or malevolent action. Adaptation is the capability to change system behavior in particular by reconfiguring its services and resources guided by knowledge acquired both at design time and at run time. We identify technical challenges for adaptive control achieved by combining three main functions: objective management, planning and learning.

Jeffrey A. Dean

"Deep Learning and the Grand Engineering Challenges"
(Tuesday, September 26, 12:15 p.m.)

Over the past several years, Deep Learning has caused a significant revolution in the scope of what is possible with computing systems. These advances are having significant impact across many fields of computer science, as well as other fields of science, engineering, and human endeavor. For the past five years, the Google Brain team (g.co/brain) has conducted research on deep learning, on building large-scale computer systems for machine learning research, and, in collaboration with many teams at Google, on applying our research and systems to dozens of Google products. In this talk, I'll describe some of the recent advances in machine learning and how they are applicable towards many of the U.S. National Academy of Engineering's Global Challenges for the 21st Century (http://engineeringchallenges.org/). I will also touch on some exciting areas of research that we are currently pursuing within our group.
This talk describes joint work with many people at Google.

Richard Edwin Stearns

"Curious Facts About Nested Canalyzing Functions"
(Tuesday, September 26, 14:30 p.m.)

If f is a binary valued function of binary variables, one of its variables v is called a "canalyzing variable" if the function can be described as follows: **IF *v*=a THEN *f*=b ELSE *f*** is a function of the remaining variables. If the "function of the remaining variables" itself has a canalyzing variable and so forth, the function is called a "nested canalyzing function" or "NCF". Because of the nesting, it is often the case that the solution to a computational problem for $(n+1)$-parameter NCFs is easy to obtain from the solution for n-parameter NCFs and by induction easy to solve for all NCFs. Because of this computational simplicity, it is easy to study NCFs experimentally by working out examples and looking for patterns. Analysis of the associated algorithms can then provide algebra for proving any resulting conjectures.
In this talk, we discuss two such discoveries. One is the appearance of Fibonacci numbers when representing an NCF by a threshold gate. The other is a characterization of the NCFs with the worst average sensitivity and the asymmetry between odd numbered variables and even numbered variables.

Madhu Sudan

"Mathematical Theories of Communication: Old and New"
(Tuesday, September 26, 15:15 p.m.)

Reliable and efficient digital communication today is possible largely in part due to some wonderful successes in mathematical modelling and analysis. A legendary figure in this space is Claude Shannon (1916-2001) who laid out the mathematical foundations of communication in his seminal 1948 treatise, where among other contributions he gave a mathematical definition of "entropy" and coined the now ubiquitous term "bit" (for binary digit). But Shannon is not the last word in communication. Communication extends to settings well beyond the carefully designed full information exchange model explored in Shannon's work. In this talk I will try to describe some of the many extensions that have been explored in the interim period including communication complexity (Yao 1980) that explores how it might be possible to achieve effective communication without a full exchange; interactive communication (Schulman 1992) which explores how to cope with errors in an interactive setting, and some of our own work on uncertain communication, which explores how shared context can make communication more effective, even if the context is shared only loosely.

Thursday, September 28

Manuel Blum

"Can a Machine be Conscious? Towards a Computational Model of Consciousness."
(Thursday, September 28, 9:00 a.m.)

Thanks to major advances in neuroscience, we are on the brink of a scientific understanding of how the brain achieves consciousness. This talk will describe neuroscientist Bernard Baars's Global Workspace Model (GWM) of the brain and propose a formal Turing-Machine-like computational model inspired by it for understanding consciousness. One of several consequences of this Model is the possibility of free will in a completely deterministic world. Another deals with the possibility of building machines that are conscious.
This talk is suitable for college students at all levels, engineers, mathematicians, and anyone who has ever wondered about consciousness.

Efim Zelmanov

"Asymptotic Group Theory"
(Thursday, September 28, 9:45 a.m.)

The talk is a very general survey of Asymptotic Group Theory. We will focus on growth of groups, growth of graphs and links to Combinatorics and Number Theory.

Friday, September 29

Sir Michael Francis Atiyah

"The Discrete and the Continuous from James Clerk Maxwell to Alan Turing"
(Friday, September 29, 9:00 a.m.)

The dichotomy between discrete and continuous splits algebra from analysis, quantum from classical, information from energy, Leibniz from Newton and Turing from Maxwell. But this separation is illusory: great scientists bridged the gap.

Vinton Gray Cerf

"An Interplanetary Internet"
(Friday, September 29, 9:30 a.m.)

As we continue our exploration of the Solar System, we can see the need for more than point-to-point radio links to support manned and robotic space exploration. In the early 1960s a Deep Space Network was constructed using 70 m antennas located in Madrid, Canberra and Goldstone, California. When the Pathfinder robot was landed on Mars in 1997, a team at the Jet Propulsion Laboratory began working on the design of a multi-node Interplanetary Internet. Its variation on store/forward protocols led to the development of Delay and Disruption Tolerant Networking (DTN) and the Bundle Protocols. These have now been standardized by the UN's Consultative Committee on Space Data Systems (CCSDS) and prototype versions are in operation on the Spirit and Opportunity Rovers, the Mars Science Laboratory, the International Space Station and the Mars mapping orbiters to return data from Mars to Earth. This talk is about the nature of these protocols and their applications. Major challenges are network management, security and flow/

congestion control in systems with round-trip times measured in minutes to hours or longer. Naming and addressing and delayed name resolution also play a role. So-called "custody transfer" is used to limit the potential for data loss.

Leslie G. Valiant

"Where Computer Science Meets Neuroscience"
(Friday, September 29, 10:30 a.m.)

For some problems in science there are several plausible theories and it remains to experimenters to resolve among them. There exist other problems for which, in contrast, no known theory is widely accepted as plausible. Currently computational neuroscience is a field full of opportunity that offers several fundamental problems of the latter kind. We shall discuss one of these problems: Over a lifetime, the brain performs hundreds of thousands of individual cognitive acts, of a variety of kinds, including the formation of new associations. Each such act depends on past experience, and, in turn, can have long lasting effects on future behavior. It is difficult to reconcile such large-scale capabilities, including fast reaction times on new inputs when using knowledge acquired at various earlier times, with the known resource constraints on cortex, such as low connectivity and low average synaptic strength. Here we shall describe an approach to this fundamental problem that attempts to explain these phenomena in terms of concrete algorithms for a model of computation that is faithful to the most basic quantitative resources.

Stephen Smale

"Perspectives on Turing."
(Friday, September 29, 11:00 a.m.)

I have been inspired by Turing and his work and will discuss some thoughts coming from this inspiration.