Karl Aberer

The Quest for Trusted Information

Abstract: In open information systems evaluating the reliability of information obtained from unknown or untrusted participants remains a constant challenge. In this talk we will review various manifestations of this problem that we have encountered over the years, together with methods for tackling the information trust challenge that we have developed. We have studied this problem in the context of peer-to-peer information sharing, decentralised data integration and evaluating credibility of information on the Web and in social networks..

The methods we present will rely on the two fundamental principles. The first principle is to rely on evaluating quality signals obtained on the producers of the information and the second to assess the semantic consistency of the data. In general, the best results are obtained by combinations of the two approaches.

***

Beat Brüderlin

Visual Analytics to Enhance the Digital Factory Planning Process

Abstract: Planning a factory for a new line of cars in the auto industry is a highly complex task involving various trades and different engineering teams. The introduction of digital factory planning methodology over a decade ago has shown substantial savings by eliminating mistakes already at the planning stage rather than correcting them after a new factory was built. For this purpose, large amounts of CAD data need to be analyzed. Attempts of finding conflicts in CAD drawings in an automated way have been ineffective even with today's tools. Much human intervention is still required, which is labor intensive as well as error prone. In this presentation we show how the application of visual analytics methods can make the evaluation of large numbers of potential design conflicts more effective.

***

Jürg Fröhlich

A theorist remembers Ernst Specker and tries to assess his ideas on quantum mechanics

Abstract: I propose to share some reminiscences of Ernst Specker going back to times when I was a student in some of his courses and when I became his colleague at ETH. One of them I have learned from Raoul Bott.

I will then sketch the contents of the Kochen-Specker Theorem concerning the non-existence of hidden variables in quantum mechanics. Some recent ideas in understanding the contents of quantum mechanics might also be sketched.

I will end by recalling some of Ernst Specker's non-scientific concerns.

***

Erich Grädel

Logic, Complexity, and Symmetry

Abstract: Part of the interesting relationship between logic and computational complexity is the tension arising from the fact that logic, and logic-based models of computation, work on abstract mathematical structures (rather than their encodings by words) and respect inherent symmetries of the data at each step of the computation.

In this talk I shall connect this to the ongoing quest for *a logic for polynomial time*, as well as to emerging notions intended to capture those problems that are efficiently solvable by *symmetric computations*.

***

Wolfgang Küchlin

60 years of Boolean Satisfiability Solving – From the Foundations of Mathematics to Industrial Applications

Abstract: This talk highlights some developments in propositional satisfiability solving (SAT-Solving). In the first part we recall the origins of DPLL SAT-Solving in 1960 as a means of automated theorem proving in Predicate Calculus. In the second part we present the key insight behind the break-through invention of Conflict Driven Clause Learning (CDCL) in 1995 which opened SAT-Solving to large-scale applications. Finally we give an overview of our commercial solutions to a number of automotive configuration problems which my group has implemented for Mercedes-Benz, BMW, AUDI, and OPEL.

***

Angus Macintyre

PA is complete for the theory of all rings of residues Z/mZ for m nonzero.

Abstract: Though PA is definitely not complete for the theory of the semi-ring N (and not even for the universal theory), PA does prove all ring sentences true in the finite residue rings of Z. The analysis depends on Ax's work on the theory of finite fields (and so appeals to work of Weil and Cebotarev from number theory), as well as to classic work of Feferman-Vaught on definability in product structures. Some related results on decidability and axiomatizability will be discussed (the latter using Specker's work on end extensions).

Roman Mäder

Experiments in Mathematics

Raw computing power and human-computer interface capabilities have grown tremendously since the days of the ZIR (Zentrum für Interaktives Rechnen) at ETH in the 1980ies. We can now do large experiments and explore phenomena, in addition to using computers mainly to speed up calculations derived from constructive proofs, such as is done in traditional computer algebra.

We give examples of experiments from areas such as combinatory logic, universal machines, and number theory, and show how mathematical concepts can be visualized interactively.

***

Janos Makowsky

Specker's work on counting labeled finite graphs.

Abstract: In 1981 C. Blatter and E. Specker announced a result on the modular periodicity of combinatorial sequences. They published a proof in 1983 and an expanded version was published by E. Specker as “Application of logic and combinatorics to enumeration problems" in 1988 and is reprinted in the Ernst Specker Selecta of 1990. I will explain the original result and outline further developments due E. Fischer, T. Kotek and myself.

***

Preda Mihailescu

On a conjecture of Vandiver which had been expressed by Kummer before him, and which in the end is true!

Abstract: The p-th cyclotomic fields (K = Q[zeta_p]) were the first deeply investigated number fields in algebraic number theory -- and Kummer did the bulk of the work ... of course, with Fermat at the back of the mind. He called the primes for which the class number h_p is p-divisible "irregular primes". They were not regular, since they made a magnificent criterion that he proved, fail. And irregular numbers turned out to be quite frequent. However, when looking at K^+, which is the field generated by zeta_p + zetabar_p, thus a real number, and investigating the class number h_p^+ of these fields, he found no p-divisibility. This led him to state in a letter to Kronecker (in 1849) his assumption that p never divides h_p^+. This assumption was never published, but 70 years later, Harry-Schulz Vandiver built many results (often incomplete!) on it, so it became the Vandiver, and then the Kummer-Vandiver Conjecture. But it still resisted time.

Only in the 90-es was it possible, with extensive computations based on K-Theory, to prove that the conjecture holds at the end of the spectrum of the group ring (this means something, but the margin of this abstract is insufficient for the explanation). Using extensively class field theory and p-adic arithmetic, together with a strong result in Iwasawa theory, we gave a proof of this Conjecture. I shall expose the main ideas of this proof in this Engeler-Talk.

***

Arne Hansen & Stefan Wolf

Ernst Specker and The Fundamental Theorem of Quantum Mechanics

Abstract: We start with a statement of Ernst Specker on what, according to him, is the "fundamental theorem of quantum mechanics." Taking into account some of Specker's written works, we attempt to reconstruct what he may have meant exactly with his remark, and we end up in a topic brought up and studied intensively only very recently in the quantum-information community. The case illustrates impressively how pioneering Specker's thoughts in the field have been.

Kochen and Specker's celebrated work on quantum theory introduces the term "contextuality." However, the concept is not necessarily restricted to quantum mechanics: The set of projectors on a Hilbert space is merely a special case of an orthomodular lattice with trivial center that does not allow for a dispersion-free state. This leads us to a perspective onto the so-called "measurement problem" as the collision of different epistemological stances.

***

Stathis Zachos

90 Years of Computability and Complexity

Abstract: Computational Complexity Theory deals with the classification of problems into classes of hardness called complexity classes. We define complexity classes using general structural properties, such as the model of computation (Turing Machine, RAM, Finite Automaton, PDA, LBA, PRAM, monotone circuits), the mode of computation (deterministic, nondeterministic, probabilistic, alternating, uniform parallel, nonuniform curcuits), the resources (time, space, # of processors, circuit size and depth) and also randomness, oracles, interactivity, counting, approximation, parameterization, etc. The cost of algorithms is measured by worst-case analysis, average-case analysis, best-case analysis, amortized analysis or smooth analysis. Inclusions and separations between complexity classes constitute central research goals and form some of the most important open questions in Theoretical Computer Science. Inclusions among some classes can be viewed as complexity hierarchies. We will present some of these: the Arithmetical Hierarchy, the Chomsky Hierarchy, the Polynomial-Time Hierarchy, a Counting Hierarchy, an Approximability Hierarchy and a Search Hierarchy.