

【ITCS Group Meeting】 Group Meeting on Nov. 22, 2007

Dear All,

We will have a group meeting at 2:00pm on Nov. 22(Thursday) in FIT-4-603. Please come and don't be late.

ITCS

2007-11-19

【ITCS Group Meeting】 Group Meeting on Dec. 13, 2007

Dear All,

We will have a group meeting at 2:00pm on Nov. 13(Thursday) in FIT-4-603. Please come and don't be late.

ITCS

2007-11-12

【ITCS Group Meeting】 Group Meeting on Nov. 8, 2007

Dear All,

We will have a group meeting at 2:00pm on Nov. 8(Thursday) in FIT-4-603. Please come and don't be late.

ITCS

2007-11-7

【ITCS Seminar】 Playing Games With Probability by Prof. Elchanan Mossel

Speaker: Prof. Elchanan Mossel

UC Berkeley

Title: Playing Games With Probability

Time: 16:00-17:00, Wednesday, Nov. 7, 2007

Place: Room 4-603, FIT Building, Tsinghua University

Abstract:

The talk will have two parts. In the first part, based on joint work with Braverman and Etesami, we will analyze the game Mafia (the chinese variant is known as Killer) - in particular focusing on optimal strategies, the strength of the different groups and the role of probability and cryptography. In the second part (based on work with Daskalakis and Dimakis) we will talk about random games and social networks.

Short Bio:

Prof. Elchanan Mossel studies mathematical and algorithmic problems arising in the theory of computing, as well as in such areas as molecular biology, evolution and social choice. He is particularly interested in problems of combinatorial and probabilistic flavor and in large-scale analysis.

Born in Jerusalem in 1973, he received a B.Sc. magna cum laude in mathematics and natural sciences from the Open University of Israel in 1992. He conducted his graduate studies in mathematics at the Hebrew University of Jerusalem, earning an M.Sc. magna cum laude in 1997 and a Ph.D. in 2000. After conducting postdoctoral studies in the theory group of Microsoft's research division for two years, he moved to the University of California at Berkeley in 2002, first

as a postdoctoral fellow and then as an assistant and an associate professor. He has received a number of grants and awards, including an Alfred Sloan Fellowship in Mathematics, a Miller Fellowship and a National Science Foundation Career Award.

ITCS

2007-11-6

【ITCS Seminar】 DNSSEC: From Cryptographic Design to Real Deployment by Prof. Lixia Zhang

Speaker: Prof. Lixia Zhang

Computer Science Department,UCLA

Title: DNSSEC: From Cryptographic Design to Real Deployment

Time: 11:00am-12:00pm, Friday, Oct. 19, 2007

Place: Room 4-603, FIT Building, Tsinghua University

Host: Prof. Andrew Yao

Abstract:

The DNS Security Extensions (DNSSEC) are among the first attempts to add cryptographic protection in large-scale operational systems. DNSSEC uses well-established public-key cryptography to authenticate DNS data. Despite its perceived need and seemingly simple cryptographic design, DNSSEC development took over a decade and several protocol revision cycles, and its deployment is barely visible on the horizon today. This talk identifies technical issues that were missed in the original DNSSEC design, the mismatch between the design and the reality, and unforeseen difficulties in deploying cryptographic protections. Using DNSSEC as a showcase, this talk exemplifies the gap between cryptographic theory and its application to the operational Internet, and identifies directions to add to Internet effective cryptographic protections.

Short Bio:

Lixia Zhang received her Ph.D in computer science from the Massachusetts Institute of Technology. She was a member of the research staff at the Xerox Palo Alto Research Center (XEROX PARC) before joining the faculty of UCLA's Computer Science Department in 1996. In the past she served as the vice chair of ACM SIGCOMM, Co-Chair of IEEE Communication Society Internet Technical Committee, and on the editorial board for the IEEE/ACM Transactions on Networking. Zhang is a fellow of both ACM and IEEE. She is currently serving on the Internet Architecture Board (IAB), and co-Chairs the Routing Research Group under IRTF.

ITCS

2007-10-17

【ITCS Group Meeting】 Group Meeting on Sept. 25, 2007

Dear All,

We will have an important group meeting at 2:00pm on September 25 (Tuesday) in FIT-4-603. Please come and don't be late.

ITCS

2007-9-11

【ITCS Seminar】 GRAND CHALLENGES IN PROOF COMPLEXITY by Prof. Alexander Razborov

Speaker: Prof. Alexander Razborov

Institute for Advanced Study, Princeton, USA

Title: GRAND CHALLENGES IN PROOF COMPLEXITY

Time: 3:00pm-4:30pm, Thursday, Sept. 13, 2007

1:00pm-2:30pm, Friday, Sept. 14, 2007

Place: Room 4-603, FIT Building, Tsinghua University

Host: Prof. Andrew Yao

Abstract:

These lectures will be centered around a set of questions that can be loosely described as follows: Are major open problems in Complexity Theory like $NP \stackrel{?}{\subseteq} P/poly$ or $P \stackrel{?}{\subseteq} NC1/poly$ independent from systems of Bounded Arithmetic? Do they possess efficient propositional proofs?

For obvious reasons (and it should be noted that we are deliberately working with the systems that, to the best of our knowledge, do prove all known results in Circuit Complexity) these independence questions are of utmost importance for both areas, Computational Complexity and Proof Complexity. Nonetheless, despite numerous efforts, they are still widely open. We will try to put these questions in the historical context and survey ideas (sometimes even with complete proofs) that have so far lead to at least non-negligible progress toward their solution. Although we will try to make the lectures as self-contained as possible, some familiarity with Circuit Complexity and Propositional Logic might be helpful. Also, the Introduction to http://www.mi.ras.ru/~razborov/res_k.ps can give a rather good impression of the set of topics we will be discussing.

Biography:

Professor Alexander A. Razborov graduated from the Moscow State University (department for mathematics and mechanics) in 1985 and in the same year entered the graduate school of the Steklov Mathematical Institute of the Russian Academy of Sciences. He defended his PhD thesis ("On systems of equations in free groups") in 1987, and his doctoral thesis ("Lower Bounds in the Boolean Complexity") in 1991.

Professor Razborov joined faculty of the Steklov Mathematical Institute in 1989 and have been working there since that. In 1999-2000 he was a Visiting Researcher at the Department of Computer Science of Princeton University, and in 2000-2008 he was holding a visiting position at the Institute for Advanced Study, Princeton.

During his career, Professor Razborov worked in various areas including mathematical logic, computational complexity, proof complexity and combinatorics. Among other things, his contributions include:

1. The first description of solutions of equations in a free group.
2. Solving the analogue of the P vs. NP question for a number of restricted models of computation.
3. Theory of Natural Proofs and closely related theory of feasible provability of major open problems in Complexity Theory, accompanied by many concrete lower bounds for the corresponding proof systems.
4. Lower bounds in quantum communication complexity.
5. The theory of Flag Algebras in Extremal Combinatorics.

Professor Razborov is a member of Academia Europea (since 1993), and a corresponding member of the Russian Academy of Sciences (since 2000). He is a recipient of the Nevanlinna

prize awarded by the International Mathematical Union (1990) and of the Goedel Prize (awarded jointly by EATCS and ACM, 2007).

ITCS

2007-9-11

【ITCS Group Meeting】 Group Meeting on Sept. 13, 2007

Dear All,

We will have group meeting at 2:00pm on September 13 (Thursday) in FIT-4-603. Prof. Yao wants everybody to attend. Please come and don't be late.

ITCS

2007-9-11