Lynne and William Frankel Center for Computer Science

Department of Computer Science, Ben-Gurion University of the Negev
Beer-Sheva, Israel 84105. Tel: (972-8) 6428032
www.cs.bgu.ac.il/~frankel
Saal Auditorium Room 202, Alon Building for High-Tech 37

Seminar Series Supported by Jeffrey and Holly Ullman

In celebration of Professor Shafi Goldwasser receiving an Honorary Doctoral Degree from Ben-Gurion University, you are invited:

Seminar in Honor of Professor Shafi Goldwasser

November 22, 2017

10:15 Gathering and Registration

10:45 Greetings

Prof. Zvi HaCohen, Rector, Ben-Gurion University

Prof. Amos Beimel, Ben-Gurion University

11:00 Hypertrees

Prof. Nati Linial, The Hebrew University of Jerusalem

Abstract: This is part of our ongoing effort to develop a theory of high-dimensional counterparts for the basic constructs of combinatorics. The definition that we adopt is that of [Kalai 1983]. I will try to give you a feeling of how these objects are similar to and yet different from the usual one-dimensional trees that we have known since the days of our academic childhood. This talk is based on joint works with Meshulam, Rosenthal, Newman, Peled and Rabinovich.

11:40 Submultiplicative Glivenko-Cantelli and Uniform Convergence of Revenues

Prof. Yishay Mansour, Tel Aviv University

Abstract: In this work we derive a variant of the classic Glivenko-Cantelli Theorem, which asserts uniform convergence of the empirical Cumulative Distribution Function (CDF) to the CDF of the underlying distribution. Our variant allows for tighter convergence bounds for extreme values of the CDF. We apply our bound in the context of revenue learning, which is a well-studied problem in economics and algorithmic game theory. We derive sample-complexity bounds on the uniform convergence rate of the empirical revenues to the true revenues, assuming a bound on the k-th moment of the valuations, for any (possibly fractional) k>1. For uniform convergence in the limit, we give a complete characterization and a zero-one law: if the first moment of the valuations is finite, then uniform convergence almost surely occurs; conversely, if the first moment is infinite, then uniform convergence almost never occurs. Join work with Noga Alon, Moshe Babaioff, Yannai A. Gonczarowski, Shay Moran, and Amir Yehudayof.

12:20 Calibration for the Masses

Dr. Guy Rothblum, Weizmann Institute of Science

Abstract: TBA

13:00 Lunch

13:50 On the Construction and Use of Oracles in Sublinear Algorithms

Prof. Dana Ron, Tel Aviv University

Abstract: In this talk I will briefly survey a few techniques in the design of sublinear algorithms, where the common theme is the (explicit or implicit) implementation of (imaginary) oracles.

14:30 Ad-Hoc Secure Computation

Prof. Eyal Kushilevitz, Technion

Abstract: TBA.

15:10 Coffee break

15:30 Can We Access a Database Both Locally and Privately?

Dr. Elette Boyle, IDC Herzliya

Abstract: We consider the following strong variant of private information retrieval (PIR). There is a large database x that we want to make publicly available. To this end, we post an encoding X of x together with a short public key pk in a publicly accessible repository. The goal is to allow any client who comes along to retrieve a chosen bit x_i by reading a small number of bits from X, whose positions may be randomly chosen based on i and pk, such that even an adversary who can fully observe the access to X does not learn information about i. Towards solving the above problem, we study a weaker secret key variant where the data is encoded and accessed by the same party. This primitive, that we call an oblivious locally decodable code (OLDC), is independently motivated by applications such as searchable symmetric encryption. In this work we reduce the public-key variant of PIR to OLDC using an ideal form of obfuscation, and give a first proposal of an OLDC candidate based on secretly permuted Reed-Muller codes. Joint work with Yuval Ishai, Rafael Pass, and Mary Wootters.

16:10 Playing 2-to-1 Games with Grassmann

Prof. Shmuel Safra, Tel Aviv University

Abstract: In this talk we discuss a recent line of attacks towards proving the 2-to-1 Games conjecture, a variant of Khot's well-known Unique-Games Conjecture. A key ingredient in this line of attack is the Grassmann Graph, and the approach relies on a certain unproven combinatorial hypothesis regarding it. We will go over the main ideas in the reductions. If time permit, we will discuss recent develops towards resolving the unproven combinatorial hypothesis.

16:50 Secure Multiparty Computation in Implementing Turing Machine, Random Access Machine, and Stabilizing State Machine

Prof. Shlomi Dolev, Ben-Gurion University

Abstract: The talk summarizes several recent works in the scope of secure multiparty computation, including: Universal Turing machine implementation, random access machine implementation, the abstraction of accumulating automata that reflects the usage of homomorphic additions vs. non-homomorphic multiplications, and self-stabilizing private computation, where all participants may be compromised for a while. Joint works with: Karim Eldefrawy, Juan A. Garay, Niv Gilboa, Vladimir Kolesnikov, Muni V. Kumaramangalam, Yin Li, Ximing Li, Rafail Ostrovsky, and Moti Yung.

17:30 Closing Remarks

Prof. Shlomi Dolev, Ben-Gurion University

17:40 End of Workshop in Honor of Professor Shafi Goldwasser