CSDM Seminars

Computer Science/Discrete Mathematics Seminar II

Submitted by admin on Mon, 04/01/2013 - 16:01
"What is Geometric Entropy, and Does it Really Increase?"
Series: Computer Science/Discrete Mathematics
Jozsef Beck
Rutgers, The State University of New Jersey
Date & Time: Tue, 04/09/2013 - 10:30 - 12:30
Location: S-101
Video Link:
http://video.ias.edu/csdm/1213/0409-JozsefBeck

We all know Shannon's entropy of a discrete probability distribution. Physicists define entropy in thermodynamics and in statistical mechanics (there are several competing schools), and want to prove the Second Law, but they didn't succeed yet (very roughly speaking, the Second Law claims that the entropy always increases). What I do is motivated by physics, but I ask a new, strictly combinatorial/geometric question. Assume that we have a large finite set of points in the unit square.

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar II

Submitted by admin on Wed, 03/27/2013 - 16:01
An Arithmetic Analogue of Fox's Improved Triangle Removal Lemma
Series: Computer Science/Discrete Mathematics
Sushant Sachdeva
Princeton University
Date & Time: Tue, 04/02/2013 - 10:30 - 12:30
Location: S-101
Video Link:
http://video.ias.edu/csdm/1213/0402-SushantSachdeva

We give an arithmetic version of the recent proof of the improved triangle removal lemma by Fox [Fox11], for the group F_2^n. A triangle in F_2^n is a tuple (x,y,z) such that x+y+z = 0. The triangle removal lemma for F_2^n states that for every \eps > 0, there is a \delta >0, such

that if a subset A of F_2^n requires the removal of at least eps 2^n elements to make it triangle-free, then it must contain at least \delta 2^{2n} triangles.

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar I

Submitted by admin on Thu, 03/21/2013 - 11:01
Cryptography and Preventing Collusion in Second Price (Vickery) Auctions
Series: Computer Science/Discrete Mathematics
Michael Rabin
Harvard University and Columbia University
Date & Time: Mon, 04/29/2013 - 11:15 - 12:15
Location: S-101
Video Link:
http://video.ias.edu/csdm/1213/0429-MichaelRabin

We present practically efficient methods for proving correctness of announced results of a computation while keeping input and intermediate values information theoretically secret. These methods are applied to solve the long standing problem of preventing collusion in second-price auctions. Second Price auctions, where the highest bidder gets the item and pays the second highest bid value, are theoretically advantageous to the Seller. Namely, absent collusion between bidders, a participant's best strategy is to bid his true private value for the item.

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar I

Submitted by admin on Mon, 03/18/2013 - 11:01
New Locally Decodable Codes from Lifting
Series: Computer Science/Discrete Mathematics
Madhu Sudan
Microsoft Research
Date & Time: Mon, 03/25/2013 - 11:15 - 12:15
Location: S-101
Video Link:

---

http://video.ias.edu/csdm/1213/0325-MadhuSudan

Locally decodable codes (LDCs) are error-correcting codes that allow for highly-efficient recovery of "pieces" of information even after arbitrary corruption of a codeword. Locally testable codes (LTCs) are those that allow for highly-efficient testing to see if some given word is close to a codeword. Codes derived from evaluations of low-degree multivariate polynomials give the simplest example of LDCs and LTCs, and these codes and their locality properties played a significant role in many results in complexity theory in the 90s.

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar I

Submitted by admin on Mon, 03/18/2013 - 10:01
Device Independence: A New Paradigm for Randomness Manipulation?
Series: Computer Science/Discrete Mathematics
Thomas Vidick
Massachusetts Institute of Technology
Date & Time: Mon, 04/01/2013 - 11:15 - 12:15
Location: S-101
Video Link:
http://video.ias.edu/csdm/1213/0401-ThomasVidick

A trusted source of independent and uniform random bits is a basic resource in many computational tasks, such as cryptography, game theoretic protocols, algorithms and physical simulations. Implementing such a source presents an immediate challenge: how can one certify whether one has succeeded? i.e. suppose someone were to claim that a particular device outputs a uniformly random n-bit string; is there a feasible test to verify that claim?

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar II

Submitted by admin on Wed, 03/13/2013 - 17:01
Series: Computer Science/Discrete Mathematics
No Seminar Talk

Date & Time: Tue, 03/26/2013 - 10:30 - 12:30
Location: S-101

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar I

Submitted by admin on Wed, 03/13/2013 - 17:01
Series: Computer Science/Discrete Mathematics
No Seminar Talk
Date & Time: Mon, 04/08/2013 - 11:15 - 12:15
Location: S-101

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar I

Submitted by admin on Wed, 03/13/2013 - 10:01
Constant Rate PCPs for Circuit-SAT with Sublinear Query Complexity
Series: Computer Science/Discrete Mathematics
Eli Ben-Sasson
Technion; Massachusetts Institute of Technology
Date & Time: Mon, 03/18/2013 - 11:15 - 12:15
Location: S-101
Video Link:
http://video.ias.edu/csdm/1213/0318-EliBen-Sasson

The PCP theorem (Arora et. al., J. ACM 45(1,3)) says that every NP-proof can be encoded to another proof, namely, a probabilistically checkable proof (PCP), which can be tested by a verifier that queries only a small part of the PCP. A natural question is how large is the blow-up incurred by this encoding, i.e., how long is the PCP compared to the original NP-proof. The state-of-the-art work of Ben-Sasson and Sudan (SICOMP 38(2)) and Dinur (J. ACM 54(3)) shows that one can encode proofs of length n by PCPs of length (n poly log n) that can verified using a constant number of queries.

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar I

Submitted by admin on Mon, 03/04/2013 - 18:01
Intractability in Algorithmic Game Theory
Series: Computer Science/Discrete Mathematics
Tim Roughgarden
Stanford University
Date & Time: Mon, 03/11/2013 - 11:15 - 12:15
Location: S-101
Video Link:
http://video.ias.edu/csdm/1213/0311-TimRoughgarden

We discuss three areas of algorithmic game theory that have grappled with intractability. The first is the complexity of computing game-theoretic equilibria, like Nash equilibria. There is an urgent need for new ideas on this topic, to enable meaningful research in the face of computational hardness results. The other domains concern the design and analysis of mechanisms (such as auctions).

terms:

- CSDM Seminars

Computer Science/Discrete Mathematics Seminar II

Submitted by admin on Wed, 02/27/2013 - 15:01
Sensitivity Versus Block Sensitivity, I
Series: Computer Science/Discrete Mathematics
Hao Huang
University of California, Los Angeles; Member, School of Mathematics
Date & Time: Tue, 03/12/2013 - 10:30 - 12:30
Location: S-101
Video Link:
http://video.ias.edu/csdm/1213/0312-HaoHuang

There are two important measures of the complexity of a boolean function: the sensitivity and block sensitivity. Whether or not they are polynomial related remains a major open question. In this talk I will survey some known results on this conjecture, and its connection with various combinatorial problems.

terms:

- CSDM Seminars

- « first
- ‹ previous
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- …
- next ›
- last »