Pseudorandomness in Mathematics and Computer Science Mini-Workshop

Friday, April 22, 2011

School of Mathematics
Institute for Advanced Study*

All sessions will take place in Simonyi Hall lecture room 101.

In math, one often studies random aspects of deterministic systems and structures. In CS, one often tries to efficiently create structures and systems with specific random-like properties. Recent work has shown many connections between these two approaches through the concept of "pseudorandomness". This workshop highlights these connections, aimed at a joint audience of mathematicians and computer scientists.

10:15-11:15 p.m. Peter Varju, Princeton University
"Random Walks in Linear Groups"

11:30 a.m.-12:30 p.m. Swastik Kopparty, Institute for Advanced Study
"The Correlation of Multiplicative Characters with Polynomials over Finite Fields"

12:30-2:30 p.m. Lunch (available in the IAS Dining Hall)**

2:30-3:30 p.m. Larry Guth, University of Toronto and Institute for Advanced Study
"The polynomial method and applications from finite field Kakeya to distinct distances"

3:30 p.m. Coffee/tea and cookies break, Fuld Hall

4:00-5:00 p.m. Zeev Dvir, Princeton University
"Monotone expanders - constructions and applications"

5:00-6:00 p.m. Alex Kontorovich, Stony Brook University
"On Zaremba's Conjecture"

*Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540
**Credit cards are not accepted at the Dining Hall – cash or IAS identification card only.
If you have any questions, please call 609-734-8117.

ABSTRACTS

Random Walks in Linear Groups

Peter Varju

I will talk about a joint work with Jean Bourgain that establishes spectral gaps for random walks on SL_n(Z/qZ). Let S be a fixed finite and symmetric subset of SL_n(Z) which generates a Zariski dense subgroup. We show that words of length C log(q) are almost uniformly distributed among congruence classes modulo q. Unlike in previous results, q is arbitrary and not restricted to any special subset of the integers. A key new ingredient for the proof is the recent work of Bourgain, Furman, Lindenstrauss and Mozes on the equidistribution of non-Abelian semigroup actions on the torus.

The Correlation of Multiplicative Characters with Polynomials over Finite Fields

Swastik Kopparty

This talk will focus on the complexity of the cubic-residue (and higher-residue) characters over GF(2^n), in the context of both arithmetic circuits and polynomials.

We show that no subexponential-size, constant-depth arithmetic circuit over GF(2) can correctly compute the cubic-residue character for more than 1/3 + o(1) fraction of the elements of GF(2^n). The key ingredient in the proof is an adaptation of the Razborov-Smolensky method for circuit lower bounds to setting of univariate polynomials over GF(2^n).

As a corollary, we show that the cubic-residue character over GF(2^n) is uncorrelated with all degree-d n-variate GF(2) polynomials (viewed as functions over GF(2^n) in a natural way), provided d << n^{0.1}. Classical approaches based on van der Corput differencing and the Weil bounds show this for d << log(n).

Monotone Expanders – constructions and applications

Zeev Dvir

A Monotone Expander is an expander graph which can be decomposed into a union of a constant number of monotone matchings, under some fixed ordering of the vertices. A matching is monotone if every two edges (u,v) and (u',v') in it satisfy u < u' --> v < v'. It is not clear a priori if monotone expanders exist or not. This is partially due to the fact that the natural application of the probabilistic method does not work in this special case.

The first construction of monotone expanders with *logarithmic* degree was given in [D. Shpilka 05] and was motivated by an application to 'Dimension Expanders' (an algebraic analog of expander graphs). Later, in [Bourgain 09], a rather involved construction with constant degree was given. A simple construction with 'log-star' degree, based on the Zig-Zag product, was given in [D. Wigderson 10], together with other applications coming from the study of Turing Machines.

This talk will survey the above results in a high-level way.

On Zaremba's Conjecture

Alex Kontorovich

Inspired by the theory of good lattice points in numerical integration, Zaremba conjectured in 1972 that for every denominator q, there is some coprime numerator p, such that the continued fraction expansion of p/q has uniformly bounded quotients. We will present recent progress on this problem, joint with Jean Bourgain.