abstract

Video of this lecture

COMPUTER SCIENCE AND DISCRETE MATHEMATICS SEMINAR II

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We give a pseudorandom generator, with seed length O(log n), for CC0[p], the class of constant-depth circuits with unbounded fan-in MODp gates, for prime p. More accurately, the seed length of our generator is O(log n) for any constant error epsilon>0. In fact, we obtain our generator by fooling distributions generated by low degree polynomials, over Fp, when evaluated on the Boolean cube. This result significantly extends previous constructions that either required a long seed [LVW93] or that could only fool the distribution generated by linear functions over Fp, when evaluated on the Boolean cube [LRTV09, MZ09].

Enroute of constructing our PRG, we prove two structural results for low degree polynomials over finite fields that can be of independent
interest:

1. Let f be an n-variate degree d polynomial over Fp. Then, for every epsilon>0 there exists a subset S of variables of size depending only on d and epsilon, such that the total weight of the Fourier coefficients that do not involve any variable from S is at most epsilon.

2. Let f be an n-variate degree d polynomial over Fp. If the distribution of f when applied to uniform zero-one bits is epsilon-far (in statistical distance) from its distribution when applied to biased bits, then for every delta>0, f can be approximated over zero-one bits, up to error delta, by a function of a small number (depending only on epsilon, delta and d) of lower degree polynomials.

Joint work with Partha Mukhopadhyay and Amir Shpilka.