abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We study solution sets to systems of 'generalized' linear equations of the form ell_i (x_1, x_2,...,x_n) \in A_i (mod m) where ell_1,...,ell_t are linear forms in n Boolean variables, each A_i is an arbitrary subset of Z_m, and m is a composite integer that is a product of two distinct primes, like 6. Our main technical result is that such solution sets have exponentially small correlation, i.e exp(-Omega(n)), with the boolean function MOD_q, when m and q are relatively prime. This bound is independent of the number t of equations.

This yields progress on limiting the power of constant-depth circuits with modular gates. We derive the first exponential lower bound on the size of depth-three circuits having a MAJORITY gate at the top, AND/OR gates at the middle layer and generalized MOD_m gates at the base. This settles an open problem of Beigel and Maciel, for the case of such modulus m.

This is joint work with Avi Wigderson.