abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Every Boolean function on n variables can be expressed as a unique multivariate polynomial modulo p for every prime p. In this work, we study how the degree of a function in one characteristic affects its complexity in other characteristics. We establish the following general principle: functions with low degree modulo p must have high complexity in every other characteristic q.

More precisely, we show the following results about Boolean functions f:{0,1}^n to {0,1} which depend on all n variables, and distinct primes p,q:

1. If f has degree o(\log n) modulo p, then it must have degree n^{1-o(1)}modulo q. Thus a Boolean function has degree o(\log n) in only one characteristic. This result is essentially tight as there exist functions that have degree \log n in every characteristic.

2. If f has degree d = o(\log n) modulo p, it cannot be computed correctly on more than 1-p^{-O(d)} fraction of the hypercube by polynomials of degree n^{1/2 - \eps} modulo q.

As a corollary of the above results it follows that if f has degree o(\log n) modulo p, then it requires super-polynomial size \AC_0[q] circuits. This gives a lower bound for a broad and natural class of functions.

This is a joint work with Shachar Lovett (Weizmann) and Parikshit Gopalan (MSR).