abstract

COMPUTER SCIENCE/DISCRETE MATH, I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In this work we study two, seemingly unrelated, notions. Locally Decodable Codes (LDCs) are codes that allow the recovery of each message bit from a constant number of entries of the codeword. Polynomial Identity Testing (PIT) is one of the fundamental problems of algebraic complexity: we are given a circuit computing a multivariate polynomial and we have to determine whether the polynomial is identically zero. We improve known results on locally decodable codes and on polynomial identity testing and show a relation between the two notions.

In particular we obtain the following results:

1. we show an exponential lower bound on the length of locally decodable codes with 2 queries, over arbitrary fields. Previously such bounds were known for fields of size << 2^n.

2. We show that from every depth 3 arithmetic circuit with a bounded top fan-in, that computes the zero polynomial, one can construct a locally decodable code with 2 queries.

3. As a corollary of the results above we prove a structural theorem for identically zero depth 3 circuits.

4. Using the structural theorem we obtain new PIT algorithms for depth 3 circuits. In particular for such circuits with bounded top fan-in we get - A deterministic algorithm that runs in quasi-polynomial time - A probabilistic algorithm that runs in polynomial time and uses only polylogarithmic number of random bits.

abstract

In particular for the case of top fan-in = 3 this resolves an open question asked by Klivans and Spielman.

This is joint work with Amir Shpilka.