abstract

Computer Science/Discrete Mathematics Seminar II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

A locally correctable code (LCC) is an error correcting code mapping d symbols to n symbols, such that for every codeword c and every received word r that is \delta-close to c, we can recover any coordinate of c (with high probability) by only making a few queries to r. LCCs are a stronger form of Locally Decodable Codes (LDCs) which have received a lot of attention recently due to their many applications and surprising constructions.

A linear LCC over a finite field F_p is a code where the codewords form a linear subspace of F_p^n. The code whose codewords are the truth tables of linear functions evaluated on all of F_p^n is an example of a linear LCC that uses only 2 queries. In this talk we will show that in some sense this is the only example of a linear 2 query LCC over F_p.
Specifically, we prove a lower bound of the form p^(\delta*d) on the length n of linear 2-query LCCs over F_p, that encode messages of length d. This also gives a separation between 2 query LCCs and 2 query LDCs over finite fields of prime order.

Constructions of such 2 query LCCs are intimately related to special configurations of lines and points in F_p^n with interesting incidence properties. The problem of ruling out constructions of small 2-query LCCs boils down to showing that certain configurations of points and lines do not exist.
Our proof makes use of tools from additive combinatorics. We also obtain, as corollaries of our main theorem, new results in incidence geometry over finite fields, such as an improvement to the Sylvester-Gallai theorem over finite fields and a new analog of Beck's theorem over finite fields

This is joint work with Arnab Bhattacharyya, Zeev Dvir and Amir Shpilka.