abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

A k-query Locally Decodable Code (LDC) encodes an n-bit message x as an N-bit codeword C(x), such that one can probabilistically recover any bit x_i of the message by querying only k bits of the codeword C(x), even after some constant fraction of codeword bits has been corrupted. The major goal of LDC related research is to establish the optimal trade-off between the length and the query complexity of such codes.

Recently vast improvements in upper bounds for the length of LDCs were achieved via constructions that rely on existence of certain "nice" subsets of finite fields. Such constructions come in two steps: 1. one argues that "nice" subsets yield short codes; 2. one constructs "nice" subsets.

In this talk we review and extend the constructions of LDCs from "nice" subsets. We argue that further progress on upper bounds for LDCs via these methods is tied to progress on an old number theory question regarding the size of the largest prime factors of Mersenne numbers.

Specifically, we show that every Mersenne number m = 2^t - 1 that has a prime factor p > m^gamma yields a family of k(gamma)-query locally decodable codes of length Exp(n^{1/t}). Conversely, if for some fixed k and all epsilon>0 one can use the "nice"-subsets technique to obtain a family of k-query LDCs of length Exp(n^epsilon); then infinitely many Mersenne numbers have prime factors larger than known currently.

(Joint work with Kiran Kedlaya.)