abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

A q-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 q bits of the codeword C(x), even after some constant fraction of codeword bits has been corrupted.

We give new constructions of three query LDCs of vastly shorter length than that of previous constructions. Specifically, given any Mersenne prime p=2^t-1, we design three query LDCs of length N=EXP(n^{1/t}), for every n. Based on the largest known Mersenne prime, this translates to a length of less than EXP(n^{10^{-7}}), compared to EXP(n^{1/2}) in the previous constructions. It has often been conjectured that there are infinitely many Mersenne primes. Under this conjecture, our constructions yield three query locally decodable codes of length N=EXP(n^{1/log log n}) for infinitely many n.

We also obtain analogous improvements for Private Information Retrieval (PIR) schemes. We give 3-server PIR schemes with communication complexity of O(n^{10^{-7}}) to access an n-bit database, compared to the previous best scheme with complexity O(n^{1/5.25}). Assuming again that there are infinitely many Mersenne primes, we get 3-server PIR schemes of communication complexity n^{O(1/log log n)} for infinitely many n.

Previous families of LDCs and PIR schemes were based on the properties of low-degree multivariate polynomials over finite fields. Our constructions are completely different and are obtained by constructing a large number of vectors in a small dimensional vector space whose inner products are restricted to lie in an algebraically nice set.