abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Error correcting codes encode messages in a way that allows recovery of the original message even in the presence of noise. We study Multiplication codes (Akavia-Goldwasser-Safra FOCS'03), extending them in different ways to allow polynomial encoding length, binary alphabet, constant distance and a variety of algorithmic properties:

1. (Polynomial time) Local self correcting with constant query complexity for codes of exponential encoding length. The local self correcting algorithm, given a corrupted codeword and an entry location, outputs (whp) the value of the closest codeword on that entry while reading only a constant number of entries.
2. (Polynomial time) Random noise decoding for codes of polynomial encoding length.
3. ($4^(e n $ time) Adversarial noise decoding for codes of linear encoding length (where n is the length of the encoded message and e is the fraction of flipped bits).

Multiplication codes are unique in achieving the above properties while having no underlying field structure, but rather only a group structure; where the underlying group is the group of integers modulo N (for growing N). We further extend the definition of Multiplication codes to allow codes where the underlying algebraic structure is any finite Abelian group. We present such codes achieving combinatorial and algorithmic properties similar to the above, albeit with alphabet size exponential in the groups generating set size.

New techniques developed in this study include:

1. Local self correcting via solving the property testing problem of distinguishing between signals with high and low Fourier coefficients in a large interval while making only a constant number of queries to the signal.
2. Finding significant Fourier coefficients of a signal when given values of the signal on a

predetermined set of entries and where values are corrupted by (random or adversarial) noise.
3. Soft local error reduction algorithm for ABNNR codes concatenated with binary codes, presenting an alternative to Forney's GMD decoding approach; joint work with Venkatesan IPAM'06.