abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We present a tradeoff between the length of a 3-query probabilistically checkable proof of proximity (PCPP) and the best possible soundness obtained by querying it.

Consider the task of distinguishing between "good" inputs w \in {0,1}^n that are codewords of a linear error correcting code C over the binary alphabet, and "bad" inputs that differ from every word of C on ~1/2 of their bits. To perform this task, we allow oracle access to w and an auxiliary proof pi, however, we place the following limitations on our verifier:

1) it can read at most 3 bits from w and pi, 2) it must accept every "good" input with probability one, 3) its decision must be linear - i.e., based on the sum of the queried bits.

We notice that all known techniques for PCPP constructions yield verifiers for linear codes that satisfy these conditions, so our tradeoff applies to all of them.

Our main result implies that for certain codes, every verifier accessing a proof of polynomial length will accept some "bad" words with probability at least 2/3.

In contrast, if no limitation is placed on the proof length, we can construct a verifier that rejects any "bad" word with the largest possible probability of ~1/2.

In other words, the closer the rejection probability is to the best possible, the longer the proof our verifier will require. This tradeoff between proof length and soundness holds for any code that is not locally testable, including codes with large dual distance and most random Low

abstract

Density Parity Check (LDPC) codes.

Joint work with Eli Ben-Sasson, Prahladh Harsha and Oded Lachish