abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The ``direct product code'' of a function f gives its values on all k-tuples $(f(x_1),\dots,f(x_k))$. This basic construct underlies "hardness amplification" in cryptography, circuit complexity and PCPs. A recent breakthrough by Dinur and Goldenberg \cite{DG08} enabled for the first time testing proximity to this important code in the "list-decoding" regime. In particular, they give a 2-query test which works for polynomially small success probability $1/k^{\alpha}$, and show that no such test works below success probability $1/k$.

Our main result is a 3-query test which works for exponentially small success probability $\exp({-k^{\alpha}})$. Our techniques (which are based on recent simplified decoding algorithms for the same code \cite{IJKW08}) also allow us to considerably simplify the analysis of the 2-query test of \cite{DG08}. We then show how to derandomize their test, achieving a code of polynomial rate, independent of k, and success probability $1/k^{\alpha}$.

Finally we show the applicability of the new tests to PCPs. Starting with a 2-query PCP of alphabet Σ of size 2^t and soundness error $1-\delta$, Raz's (k-fold) parallel repetition theorem (and Holenstein's proof) \cite{Raz-parallel,Hol07} yields a new 2-query PCP with soundness error $\exp(-(\delta^3k)/t)$, with the dependence on the alphabet size essential \cite{Feige-Verbitsky}. Our techniques yield a 2-query PCP with soundness error $\exp(-\delta \sqrt{k})$. While having an incomparable exponential decay, our error is independent of the alphabet size!

This is joint work with Russell Impagliazzo and Avi Wigderson.