abstract

COMPUTER SCIENCE/DISCRETE MATH SEMINAR, I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We present new PCPs for NP-complete languages. The PCPs are only n poly log n bits long, when proving satisfiability of formulae of length n. However, the probabilistic verifier needs to query poly log n bits of the proof to verify it.

In contrast to most earlier PCP constructions, these PCPs are based on the properties of (relatively high-degree)
univariate polynomials. Most of the earlier steps in PCPs get simplified in our setting by our ability to work with such high-degree polynomials. The technical crux of the construction is a ``low-degree test/proof'' for univariate polynomials that is verifiable with only polylogarithmically many queries (relative to the degree of the polynomial being tested) into the proof.

Joint work with Eli Ben-Sasson (Toyota Institute of Technology)