abstract

Computer Science/Discrete Mathematics Seminar II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The PCP theorem (Arora et. al., J. ACM 45(1,3)) asserts the existence of proofs that can be verified by reading a very small part of the proof. Since the discovery of the theorem, there has been a considerable work on improving the theorem in terms of the length of the proofs, culminating in the construction of PCPs of quasi-linear length, by Ben-Sasson and Sudan (SICOMP 38(2)) and Dinur (J. ACM 54(3)).

One common theme in the aforementioned PCP constructions is that they all rely heavily on sophisticated algebraic machinery. The aforementioned work of Dinur (J. ACM 54(3)) suggested an alternative approach for constructing PCPs, which gives a simpler and arguably more intuitive proof of the PCP theorem using combinatorial techniques. However, this combinatorial construction only yields PCPs of polynomial length, and is therefore inferior to the algebraic constructions in this respect. This gives rise to the natural question of whether the proof length of the algebraic constructions can be matched using the combinatorial approach.

In this work, we provide a combinatorial construction of PCPs of whose length blow-up is quasi-poly-logarithmic, coming very close to the state of the art algebraic constructions (whose length blow up is poly-logarithmic). To this end, we develop a few generic PCP techniques which may be interesting in their own right.

It should be mentioned that our construction does use low degree polynomials at one point. However, our use of polynomials is confined to the construction of error correcting codes with a certain simple multiplication property, and it is conceivable that such codes can be constructed without the use of polynomials.