abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The PCP theorem (Arora et. al., J. ACM 45(1,3)) says that every NP-proof can be encoded to another proof, namely, a probabilistically checkable proof (PCP), which can be tested by a verifier that queries only a small part of the PCP. A natural question is how large is the blow-up incurred by this encoding, i.e., how long is the PCP compared to the original NP-proof. The state-of-the-art work of Ben-Sasson and Sudan (SICOMP 38(2)) and Dinur (J. ACM 54(3)) shows that one can encode proofs of length n by PCPs of length (n poly log n) that can verified using a constant number of queries. In this work, we show that if the query complexity is relaxed to n^epsilon, then one can construct PCPs of length O(n) for circuit-SAT, and PCPs of length O(n log n) for all NP. Our PCPs have perfect completeness and constant soundness. This is the first constant-rate PCP construction that achieves constant soundness with nontrivial query complexity (o(n)).

Our proof relies on replacing the use of low-degree polynomials in PCP constructions with transitive algebraic geometry (AG) codes. In particular, we show that the automorphisms of an AG code can be used to simulate the role of affine transformations which are crucial in earlier high-rate algebraic PCP constructions. Using this observation we conclude that any asymptotically good family of transitive AG codes over a constant-sized alphabet --- like the family of AG codes presented by Stichtenoth in [Trans. Information Theory 2006] and in an appendix to this work --- leads to constant-rate PCPs with polynomially small query complexity.

Joint work with Yohay Kaplan, Swastik Kopparty and Or Meir, with an appendix by Henning Stichtenoth.