abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We prove a strong limitation on the ability of entangled provers to collude in a multiplayer game. Our main result is the first nontrivial lower bound on the class MIP* of languages having multi-prover interactive proofs with entangled provers; namely MIP* contains NEXP, the class of languages decidable in non-deterministic exponential time. While Babai, Fortnow, and Lund (Computational Complexity 1991) proved the celebrated equality MIP=NEXP in the absence of entanglement, ever since the introduction of the class MIP* it was open whether shared entanglement between the provers could weaken or strengthen the computational power of multi-prover interactive proofs. Our result shows that it does not weaken their computational power: MIP \subseteq MIP*. At the heart of our result is a proof that Babai, Fortnow, and Lund's ``multilinearity test'' is sound even in the presence of entanglement between the provers, and our analysis of this test could be of independent interest. As a byproduct we show that the correlations produced by any entangled strategy which succeeds in the multilinearity test with high probability can always be closely approximated using shared randomness alone. This is a joint work with Thomas Vidick. A paper is available at http://arxiv.org/abs/1207.0550.