abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

I will present Holenstein's (STOC 07) simplification of Raz's (STOC '95) proof of the parallel repetition theorem for two prover games. This theorem is a crucial component in many PCP constructions leading to tight hardness of approximation results.

In a 2 prover game, two computationally unbounded provers can coordinate a randomized or deterministic strategy and then are isolated from one another. Then, one verifier (sometimes called referee) sends a query to each prover, and decide whether the two provers won the game based on the answers to these two queries. The value of the game is the maximum probability of winning taken over all possible prover strategies.

In 1988, Fortnow Rompel and Sipser conjectured that if the game has value V and is repeated n times (Verifier sends an n-tuple of independently chosen queries to each prover, received an n-tuple of answers, and the provers win iff they won in all n games) then the new game's value is V^n. This conjecture was refuted by Fortnow in 89.

However, the parallel repetition theorem implies that the value of the game still decays exponentially. Specifically, if V=1-x for some x>0 then the value of the repeated game will be at most (1-x3)^{cn} for some constant c independent of n (but depending logarithmically on the alphabet size of the provers' answer).