abstract

Video of this lecture

COMPUTER SCIENCE/DISCRETE MATH I

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The question whether or not parallel repetition reduces the soundness error is a fundamental question in the theory of protocols. While parallel repetition reduces (at an exponential rate) the error in interactive proofs and (at a weak exponential rate) in special cases of interactive arguments (e.g., 3-message protocols - Bellare, Impagliazzo and Naor [FOCS '97], and public-coin protocols - Håstad, Pass, Pietrzak and WikstrÄm [Manuscript '08]), Bellare et. al gave example of interactive arguments for which parallel repetition does not reduce the soundness error at all.

We show that by slightly modifying any interactive argument, in a way that preserves its completeness and only slightly deteriorates its soundness, we get a protocol for which parallel repetition does reduce the error at a weak exponential rate. In this modified version, the verifier flips at the beginning of each round an (1 - (1/4m), 1/4m) biased coin (i.e., 1 is tossed with probability 1/4m), where m is the round complexity of the (original) protocol. If the coin is one, the verifier halts the interaction and accepts, otherwise it sends the same message that the original verifier would. At the end of the protocol (if reached), the verifier accepts if and only if the original verifier would.