

abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In this talk I will describe nondeterministic reductions which yield new direct product theorems (DPTs) for Boolean circuits. In our theorems one assumes that a function F is "mildly hard" against *nondeterministic* circuits of some size $s(n)$, and concludes that the t -fold direct product F^t is "extremely hard" against probabilistic circuits of only polynomially smaller size $s'(n)$. The main advantage of these results compared with previous DPTs is the strength of the size bound in our conclusion.

As an application, we show that if NP is not in $coNP/poly$ then, for every PPT algorithm attempting to produce satisfying assignments to Boolean formulas, there are infinitely many satisfiable instances on which the algorithm's success probability is nearly-exponentially small. This furthers a project of Paturi and Pudlák [STOC'10].