abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We show new connections between derandomization, worst-case hardness and average-case hardness. Specifically, we show that a mild derandomization assumption together with the worst-case hardness of NP implies the average-case hardness of a language in non-deterministic quasi-polynomial time. Previously such connections were only known for high classes such as EXP and PSPACE.

Our key lemma, which may be of independent interest, is the following: given a description of an efficient algorithm that fails to solve SAT in the worst-case, we can efficiently generate at most three formulae (of increasing lengths) such that the algorithm errs on at least one of them.

Our proof uses a non-block-box reduction, and furthermore, we show that this reduction is highly unlikely to be done in a black-box way. Thus our technique suggests a way to bypass black-box limitations regarding worst-case to average-case reductions (e.g. Feigenbaum & Fortnow (SICOMP 1993), Bogdanov & Trevisan (FOCS 2003), and Akavia et. al. (STOC 2006)).

Based on joint works with Ronen Shaltiel and Amnon Ta-Shma.