abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Hardness amplification is a major line of research that mainly seeks to transform a given lower bound (e.g. a function that has correlation at most 99% with small circuits) into a strongly average-case one (i.e. a function that has negligible correlation with small circuits). Strongly average-case lower bounds are of central importance in complexity theory and in particular are necessary for most cryptography and pseudorandom generators.

In this work we show that standard techniques for proving hardness amplification against a class of circuits require that same class of circuits to compute the Majority function.

Our work is most significant when coupled with the celebrated ``natural proofs'' result by Razborov and
Rudich (J. CSS '97) and Naor and Reingold (J. ACM '04), which shows that most lower-bounding techniques cannot be applied to circuits that can compute Majority. The combination of our results with theirs shows that **standard techniques for hardness amplification can only be applied to those circuit classes for which standard techniques cannot prove circuit lower bounds.** This in particular explains the lack of strong average-case lower bounds for a number of
circuit classes for which we have lower bounds.

Our results also show a qualitative difference between the direct product lemma and Yao's XOR lemma, and they
give tight bounds on the number of queries needed for hardness amplification.

To obtain our results we introduce a new proof technique to argue about reductions among

primitives. One of its components is a generalization of an information-theoretic lemma used by Raz in his parallel repetition theorem (SICOMP '98).

Joint work with Ronen Shaltiel.