abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

One-way functions (i.e., polynomial-time computable functions that are hard to invert on the average case) are the cornerstone of modern cryptography. The hardness condition on the task of inverting a one-way function is an *average-case* complexity condition; this clearly implies a *worst-case* hardness condition. A puzzling question of fundamental nature is whether the necessary worst-case condition is also a sufficient one. In particular: Can one-way functions be based on NP-hardness? Namely, is there a reduction from a (worst case) NP-complete problem to the task of (average case) inverting a polynomial-time computable function?

We prove two results on the impossibility of basing one-way functions on NP-hardness.

1. One-way functions cannot be based on NP-hardness via *non-adaptive* reductions (unless coNP is contained in AM).

2. Size-computable one-way functions cannot be based on NP-hardness via *any* (possibly *adaptive*) reduction (unless coNP is contained in AM); where we call f *size-computable* if given y the number of pre-image $|f^{-1}(y)|$ is efficiently computable (or, more generally, if the approximate number of pre-image is verifiable via an AM protocol).

Our results improve on previously known negative results of [Feigenbaum-Fortnow, Bogdanov-Trevisan] by (i) handling *adaptive* reductions (whereas previous works were essentially confined to *non-adaptive* reductions) and by (ii) relying on a (seemingly) weaker complexity assumption.

abstract

In the course of proving the above results, two new AM protocols emerge for proving *upper bounds* on the sizes of NP sets. Whereas the known *lower* bound protocol on set sizes by [Goldwasser-Sipser] works for any NP set, the known *upper* bound protocol on set sizes by [Fortnow, Aiello-Hastad] works only in a settings where the verifier knows a random secret element (unknown to the prover) in the NP set. The new protocols we develop here, each work under different requirements than that of [Fortnow, Aiello-Hastad], enlarging the settings in which it is possible to prove upper bounds on NP set size.

Joint work with Oded Goldreich, Shafi Goldwasser and Dana Moshkovitz