Deterministic Randomness Extraction from Generalized and Distributed Santha-Vazirani Sources

By: Dr. O. Etesami
Faculty member, School of Mathematics, IPM

Abstract

Randomized algorithms and protocols require a source of randomness for their execution. However, in the real world most sources of randomness are imperfect. Randomness extraction is the process of turning a slightly random bit string into a shorter almost perfectly random string.

A Santha-Vazirani (SV) source is a sequence of random bits where the conditional distribution of each bit, given the previous bits, can be partially controlled by an adversary. We talk about a generalization of SV sources for non-binary sequences. We show that unlike the binary case, deterministic randomness extraction in the generalized case is sometimes possible.

We also consider a distributed version of SV sources in which the goal of the extraction is to obtain common randomness shared among different parties. We show that randomness extraction in this distributed case essentially reduces to randomness extraction from (non-distributed) SV sources.

http://cs.ipm.ac.ir/alg-group/

وبسایت گروه الگوریتم:

زمان: پنجشنبه 94/4/11 ساعت 14

مکان: فرهنگی و تربیتی دانشگاه آزاد اسلامی - برج کوه نور - نبش خیابان فربین - پژوهشگاه دانش های بی نیادی - طبقه همکف

***شرکت برای عموم علاقه مندین آزاد است***