abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Getting the deterministic complexity closer to the best known randomized complexity is an important goal in algorithms and communication protocols. In this work, we investigate the case where instead of one input, the algorithm/protocol is given multiple inputs sampled independently from an arbitrary unknown distribution. We show that in this case a strong and generic derandomization result can be obtained by a simple argument.

Our method relies on extracting randomness from ``same-source'' product distributions, which are distributions generated from multiple independent samples from the same source. The extraction process succeeds even for arbitrarily low min-entropy, and is based on the order of the values and not on the values themselves (This may be seen as a generalization of the classical method of Von-Neumann extended by Elias for extracting randomness from a biased coin).

The tools developed in the paper are generic, and can be used elsewhere. We present applications to streaming algorithms, and to implicit probe search [FiaNao93]. We also refine our method to handle product distributions, where the i'th sample comes from one of several arbitrary unknown distributions. This requires creating a new set of tools, which may also be of independent interest.

Joint work with Ariel Gabizon