Bocconi

8 JUNE 2023
12:00 PM

Bocconi University
Room 3-E4-SR03
Via Röntgen 1 Milano (3° floor)

Almost Chor-Goldreich Sources and Adversarial Random Walks

Speaker

David Zuckerman
Professor
The University of Texas

Abstract

A Chor-Goldreich (CG) source is a sequence of random variables where each has min-entropy, even conditioned on the previous ones. We extend this notion in several ways, most notably allowing each random variable to have Shannon entropy conditioned on previous ones. We achieve pseudorandomness results for Shannon-CG sources that were not known to hold even for standard CG sources, and even for the weaker model of Santha-Vazirani sources.

Specifically, we construct a deterministic condenser that on input a Shannon-CG source, outputs a distribution that is close to having constant entropy gap, namely its min-entropy is only an additive constant less than its length. Therefore, we can simulate any randomized algorithm with small failure probability using almost CG sources with no multiplicative slowdown. This result extends to randomized protocols as well, and any setting in which we cannot simply cycle over all seeds, and a "one-shot" simulation is needed. Moreover, our construction works in an online manner, since it is based on random walks on expanders.

Our main technical contribution is a novel analysis of random walks, which should be of independent interest. We analyze walks with adversarially correlated steps, each step being entropy-deficient, on good enough lossless expanders. We prove that such walks (or certain interleaved walks on two expanders) accumulate entropy. This is the first positive result for random walks with entropy rate under 1/2.

Joint work with Dean Doron, Dana Moshkovitz, and Justin Oh.

Università
Bocconi
DEPARTMENT
OF COMPUTING
SCIENCES