abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

It is now well-known that a random walk on an expander graph is a very good "sampler", and this has been used to prove a variety of important results in complexity theory, cryptography and algorithms.

On the surface, however, taking a walk on an expander graph seems like an inherently sequential process, and in this work we show that the same task can be accomplished in a highly-parallel fashion, i.e. in parallel time O(log n) or NC^1.

Specifically, we construct a randomness-efficient averaging sampler that is computable by uniform constant-depth circuits with parity gates (i.e., in AC^0[mod 2]). Our sampler matches the parameters achieved by random walks on constant-degree expander graphs, allowing us to apply a variety expander-based techniques within NC^1.

For example, we obtain the following new results:

- Randomness-efficient error-reduction for uniform probabilistic NC^1, TC^0, AC^0[mod 2] and AC^0: Any function computable by uniform probabilistic circuits with error 1/3 using r random bits is computable by uniform probabilistic circuits with error delta using r + O(log(1/delta)) random bits.

- An optimal explicit epsilon-biased generator in AC^0[mod 2], resolving a question raised by Gutfreund and Viola (Random 2004).

- uniform BPAC^0 is contained in uniform AC^0 / O(n).

abstract

Our sampler is based on the zig-zag graph product of Reingold, Vadhan and Wigderson (Annals of Math 2002) and as part of our analysis we give an elementary proof of a generalization of Gillman's Chernoff Bound for Expander Walks (FOCS 1994).