Deterministic Simulation of Probabilistic Constant Depth Circuits

Miklos Ajtai
Avi Wigderson

Abstract

We explicitly construct, for every integer n and $\varepsilon >0$, a family of functions (pseudo-random bit generators) $f_{n,\varepsilon}:{0,1}^{n^{\varepsilon}} \rightarrow {0,1}^n$ with the following property: for a random seed, the pseudorandom output "looks random" to any polynomial size, constant depth, unbounded fan-in circuit. Moreover, the functions $f_{n,\varepsilon}$ themselves can be computed by uniform polynomial size, constant depth circuits.

Some (interrelated) consequences of this result are given below.

1. *Deterministic simulation of probabilistic algorithms.* The constant depth analogues of the probabilistic complexity classes RP and BPP are contained in the deterministic complexity classes $DSPACE(n^{\varepsilon})$ and $DTIME(2^{n^{\varepsilon}})$ for any $\varepsilon >0$.
2. *Making probabilistic constructions deterministic.* Some probabilistic constructions of structures that elude explicit constructions can be simulated in the above complexity classes.
3. *Approximate counting.* The number of satisfying assignments to a (CNE or DNE) formula, if not too small, can be arbitrarily approximated in $DSPACE(n^\varepsilon)$ and $DTIME(2^{n^{\varepsilon}})$, for any $\varepsilon >0$.

We also present two results for the special case of depth 2 circuits. They deal, respectively, with finding an assignment and approximately counting the number of assignments. For example, for 3-CNF formulas with a fixed fraction of satisfying assignments, both tasks can be performed in polynomial time!