Hardness vs. Randomness

Noam Nisan
Avi Wigderson

Abstract
We present a simple new construction of a pseudorandom bit generator, based on the constant depth generators of [N]. It stretches a short string of truly random bits into a long string that looks random to any algorithm from a complexity class *C* (eg *P*, *NC*, *PSPACE*…) using an *arbitrary* function that is hard for *C*.

This construction reveals an *equivalence* between the problem of proving lower bounds and the problem of generating good pseudorandom sequences.

Our construction has many consequences. The most direct one is that efficient deterministic simulation of randomized algorithms is possible under much weaker assumptions than previously known. The efficiency of the simulations depends on the strength of the assumptions, and may achieve $*P =BPP*$. We believe that our results are very strong evidence that the gap between randomized and deterministic complexity is not large.

Using the known lower bounds for constant depth circuits, our construction yields an unconditionally proven pseudorandom generator for constant depth circuits. As an application of this generator we characterize the power of NP with a random oracle.