Derandomization that is Rarely Wrong from Short Advice that is Typically Good

June 22, 2002

Oded Goldreich
Avi Wigderson

Abstract
For every $\varepsilon >0$, we present a log-space *deterministic* algorithm that correctly decides undirected graph connectivity on all but at most $2^{n^{\varepsilon}}$ of the n-vertex graphs. The same holds for every problem in Symmetric Log-space (i.e., SL).

Make no assumptions (and in particular not assuming the ERH), we present a polynomial-time *deterministic* algorithm that correctly decides primarily on all but at most $2^{0.63n}$ of the n-bit integers.

Using a plausible complexity assumption (i.e., that P cannot be approximated by $SIZE(p)^{SAT}$, for every polynomial $p)$ we show that, for every $\varepsilon >0$, each problem in BPP has a polynomial-time *deterministic* algorithm that errs on at most $2^{n^{\varepsilon}}$ of the n-bit long inputs. (The complexity assumption that we use is not known to imply $BPP=P$.)

All results are obtained as special cases of a general methodology that explores which probabilistic algorithms can be derandomized by generating their coin tosses *deterministically* from the input itself. We show that this is possible (for all but extremely few inputs) for algorithms which take advice (in the usual Karp-Lipton sense), in which the advice string is short, and most choices of the advice string are good for the algorithm.

To get the applications above and others, we show that algorithms with short and typically good advice strings do exist, unconditionally for SL and Primality Testing, and under reasonable assumptions for BPP and AM.