Derandomization

Ahto Buldas

September 12, 2007

By *derandomization* we mean the following paradigm:

- First, design a probabilistic algorithm for a given problem. Note that good probabilistic algorithms are often easier to find than deterministic ones.
- Then, show that the correctness analysis remains valid, if the uniformly random strings (coin-tosses) are replaced with a distribution of a very small amount of entropy.

In some cases, it is even possible to construct a deterministic algorithm that, instead of using random coin-tosses, executes the algorithm with all possible outcomes of the small-entropy distribution.

- Derandomization techniques are used in Complexity Theory to show that certain randomized complexity classes belong to deterministic complexity classes (like $\mathbf{BPP} \subseteq \Sigma_2$), as well as in Cryptography for constructing pseudo-random generators and building strong one-way functions from weak ones.
- The paper by Michael Luby and Avi Wigderson "Pairwise Independence and Derandomization" focuses on some classical derandomization results in a self-contained manner and offers a good view on what happens in derandomization.