Dispersers, Deterministic Amplification, and Weak Random Sources

Aviad Cohen
Avi Wigderson

Abstract

We use a certain type of expanding bipartite graphs, called disperser graphs, to design procedures for picking highly correlated samples from a finite set, with the property that the probability of hitting any sufficiently large subset is high. These procedures require a relatively small number of random bits and are robust with respect to the quality of the random bits.

Using these sampling procedures to sample random inputs of polynomial time probabilistic algorithms, we can simulate the performance of some probabilistic algorithms with less random bits or with low quality random bits. We obtain the following results:

1. The error probability of an RP or BPP algorithm that operates with a constant error bound and requires n random bits, can be made exponentially small (i.e. 2^{-n}), with only $(3+\varepsilon)n$ random bits, as opposed to standard amplification techniques that require $\Omega(n^2)$ random bits for the same task. This result is nearly optimal, since the information theoretic lower bound on the number of bits required for such an amplification is $2n$.
2. It is shown that the output of any random source whose Renyi entropy rate exceeds $1/2(3/4)$, can be used to simulate $RP(BPP)$ algorithms. This is far from the information theoretic lower bound which is $m^{\mu – 1}$, where m is the number of bits and $0<\mu <1$ is any constant. We show that the lower bound can be achieved for a specific class of random sources called oblivious bit fixing sources.