Extracting randomness using few independent sources
Boaz Barak, Russell Impagliazzo and Avi Wigderson

Abstract

In this work we give the first deterministic extractors from a constant number of weak sources whose entropy rate is less than ½. Specifically, for every $\delta > 0$ we give an explicit construction for extracting randomness from a constant (depending polynomially on $1/\delta$) number of distributions over $\{0,1\}^n$, each having min-entropy $\delta n$. These extractors output $n$ bits, which are $2^{-n}$ close to uniform. This construction uses several results from additive number theory, and in particular a recent one by Bourgain, Katz and Tao [BKT03] and of Konyagin [Kon03].

We also consider the related problems of constructing randomness dispersers. For any constant output length $m$, our dispersers use a constant number of identical distributions, each with min-entropy $\omega(\log n)$ and outputs every tool we use is a variant of the “stepping-up lemma” used in establishing lower bound on the Ramsey number for hypergraphs (Erdos and Hajnal, [GRS80]).