

Simulating independence: New constructions of condensers, ramsey graphs, dispersers, and extractors

B. Barak, G. Kindler, R. Shaltiel, B. Sudakov and A. Wigderson

Abstract

We present new explicit constructions of *deterministic* randomness extractors, dispersers and related objects. We say that a distribution X on binary strings of length n is a δ -source if X assigns probability at most $2^{-\delta n}$ to any string of length n . For every $\delta > 0$, we construct the following poly(n)-time computable functions:

2-source disperser: $D: (\{0, 1\}^n)^2 \rightarrow \{0, 1\}$ such that for any two independent δ -sources X_1, X_2 we have that the support of $D(X_1, X_2)$ is $\{0, 1\}$.

Bipartite Ramsey graph: Let $N = 2^n$. A corollary is that the function D is a 2-coloring of the edges of $K_{N,N}$ (the complete bipartite graph over two sets of N vertices) such that any induced subgraph of size N^δ by N^δ is not monochromatic.

3-source extractor: $E: (\{0, 1\}^n)^3 \rightarrow \{0, 1\}$ such that for any three independent δ -sources X_1, X_2, X_3 we have that $E(X_1, X_2, X_3)$ is $o(1)$ -close to being an unbiased random bit.

No previous explicit construction was known for either of these for any $\delta < 1/2$, and these results constitute significant progress to long-standing open problems.

A component in these results is a new construction of condensers that may be of independent interest: This is a function $C: \{0, 1\}^n \rightarrow (\{0, 1\}^{n/c})^d$ (where c and d are constants that depend only on δ) such that for every δ -source X one of the output blocks of $C(X)$ is (exponentially close to) a 0.9-source. (This result was obtained independently by Ran Raz.)

The constructions are quite involved and use as building blocks other new and known objects. A recurring theme in these constructions is that objects that were designed to work with independent inputs, sometimes perform well enough with correlated, high entropy inputs.

The construction of the disperser is based on a new technique which we call “the challenge-response mechanism” that (in some sense) allows “identifying high entropy regions” in a given pair of sources using only one sample from the two sources.