Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers, and Extractors*

Boaz Barak† Guy Kindler‡ Ronen Shaltiel§ Benny Sudakov¶ Avi Wigderson‖

May 20, 2009

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: $D : (\{0,1\}^n)^2 \to \{0,1\}$ 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: $E : (\{0,1\}^n)^3 \to \{0,1\}$ 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 $C : \{0,1\}^n \to (\{0,1\}^{n/c})^d$ (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 which 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.

Categories and Subject Descriptors: G.2.1 [Discrete Mathematics]: Combinatorics

General Terms: Theory.

Keywords: Ramsey Graphs, Explicit Constructions, Extractors, Dispersers, Condensers.

*A preliminary version of this paper appeared in STOC 2005.

†Department of Computer Science, Princeton University, boaz@cs.princeton.edu. Supported by NSF grants CNS-0627526 and CCF-0426582, US-Israel BSF grant 2004288 and Packard and Sloan fellowships. Most of this work was done when the author was a member in the school of Mathematics at the Institute for Advanced study.

‡Faculty of Computer Science and Mathematics, Weizmann Institute of Science, guy.kindler@weizmann.ac.il. Most of this work was done while the author was member in the School of Mathematics, Institute for Advanced Study.

§Department of Computer Science, University of Haifa, Israel, ronen@cs.haifa.ac.il. Supported by US-Israel BSF grant 2004329 and ISF grant 686/07.

¶Department of Mathematics, University of California at Los Angeles, bsudakov@math.ucla.edu. Supported in part by NSF CAREER award DMS-0812005 and a USA-Israeli BSF grant. Most of this work was done while author was at Princeton University.

‖School of Mathematics, Institute for Advanced Study, Princeton, NJ, avi@ias.edu.