2-Source Dispersers for Sub-Polynomial Entropy and Ramsey Graphs Beating the Frankl-Wilson Construction

Boaz Barak* Anup Rao † Ronen Shaltiel‡ Avi Wigderson§

ABSTRACT

The main result of this paper is an explicit disperser for two independent sources on n bits, each of entropy $k = n^{o(1)}$. Put differently, setting $N = 2^n$ and $K = 2^k$, we construct explicit $N \times N$ Boolean matrices for which no $K \times K$ submatrix is monochromatic. Viewed as adjacency matrices of bipartite graphs, this gives an explicit construction of K-Ramsey *bipartite* graphs of size N.

This greatly improves the previous bound of $k = o(n)$ of Barak, Kindler, Shaltiel, Sudakov and Wigderson [4]. It also significantly improves the 25-year record of $k = \tilde{O}(\sqrt{n})$ on the special case of Ramsey graphs, due to Frankl and Wilson [9].

The construction uses (besides "classical" extractor ideas) almost all of the machinery developed in the last couple of years for extraction from independent sources, including:

- Bourgain's extractor for 2 independent sources of some entropy rate $< 1/2$ [5]
- Raz's extractor for 2 independent sources, one of which has any entropy rate $> 1/2$ [18]
- Rao's extractor for 2 independent block-sources of entropy $n^{\Omega(1)}$ [17]
- The "Challenge-Response" mechanism for detecting "entropy concentration" of [4].

The main novelty comes in a bootstrap procedure which allows the Challenge-Response mechanism of [4] to be used with sources of less and less entropy, using recursive calls to itself. Subtleties arise since the success of this mechanism depends on restricting the given sources, and so recursion constantly changes the original sources. These are resolved via a new construct, in between a disperser and an extractor, which behaves like an extractor on sufficiently large subsources of the given ones.

This version is only an extended abstract, please see the full version, available on the authors' homepages, for more details.

Categories and Subject Descriptors

G.2.2 [**Mathematics of Computing**]: Discrete Mathematics—*Graph algorithms*

General Terms

Theory, Algorithms

Keywords

Dispersers, Ramsey Graphs, Independent Sources, Extractors

1. INTRODUCTION

This paper deals with randomness extraction from weak random sources. Here a weak random source is a distribution which contains some entropy. The extraction task is to design efficient algorithms (called *extractors*) to convert this entropy into useful form, namely a sequence of independent unbiased bits. Beyond the obvious motivations (potential use of physical sources in pseudorandom generators and in derandomization), extractors have found applications in a variety of areas in theoretical computer science where randomness does not seem an issue, such as in efficient constructions of communication networks [24, 7], error correcting codes [22, 12], data structures [14] and more.

Most work in this subject over the last 20 years has focused on what is now called *seeded* extraction, in which the extractor is given as input not only the (sample from the) defective random source, but also a few truly random bits (called the *seed*). A comprehensive survey of much of this body of work is [21].

*Department of Computer Science, Princeton University. boaz@cs.princeton.edu. Supported by a Princeton University startup grant.

†Department of Computer Science, University of Texas at Austin. arao@cs.utexas.edu. Most of this work was done while the author was visiting Princeton University and the Institute for Advanced Study. Supported in part by an MCD fellowship from UT Austin and NSF Grant CCR-0310960.

‡Ronen Shaltiel, University of Haifa, Mount Carmel, Haifa, Israel. ronen@cs.haifa.ac.il. This research was supported by the United States-Israel Binational Science Foundation (BSF) grant 2004329.

§Institute for Advanced Study, Princeton, New Jersey. avi@math.ias.edu. This research was supported by NSF Grant CCR-0324906

STOC'06, May21–23, 2006, Seattle, Washington, USA.