Extractors: Optimal up to Constant Factors

Chi-Jen Lu
Institute of Information Science,
Academia Sinica, Taipei, Taiwan.
cjlu@iis.sinica.edu.tw

Omer Reingold[*]
AT&T Labs - Research.
omer@research.att.com

Salil Vadhan[†]
Harvard University.
salil@eecs.harvard.edu.

Avi Wigderson[‡]
Institute for Advanced Study, Princeton and the
Hebrew University , Jerusalem.
avi@ias.edu

ABSTRACT

This paper provides the first explicit construction of extractors which are simultaneously optimal up to constant factors in *both* seed length and output length. More precisely, for every n, k, our extractor uses a random seed of length $O(\log n)$ to transform any random source on n bits with (min-)entropy k, into a distribution on $(1 - \alpha)k$ bits that is ϵ-close to uniform. Here α and ϵ can be taken to be any positive constants. (In fact, ϵ can be almost polynomially small).

Our improvements are obtained via three new techniques, each of which may be of independent interest. The first is a general construction of *mergers* [22] from locally decodable error-correcting codes. The second introduces new *condensers* that have *constant seed length* (and retain a constant fraction of the min-entropy in the random source). The third is a way to augment the "win-win repeated condensing" paradigm of [17] with error reduction techniques like [15] so that the our constant seed-length condensers can be used without error accumulation.

Categories and Subject Descriptors

G.3 [**Probability and Statistics**]: Random number generation, Probabilistic algorithms; G.2 [**Discrete Mathematics**]: Combinatorics, Graph Theory; F.2 [**Analysis of Algorithms and Problem Complexity**]: General; H.1.1 [**Systems and Information Theory**]: Information theory

General Terms

Theory, Algorithms

Keywords

Randomness Extractors, Pseudorandomness, Condensers, Mergers, Locally Decodable Error-Correcting Codes

1. INTRODUCTION

Extractors are functions that extract almost-uniform bits from sources of biased and correlated bits. Since their introduction by Nisan and Zuckerman [14], extractors have played a fundamental and unifying role in the theory of pseudorandomness. In particular, it has been discovered that they are intimately related to a number of other important and widely studied objects, such as hash functions [9], expander graphs [14, 28, 18, 23, 4], samplers [7, 30], pseudorandom generators [26] and error-correcting codes [26, 25, 24]. In addition, extractors have been found to have a vast and ever-growing collection of applications in diverse aspects of computational complexity, combinatorics, and cryptography. See the excellent surveys [13, 19].

Like the other objects listed above, extractors with very good parameters can be nonconstructively shown to exist via the Probabilistic Method, but finding *explicit* constructions — ones computable in polynomial time — has been much more difficult. A long body of work has sought to find explicit constructions which approach the optimal, nonconstructive bounds.

In this paper, we achieve one of the goals of this line of work, namely the explicit construction of extractors that are "optimal up to constant factors". In order to make sense of this, we need to define extractors more precisely.

1.1 Extractors and their parameters

To formalize the notion of extractors we first need a measure of randomness in a source of biased and correlated bits.