Extracting Randomness via Repeated Condensing

Omer Reingold[*] Ronen Shaltiel[†] Avi Wigderson[‡]

Abstract

On an input probability distribution with some (min-)entropy an *extractor* outputs a distribution with a (near) maximum entropy rate (namely the uniform distribution). A natural weakening of this concept is a *condenser*, whose output distribution has a higher entropy rate than the input distribution (without losing much of the initial entropy).

In this paper we construct efficient explicit condensers. The condenser constructions combine (variants or more efficient versions of) ideas from several works, including the block extraction scheme of [NZ96], the observation made in [SZ94, NT99] that a failure of the block extraction scheme is also useful, the recursive "win-win" case analysis of [ISW99, ISW00], and the error correction of random sources used in [Tre99].

As a natural byproduct, (via repeated iterating of condensers), we obtain new extractor constructions. The new extractors give significant qualitative improvements over previous ones for sources of arbitrary min-entropy; they are nearly optimal *simultaneously* in the main two parameters - seed length and output length. Specifically, our extractors can make any of these two parameters optimal (up to a constant factor), only at a *poly-logarithmic* loss in the other. Previous constructions require *polynomial* loss in both cases for general sources.

We also give a simple reduction converting "standard" extractors (which are good for an average seed) to "strong" ones (which are good for most seeds), with essentially the same parameters. With it, all the above improvements apply to strong extractors as well.

[*] AT&T Labs - Research. Room A243, 180 Park Avenue, Bldg. 103, Florham Park, NJ, 07932, USA. E-mail: omer@research.att.com. Part of this research was performed while visiting the Institute for Advanced Study, Princeton, NJ.

[†] Department of Computer Science, Hebrew University, Jerusalem, Israel, and Institute for advanced study, Princeton, NJ. E-mail:ronens@cs.huji.ac.il.

[‡] Department of Computer Science, Hebrew University, Jerusalem, Israel, and Institute for advanced study, Princeton, NJ. E-mail:avi@ias.edu. This research was supported by USA-Israel BSF Grant 97-00188.