Kakeya sets, new mergers and old extractors

Zeev Dvir
Avi Wigderson

August 3, 2009

Abstract

A merger is a probabilistic procedure which extracts the randomness out of any (arbitrarily correlated) set of random variables, as long as one of them is uniform. Our main result is an efficient, simple, optimal (to constant factors) merger, which, for k random variables on n bits each, uses an $O(log(nk))$ seed, and whose error is $1/nk$. Our merger can be viewed as a derandomized version of the merger of Lu, Reingold, Vadhan and Wigderson (2003). Its analysis generalizes the recent resolution of the Kakeya problem in finite fields of Dvir (2008).

Following the plan set forth by Ta-Shma (1996), who defined mergers as part of this plan, our merger provides the last "missing link" to a simple and modular construction of extractors for all entropies, which is optimal to constant factors in all parameters. This complements the elegant construction of optimal extractor by Guruswami, Vadhan and Umans (2007).

We also give simple extensions of our merger in two directions. First, we generalize it to handle the case where no source is uniform in that case the merger will extract the entropy present in the most random of the given sources. Second, we observe that the merger works just as well in the computational setting, when the sources are efficiently samplable, and computational notions of entropy replace the information theoretic ones.