Explicit Two-Source Extractors and Resilient Functions

David Zuckerman, University of Texas, Austin

We explicitly construct an extractor for two independent sources on n bits, each with min-entropy at least log^C n for a large enough constant C. Our extractor outputs one bit and has error n^{-\Omega(1)}. The best previous extractor, by Bourgain, required each source to have min-entropy .499n.

A key ingredient in our construction is an explicit construction of a monotone, almost-balanced boolean function on n bits that is resilient to coalitions of size n^{1-delta}, for any delta>0. In fact, our construction is stronger in that it gives an explicit extractor for a generalization of non-oblivious bit-fixing sources on n bits, where some unknown n-q bits are chosen almost polylog(n)-wise independently, and the remaining q=n^{1-\delta} bits are chosen by an adversary as an arbitrary function of the n-q bits. The best previous construction, by Viola, achieved q=n^{1/2 - \delta}.

Our explicit two-source extractor directly implies an explicit construction of a 2^{(log log N)^{O(1)}}-Ramsey graph over N vertices, improving bounds obtained by Barak et al. and matching independent work by Cohen.

This is a joint work with Eshan Chattopadhyay.