Local Correlation Breakers and Applications to Mergers and Multi-Source Extractors

Abstract:

We introduce and construct a pseudo-random object which we call a local correlation breaker (LCB). This is an algorithm that gets as input a sequence of (possibly correlated) random variables and an independent weak source of randomness. The output of the LCB is a sequence of random variables with the following property. If the i'th input random variable is uniform then the i'th output variable is uniform even if a bounded number of any other output variables are given. That is, an LCB uses the weak-source to "break" local correlations between random variables.

Based on LCBs we obtain improved constructions of mergers with weak-seeds and multi-source extractors. In particular, we construct a 3-source extractor for entropies $\delta n$, $\mathcal{O}(\log n)$ and $\mathcal{O}(\log\log n)$, for any constant $\delta$. We further construct a 7-source extractor for poly-logarithmic entropy.

Joint work with Guy Rothblum.
No prior knowledge is assumed.