Dispersers for Affine Sources with Sub-polynomial Entropy

Ronen Shaltiel, Haifa University

Abstract

We construct an explicit disperser for affine sources over $\F_2^n$ with entropy $k = 2^{\log^{0.9} n} = n^{o(1)}$. More precisely, we construct a polynomial time computable function $D:\F_2^n \to \set{0,1}$ such that for every affine space V of $\F_2^n$ that has dimension at least k, $D(V)=\set{0,1}$ (meaning that D is not constant on V). This improves the best previous construction of Ben-Sasson and Kopparty that achieved $k = \Omega(n^{4/5})$, and is the first pseudorandom object for affine sources with entropy less than $\sqrt{n}$.

This research continues to a long line of work on "deterministic extraction from weak random sources" and I will use the opportunity to briefly survey this area.

Our technique follows a high level approach that was developed in two papers by Barak, Kindler, Shaltiel, Sudakov and Wigderson, and Barak, Rao, Shaltiel and Wigderson (in the context of explicit construction of 2-source dispersers and Ramsey graphs). We design a "challenge-response game" for affine sources. Loosely speaking, this is a function that receives one uniform sample from an arbitrary affine subspace of sufficiently large dimension, and is able (in some precise sense) to identify high entropy blocks in the input distribution.