

abstract

[Video of this lecture](#) COMPUTER SCIENCE/DISCRETE MATH II

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

An affine disperser over F_2^n for sources of dimension d is a function $f: F_2^n \rightarrow F_2$ such that for any affine subspace S in F_2^n of dimension at least d , we have $\{f(s) : s \in S\} = F_2$. Affine dispersers have been considered in the context of deterministic extraction of randomness from structured sources of imperfect randomness. Previously, explicit constructions of affine dispersers were known for every $d = O(n)$, due to Barak-Kindler-Shaltiel-Sudakov-Wigderson and Bourgain (the latter in fact gives stronger objects called affine extractors).

In this talk, I will describe an explicit affine disperser for sublinear dimension. Specifically, the disperser works even when $d = O(n^{\{4/5\}})$. The main novelty in our construction lies in the method of proof, which uses elementary properties of simple-but-powerful algebraic objects called subspace polynomials. In contrast, the previous works mentioned above relied on sum-product theorems for finite fields. (Joint work with Eli Ben-Sasson)