

abstract

COMPUTER SCIENCE/DISCRETE MATH I

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

This talk describes new explicit constructions of dispersers for affine sources of dimension below the notorious $n/2$ threshold. The main novelty in our construction lies in the method of proof which relies (solely) on elementary properties of linearized polynomials. In this respect we differ significantly from previous solutions to the problem, due to [Barak et al. 2005] and [Bourgain 2007]. These two breakthrough results used recent sum-product theorems over finite fields, whereas our analysis relies on properties of linearized polynomials that have been well-known since the work of Ore in the 1930's.

Definition of affine dispersers:

A disperser for affine sources of dimension d is a function $\text{Disp}: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ that is nonconstant on every affine space of dimension $> d$. Formally, for every affine $S \subseteq \mathbb{F}_2^n$, $\dim(S) > d$ we have $\{\text{Disp}(s) : s \in S\} = \{0, 1\}$.

Joint work with Swastik Kopparty.