Dvir, Zeev; Shpilka, Amir
Towards dimension expanders over finite fields. (English) Zbl 1265.05595

Summary: In this paper we study the problem of explicitly constructing a dimension expander raised by B. Barak, R. Impagliazzo, A. Shpilka and A. Wigderson [Unpublished Manuscript (2004)]: Let $\mathbb{F}^n$ be the $n$-dimensional linear space over the field $\mathbb{F}$. Find a small (ideally constant) set of linear transformations from $\mathbb{F}^n$ to itself $\{A_i\}_{i \in I}$ such that for every linear subspace $V \subset \mathbb{F}^n$ of dimension $\dim(V) < n/2$ we have
\[
\dim \left( \sum_{i \in I} A_i(V) \right) \geq (1 + \alpha) \cdot \dim(V),
\]
where $\alpha > 0$ is some constant. In other words, the dimension of the subspace spanned by $\{A_i(V)\}_{i \in I}$ should be at least $(1 + \alpha) \cdot \dim(V)$. For fields of characteristic zero Lubotzky and Zelmanov [J. Algebra 319, No. 2, 730–738 (2008; Zbl 1154.15002)] completely solved the problem by exhibiting a set of matrices, of size independent of $n$, having the dimension expansion property. In this paper we consider the finite field version of the problem and obtain the following results.

1. We give a constant number of matrices that expand the dimension of every subspace of dimension $d < n/2$ by a factor of $(1 + 1/\log n)$.

2. We give a set of $O(\log n)$ matrices with expanding factor of $(1 + \alpha)$, for some constant $\alpha > 0$.

Our constructions are algebraic in nature and rely on expanding Cayley graphs for the group $\mathbb{Z}/\mathbb{Z}n$ and small-diameter Cayley graphs for the group $SL_2(p)$.

MSC:
05E99 Algebraic combinatorics

Keywords:
dimension expander; finite field; Cayley graphs

Full Text: DOI

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.