Expanders from Symmetric Codes

Roy Meshulam
Technion, Haifa 32000, Israel and
Institute for Advanced Study, Princeton
meshulam@math.technion.ac.il

Avi Wigderson
Hebrew University, Jerusalem, and
Institute for Advanced Study, Princeton
avi@ias.edu

Abstract

A set $S$ in the vector space $\mathbb{F}_p^n$ is "good" if it satisfies any of the following (almost) equivalent conditions: (1) $S$ are the rows of a generating matrix for a linear distance code, (2) All (nontrivial) Fourier coefficients of $S$ are bounded away from 1, (3) The Cayley graph on $\mathbb{F}_p^n$ with generator $S$ is a good expander.

A good set $S$ must have at least $cn$ vectors (with $c > 1$). We study conditions under which $S$ is the orbit of only a constant number of vectors, under the action of a finite group $G$ on the $n$ coordinates. Such succinctly described sets yield very symmetric codes, and can "amplify" small constant-degree Cayley expanders to exponentially larger ones.

For the regular action (the coordinates are named by the elements of the group $G$), we develop representation theoretic conditions on the group $G$ which guarantee the existence (in fact, abundance) of such few expanding orbits. The condition is a (nearly tight) upper bound on the distribution of dimensions of the irreducible representations of $G$, and is the main technical contribution of this paper. We further show a class of groups for which this condition is implied by the expansion properties of the group $G$ itself.

Combining these, we can iterate the amplification process above, and give (near constant degree) Cayley expanders which are built from Abelian components.

For other natural actions, such as of the affine group on a finite field, we give the first explicit construction of such few expanding orbits.

1 Technical summary

Below we list the main technical results of the paper. More details, intuition and references can be found in the proceedings of STOC 2002.

Identify $\mathbb{F}_p^n$ with the group algebra $\mathbb{F}_p[G]$. For a vector $f$ let $Gf = \{ \sigma f : \sigma \in G \}$ denote the orbit of $f$ under $G$. We first give a representation theoretic condition which guarantees the existence of few orbits whose union form an expander in $\mathbb{F}_p[G]$.

Let $r_d(G; \mathbb{F})$ denote the number of irreducible representations of $G$ over $\mathbb{F}$ of dimension at most $d$ and let

$$m(G; \mathbb{F}) = \max_{d \geq 1} \frac{\log r_d(G; \mathbb{F})}{d}.$$ 

Theorem 1.1 Suppose $(p, n) = 1$. Then for any $\delta < \frac{1}{4}$ there exist $t = O\left( \frac{1}{t^{1-2\delta}} (m(G; \mathbb{F}_p) + \log p) \right)$ elements $h_1, \ldots, h_t \in \mathbb{F}_p[G]$ such that the multiset $S = \cup_{i=1}^t G h_i \subset \mathbb{F}_p[G]$ is a $\delta$-expander (i.e. the spectral gap is $\delta$).

We next show a class of groups for which the boundedness of $m(G; \mathbb{C})$ and hence the existence of few expanding orbits in $\mathbb{F}_p[G]$ is in fact implied by the expansion properties of the group $G$ itself. For a symmetric generating set of $G$, let $\lambda_G(S)$ denote the spectral gap in the normalized adjacency matrix of the Cayley graph $C(G, S)$. The group $G$ is an $M_t$-group if for any complex irreducible representation of $G$ is induced from a representation of dimension at most $t$ of some subgroup $H \subset G$.

Theorem 1.2 There exists a constant $c$ such that for any $M_t$-group $G$ and $d \geq 1$

$$r_d(G; \mathbb{C}) \leq \left( \frac{c}{\lambda_G(S)^2} \right)^d |d|.$$

Results of Lubotzky and Weiss imply that if $G$ is a solvable group of derived length $\ell$ and $S \subset G$ is a generating set such that $\lambda_G(S) \geq 1/2$ then $|S| \geq \log(\ell^n) |G|$ (log$^n$ denotes the $n$ times iterated logarithm). Our third result combines the Zig-Zag construction of Reingold, Vadhan and Wigderson with Theorems 1.1 and 1.2 to give an example of a sequence of solvable groups which comes close to the Lubotzky-Weiss bound. Let $\{p_i\}_{i \geq 1}$ denote the sequence of odd primes. Let $G_0 = S_0 = \mathbb{F}_2$ and for $n \geq 0$ let $G_{n+1}$ be the semi-direct product of $G_n$ and $\mathbb{F}_{p_n}[G_n]$.

Theorem 1.3 There exist symmetric generating sets $S_n$ of $G_n$ such that $\lambda_{G_n}(S_n) \geq \frac{1}{4}$ and for sufficiently large $n$

$$|S_n| \leq \log^{(n/2)} |G_n|.$$