Expanders in Group algebras

Roy Meshulam[*]and Avi Wigderson[†]

Abstract

Let G be a finite group and let p be a prime such that $(p, |G|) = 1$. We study conditions under which the Abelian group $\mathbb{F}_p[G]$ has a few G-orbits whose union generate it as an expander (equivalently, all the discrete Fourier coefficients (in absolute value) of this generating set are bounded away uniformly from one).

We prove a (nearly sharp) bound on the distribution of dimensions of irreducible representations of G which implies the existence of such expanding orbits. We further show a class of groups for which such a bound follows from the expansion properties of G. Together, these lead to a new iterative construction of expanding Cayley graphs of nearly constant degree.

1 Introduction

We first describe our results and their context in a high level, relatively informal style. We then give precise definitions and theorems.

1.1 Background and Motivation

A graph is called an α *-expander* if the first nonzero eigenvalue of its Laplacian is at least $\alpha > 0$ (equivalently the ratio between the first and second largest eigenvalues of its adjacency matrix is at most $1-\alpha < 1$). An expander family

[*]Department of Mathematics, Technion, Haifa 32000, Israel and Institute for Advanced Study, Princeton. e-mail: meshulammath.technion.ac.il

[†]Hebrew university, Jerusalem and Institute for Advanced Study, Princeton. email: avi@ias.edu

is a sequence of graphs which are all α -expanders with the same α. A single graph will be called an expander only in the context of some such family.

Expander graphs are highly connected: all small sets of vertices have many neighbors; all cuts have many edges; and the random walk converges to the stationary (uniforms) distribution extremely quickly. Indeed, the original definition of expanders (and the reason for their name) was in terms of connectivity properties, and the connection to the spectral gap was developed in [Tan84, AM84, A86].

Sparse expanders, especially those which can be explicitly and efficiently constructed, have numerous diverse applications both in Computer Science and in pure Mathematics. The challenge to explicitly construct such graphs was met successfully - there are several explicit families of expanders of constant degree. Until last year, essentially all explicit constructions were of algebraic nature - they were either Cayley graphs of certain groups (e.g. [AM84, LPS88, Mar88]), or graphs whose vertices are identified with some algebraic structure on which there is a natural action of a group preserving adjacency (e.g. [Mar73, GG81]). Moreover, the groups used in all of these constructions were finite quotients of the infinite groups $SL_n(Z)$ and their relatives, which posses Kazhdan's property T or at least its relative property τ (see [L94] for details).

In this paper we'll give a completely different family of (near-constant degree) expanding Cayley graphs. In particular, the groups involved will be solvable, and moreover will have huge Abelian subgroups. Another difference will be that they will be constructed iteratively, rather than as quotients of one infinite "mother" group.

The motivation and starting point for our paper are the recent papers [RVW00, ALW01]. The first paper [RVW00] broke the mold of algebraic expander constructions. It introduced the zig-zag product on graphs, and proved that it preserves expansion. This allowed the construction of large expanding graphs from smaller ones (without enlarging the degree) and led to a combinatorial iterative construction of constant degree expander families. The second paper [ALW01] observed that the zig-zag graph product can be viewed as a generalization of the classical semi-direct product in groups. With some provisos, this allowed the construction of large expanding Cayley graphs from small ones. To understand their construction, and how it leads to our work, we give some more detail.

Let G be a group, and assume it has a small *expanding* generating set S (namely the Cayley graph $C(G;S)$ is an expander). Now assume G acts on another group H. When can we have a small expanding set of generators for the semi-direct product $G \times H$? A sufficient condition proved in [ALW01] (using [RVW00]) is that H has an (not necessarily small) expanding generating set which is the union of a few G-orbits. Furthermore, they prove that this condition is satisfied for an arbitrary group G, and H is the invariant subspace of any *irreducible* representation of G over a fixed finite field (note that H is Abelian!).

This idea gives hope that sparse expanding Cayley graphs may now be constructed iteratively (as in [RVW00]), by somehow iterating the above procedure. But understanding the irreducible representations of the newly constructed groups seems to be essential for the argument, and this seems quite complex.

1.2 Overview of our Results

A natural idea to facilitate iteration is to try something more generic, namely to take $H = \mathbb{F}_p[G]$, the group algebra of G over $\mathbb{F}_p$ (this is simply the vector space over $\mathbb{F}_p$ whose coordinates are labelled by elements of G). If G were a Cayley expander, and we could find a few expanding G-orbits in $\mathbb{F}_p[G]$ then $G \ltimes \mathbb{F}_p[G]$ would be a larger Cayley expander and we could repeat the argument.

It is interesting to note that in this setting such constant number s of orbits actually forms the generating matrix of an asymptotically good linear error correcting code which is highly symmetric. This code is invariant under the diagonal action of G on $\mathbb{F}_p[G]^s$. In contrast with cyclic codes this action is of course non transitive on the coordinates.

How can we guarantee the existence of such few generating orbits? As in [ALW01], these s orbits will be chosen randomly. What becomes much harder is the analysis. A key simplifying factor in the [ALW01] analysis is that, when H is an irreducible representation, *all* orbits have full rank. This is not true for $H = \mathbb{F}_p[G]$. To fix this, we go through a chain of reductions involving the growth of several group theoretic functions, and their (surprising?) relation to expansion.

We first note that the analysis in [ALW01] goes through if the number of orbits of rank r grows at most exponentially with r. We then give a natural condition on G which ensures this growth: the number of irreducible complex representations of G of dimension d grows at most exponentially with d. We now show that if G is a *monomial*[1] group, such a bound follows from the expansion properties of G (which we inductively assume!). We finally prove that if G is monomial, so is $G \ltimes \mathbb{F}_p[G]$.

This facilitates the iterative construction (using distinct primes p), which can start with any Abelian group[2]. The components of the construction are symmetric linear codes, which are "glued" using the semi-direct (=zig-zag) product. As each new code is exponentially larger than its predecessor, the "non-Abelian" part of any group in this sequence is only of logarithmic size! Moreover, this fact controls the growth of the degrees in our expanders to be only slightly more than constant.

To summarize, denoting the resulting sequence of groups G_n and their respective generating sets S_n we have the following: all G_n are 1/2-expanders, with $|S_n| \leq O(\log^{(n-\log^* n)} |G_n|)$ (where $\log^{(k)}$ denotes the k time iterated logarithm function).

We find the connection between the expansion of groups and the growth rate of the above functions defined by the group interesting in its own right. We compute them for some concrete groups, and use it to show that the sufficient conditions we give on the growth functions of ranks and dimensions are essentially tight.

Finally, we touch the explicitness issue. The basic construction above (and thus also the iterative one) uses a probabilistic argument to show the existence of few expanding orbits. This is not explicit, and a derandomization of this argument would be very interesting. Nevertheless, it is far more explicit than generating the whole graph at random. Observe that given these (randomly chosen) orbit representatives, neighbors of a vertex can be computed efficiently, and thus an expanding Cayley graph of size $\exp(n)$ can be described by a Boolean circuit of size polynomial in n.

To be completely explicit, we move back into the general setting of a group G acting on a set X which labels the coordinates of the vector space H. In this setting, we give the first explicit construction of a constant number of expanding orbits, for some natural choices of G and X above. We exhibit two expanding G-orbits in $\mathbb{F}_2[X]$ where

[1] We define it later. It is however worth noting that in such groups the number of subgroups of index i grows exponentially with i, a property which is used to prove the last implication

[2] To allow an arbitrary group as a starting point, we generalize the above to the so called M_ℓ-groups.

- X is the finite field $\mathbb{F}_p$ and G is the group of affine linear transformations acting on it.

- X is the projective line $\mathbb{F}_p \cup \{\infty\}$ and G is the group $SL_2(p)$, acting on X as Mobius transformations.

Note that the second case is exactly the one used by [ALW01] to exhibit a group which can be expanding with one set of generators and non-expanding with another. They used a probabilistic argument to obtain the expanding generators, and the result above completely derandomizes their construction.

1.3 Definitions and Results

This work uses some elements of the Representation Theory of finite groups. We try to give precise references for key results we use. Our main general references are the books of Aschbacher [Asc00] and Isaacs [Is76].

Let G be a finite group and let $\mathbb{F}[G]$ denote the group algebra of G over the field $\mathbb{F}$. We always assume that the characteristic of $\mathbb{F}$ is coprime to $|G|$. The *Fourier Transform* of $f = \sum_{x \in G} f(x)x \in \mathbb{F}[G]$ at a representation $\rho : G \to \mathrm{GL}(V_\rho)$ is given by

$$\widehat{f}(\rho) = \sum_{x \in G} f(x)\rho(x^{-1}) \in \mathrm{End}_{\mathbb{F}}(V_\rho) \ .$$

Let S be a generating multiset of G of cardinality $|S| = l$ and let $h = \frac{1}{l} \sum_{s \in S} s \in \mathbb{C}[G]$. The *Kazhdan Constant* of S is given by

$$\tilde{\kappa}_G(S) = \min_{\rho} \min_{\{v \in V_\rho : \|v\|_2 = 1\}} \|\widehat{h}(\rho)v - v\|_2$$

where ρ ranges over all unitary representations of G which do not contain the trivial representation. It is easy to see that the minimum is always attained at an irreducible representation.

This definition slightly deviates from the usual definition of the Kazhdan constant, see e.g. [HRV93]. We take the average (rather than the original definition which takes the maximum) over the generators; this makes the notion robust for any number of generators (not necessarily constant), and makes the expansion based on it equivalent to the one using the spectral gap (see below).

When S is symmetric, the Kazhdan constant has the following spectral interpretation: Let $C = C(G; S)$ denote the Cayley graph of G with respect to S and let $M(C)$ denote the normalized Laplacian of C. Then $\tilde{\kappa}_G(S)$ is equal to the first non-zero eigenvalue of $M(C)$. Equivalently, it is the eigenvalue gap in the transition probability matrix of the random walk on the graph C. Thus, in the notation of the first subsection, C is a $\tilde{\kappa}_G(S)$-expander. This connection has been observed in many previous papers – however, since they used the original definition of the Kazhdan constant, it was not tight. Summarizing the above, we have

Fact 1.1 $\tilde{\kappa}_G(S) = 1 - \lambda(C(G; S))$
where $\lambda(C)$ *is the second largest eigenvalue of the random walk matrix on* C.

This value controls the expansion properties of C. In some papers, the second largest *in absolute value* eigenvalue is used to define expansion. The conversion between the two notions is easy – simply add self loops with probability 1/2 to each vertex (in other words, add $|S|$ identity elements to the generating set). All eigenvalues become nonnegative, the random walk becomes ergodic, and the spectral gap shrinks by a factor of 2.

For an Abelian group H it is especially easy to compute the expansion, as all irreducible representations are 1-dimensional.

$$\tilde{\kappa}_H(S) = \min_{\chi \neq 1} |\frac{1}{l} \sum_{s \in S} \chi(s) - 1| \tag{1}$$

where χ ranges over all non-trivial characters of H.

Let p be a prime such that $(p, |G|) = 1$. We will be interested in expanding generators for the group algebra $\mathbb{F}_p[G]$ as an Abelian group. The inner product of two elements $f = \sum_{x \in G} f(x)x$, $g = \sum_{x \in G} g(x)x \in \mathbb{F}_p[G]$ is given by $f \cdot g = \sum_{x \in G} f(x)g(x) \in \mathbb{F}_p$. Let $e_p(\alpha) = \exp(\frac{2\pi\alpha i}{p})$. A multiset $A \subset \mathbb{F}_p[G]$ is *δ-balanced* if for all $0 \neq f \in \mathbb{F}_p[G]$

$$|\sum_{h \in A} e_p(f \cdot h)| \leq (1 - \delta)|A| \ .$$

By (1) if A is δ-balanced then $\tilde{\kappa}_{\mathbb{F}_p[G]}(A) \geq \delta$.
For $f \in \mathbb{F}_p[G]$ let $Gf = \{\sigma f : \sigma \in G\}$ denote the orbit of f under G. It will be convenient to regard Gf as a multiset with $|G|$ elements.

This work is concerned with representation theoretic conditions which guarantee the existence of few orbits whose union form a balanced set in $\mathbb{F}_p[G]$ and with an application to the construction of expanding groups.
Let $r_d(G;\mathbb{F})$ denote the number of irreducible representations of G over $\mathbb{F}$ of dimension at most d and let

$$m(G;\mathbb{F}) = \max_{d\geq 1} \frac{\log_2 r_d(G;\mathbb{F})}{d} \ .$$

Theorem 1.2 *For any $\delta < \frac{1}{2}$ there exist $s = O(\frac{1}{(1-2\delta)^2}(m(G;\mathbb{F}_p) + \log p))$ elements $h_1,\ldots,h_s \in \mathbb{F}_p[G]$ such that the multiset $A = \cup_{i=1}^{s} Gh_i \subset \mathbb{F}_p[G]$ is δ-balanced. Indeed, a random choice of the elements h_i will guarantee this property with arbitrarily high probability.*

The proof of Theorem 1.2 given in section 3 combines the approach of Alon, Lubotzky and Wigderson [ALW01] with some estimates on the distribution of ranks in the group algebra given in section 2.
In section 4 we consider the number of the unitary $d-$dimensional representations of G and its connection with the Kazhdan constants of a generating set $S \subset G$. Wasserman [Wa91] showed that $r_d(G) = r_d(G;\mathbb{C})$ can be bounded in terms of d , $|S|$ and $\tilde{\kappa}_G(S)$ alone. An explicit form of his argument due to de la Harpe, Robertson and Vallete [HRV93] gives the following

Theorem 1.3 *([Wa91, HRV93])*

$$r_d(G) \leq (\frac{1}{\tilde{\kappa}_G(S)})^{O(|S|d^2)} \ .$$

For applications involving Theorem 1.2 we need a sharper bound which we can only prove in the following restricted case. A group G is an M_ℓ-group if any complex irreducible representation of G is induced from a representation of dimension at most ℓ of some subgroup $H \subset G$. A group with property M_1 is called a *Monomial group.*

Theorem 1.4 *There exists a constant c such that for any M_ℓ-group G and $d \geq 1$*

$$r_d(G) \leq (\frac{c}{\tilde{\kappa}_G(S)})^{2\ell|S|d} \ . \qquad (2)$$

As a consequence we obtain

Theorem 1.5 *Let G be an M_ℓ-group with a generating set S. Then there exist $s = O(\log p + \ell|S| \log \frac{1}{\tilde{\kappa}_G(S)})$ orbits whose union is $\frac{1}{3}$-balanced.*

For a group G, let $G^{(k)}$ be given by $G^{(0)} = G$ and $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$. The *derived length* of a solvable group G is the minimal n such that $G^{(n)} = 1$. Results of Lubotzky and Weiss [LW93] imply the following

Proposition 1.6 *Let G be a solvable group of derived length n. If $S \subseteq G$ is a generating set such that $\tilde{\kappa}_G(S) \geq 1/2$ then $|S| = \Omega(\log^{(n)} |G|)$.*

In section 5 we combine the Zig-zag construction of Reingold, Vadhan and Wigderson [RVW00] with Theorem 1.5 to give a simple example (below) of a sequence of solvable groups which come close to the bound of Proposition 1.6. 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 $G_{n+1} = G_n \ltimes \mathbb{F}_{p_n}[G_n]$.

Theorem 1.7 *There exist symmetric generating sets S_n of G_n such that $\tilde{\kappa}_{G_n}(S_n) \geq \frac{1}{2}$ and for sufficiently large n*

$$|S_n| \leq \log^{(n-\log^* n)} |G_n| \ .$$

In section 6 we give an explicit construction of two expanding orbits for $\mathbb{F}_2[\mathbb{F}_p]$ under the action of the affine group $G = \mathrm{Aff}(p)$ where $p \equiv 1(4)$. Let $v \in H$ be the characteristic function of $\{0\}$ and let $u \in H$ be the characteristic function of $I = \{1, 2, \ldots, \frac{p-1}{2}\}$.

Theorem 1.8 *The set $S = \{Gv, Gu\} \subset H$ is .01 balanced.*

Let $v_1, u_1 \in \mathbb{F}_2[PG(2, \mathbb{F}_p)] = H_1$ denote the images of v, u under the embedding $x \rightarrow (x, 1)$ of $\mathbb{F}_p$ in the projective line $PG(1, p)$. Let $G_1 = SL(2, p)$ then

Theorem 1.9 *The set $S_1 = \{G_1 v_1, G_1 u_1\} \subset H_1$ is .01 balanced.*

2 Rank Varieties in Group Algebras

In this section we relate the distribution of ranks in the group algebra of G to the distribution of dimensions of the irreducible representations of G.

Let $\mathbb{F}$ be a field of characteristic coprime to $|G|$ and let $\mathrm{Irr}(G; \mathbb{F})$ denote the set of irreducible representations of G over $\mathbb{F}$. For $f = \sum_{x \in G} f(x)x \in \mathbb{F}[G]$

let $T_f : \mathbb{F}[G] \to \mathbb{F}[G]$ be the linear map given by $T_f(h) = hf$. Clearly $\dim \mathrm{Span}\; Gf = \mathrm{rank}\; T_f$. Let

$$V_r(\mathbb{F}) = \{f \in \mathbb{F}[G] \;:\; \mathrm{rank}\; T_f \leq r\} \;.$$

While we are mainly interested in the cardinality of $V_r(\mathbb{F})$ when $\mathbb{F} = \mathbb{F}_q$ is finite, it is instructive to first determine $\dim V_r(\mathbb{F})$ when $\mathbb{F}$ is algebraically closed.
Let $M_d(\mathbb{F})$ denote the space of $d \ltimes d$ matrices over $\mathbb{F}$ and let

$$R_{d,k}(\mathbb{F}) = \{A \in M_d(\mathbb{F}) : \mathrm{rank}\; A = k\}.$$

When $\mathbb{F}$ is algebraically closed the closure $\overline{R_{d,k}(\mathbb{F})}$ is an affine irreducible algebraic variety and

$$\dim \overline{R_{d,k}(\mathbb{F})} = k(2d-k). \tag{3}$$

In the finite field case

$$|R_{d,k}(\mathbb{F}_q)| = N(q;d,k) =$$

$$\frac{u(d,q)^2}{u(k,q)u(d-k,q)^2}\; q^{k(2d-k)} \;\leq C(q)\; q^{k(2d-k)}$$

where $u(m,x) = \prod_{i=1}^{m}(1-x^{-i})$ and $C(q) = \prod_{i=1}^{\infty}(1-q^{-i})^{-1} < 4$.

Suppose $\mathbb{F}$ is algebraically closed and let $\mathrm{Irr}(G;\mathbb{F}) = \{\rho_1,\ldots,\rho_t\}$ where $\rho_i : G \to \mathrm{GL}(V_i)$ and $\dim_{\mathbb{F}} V_i = d_i$.

Claim 2.1

$$\dim V_r(\mathbb{F}) = \max\{\sum_{i=1}^{t} k_i(2d_i - k_i) : 0 \leq k_i \leq d_i \;,\; \sum_{i=1}^{t} k_i d_i \leq r\} \;. \tag{4}$$

In particular $\dim V_r \leq 2r$.

Proof: Let

$$\phi : \mathbb{F}[G] \to \prod_{i=1}^{t} \mathrm{End}(V_i)$$

denote the Fourier Transform isomorphism given by

$$\phi(f) = (\widehat{f}(\rho_1),\ldots,\widehat{f}(\rho_t)) \;.$$

For $A = (A_1, \dots, A_t) \in \prod_{i=1}^t \mathrm{End}(V_i)$ let S_A denote the endomorphism of $\prod_{i=1}^t \mathrm{End}(V_i)$ given by

$$S_A(X_1, \dots, X_t) = (X_1 A_1, \dots, X_t A_t) \ .$$

Commutativity $S_{\phi(f)}\phi = \phi T_f$ implies

$$\text{rank } T_f = \text{rank } S_{\phi(f)} = \sum_{i=1}^t d_i \text{ rank } \widehat{f}(\rho_i) \ .$$

Therefore

$$\phi(V_r(\mathbb{F})) = \{(A_1, \dots, A_t) : \sum_{i=1}^t d_i \text{ rank } A_i \le r\}$$

and (4) follows from (3) .

$\square$

We now turn to the finite field case. The Galois group $\Gamma = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ acts naturally on the set $\mathrm{Irr}(G; \overline{\mathbb{F}_q})$ of irreducible representations of G over $\overline{\mathbb{F}_q}$. Let $\mathcal{F}_1, \dots, \mathcal{F}_t$ denote the orbits of $\mathrm{Irr}(G; \overline{\mathbb{F}_q})$ under Γ and for each $1 \le i \le t$ choose a representative $\eta_i \in \mathcal{F}_i$ of dimension d_i. Let $\Gamma_i < \Gamma$ denote the stabilizer of η_i and let σ denote the Frobenius automorphism $\sigma(x) = x^q$. For $e_i = (\Gamma : \Gamma_i)$ the direct sum $\oplus_{j=0}^{e_i - 1} \eta_i^{\sigma^j}$ is equivalent to a $d_i e_i$-dimensional irreducible $\mathbb{F}_q-$representation ρ_i of G. All irreducible representations of G arise this way, thus $\mathrm{Irr}(G; \mathbb{F}_q) = \{\rho_1, \dots, \rho_t\}$ and

$$\mathbb{F}_q[G] \cong \prod_{i=1}^t M_{d_i}(\mathbb{F}_{q^{e_i}}) \ .$$

For $A = (A_1, \dots, A_t) \in \prod_{i=1}^t M_{d_i}(\mathbb{F}_{q^{e_i}})$ let S_A denote the endomorphism of the $\mathbb{F}_q$-space $\prod_{i=1}^t M_{d_i}(\mathbb{F}_{q^{e_i}})$ given by

$$S_A(X_1, \dots, X_t) = (X_1 A_1, \dots, X_t A_t) \ .$$

Clearly

$$\text{rank } S_A = \sum_{i=1}^t d_i e_i \text{ rank}_{\mathbb{F}_{q^{e_i}}} A_i \ .$$

Denoting

$$K_r = \{\mathbf{k} = (k_i : 1 \le i \le t) : 0 \le k_i \le d_i \ , \sum_{i=1}^{t} k_i d_i e_i = r\}$$

it follows that

$$|\{f \in \mathbf{F}_q[G] \ : \ \text{rank } T_f = r\}| = \sum_{\mathbf{k}\in K_r} \prod_{i=1}^{t} N(q^{e_i}; d_i, k_i) \ . \tag{5}$$

Let

$$\gamma(z) = \sum_{f\in \mathbf{F}_q[G]} z^{\text{rank } T_f}$$

be the generating function of the ranks attained in $\mathbf{F}_q[G]$. Equation (5) implies the following

Proposition 2.2

$$\gamma(z) = \prod_{i=1}^{t} (\sum_{k_i=0}^{d_i} N(q^{e_i}; d_i, k_i) \ z^{e_i k_i d_i}) \ .$$

□

3 Balanced Orbits

In this section we prove Theorem 1.2, that when the distribution of ranks is controlled, the group algebra has a few expanding orbits. In the following two subsections, we give examples of groups in which (respectively) have/ do not have this property (exhibiting the near tightness of our bounds).

Let $|G| = n$. We regard $\mathbf{F}_p[G]^s$ as a probability space with the uniform distribution.
For $f \in \mathbf{F}_p[G]$ and $\delta > 0$ let $B_\delta(f) =$

$$\{(h_1, \dots, h_s) \in \mathbf{F}_p[G]^s \ : \ |\frac{1}{sn} \sum_{i=1}^{s} \sum_{\sigma\in G} e_p(\sigma h_i \cdot f)| > 1 - \delta\} \ .$$

For $f_1, \dots, f_r \in \mathbf{F}_p[G]$ let $C_\delta(f_1, \dots, f_r) =$

$$\{(h_1, \dots, h_s) \in \mathbf{F}_p[G]^s \ : \ |\frac{1}{rs} \sum_{i=1}^{s} \sum_{j=1}^{r} e_p(h_i \cdot f_j)| > 1 - \delta\} \ .$$

Claim 3.1 *If $f_1, \ldots, f_r$ are linearly independent in $\mathbf{F}_p[G]$ then*

$$\Pr(C_\delta(f_1, \ldots, f_r)) \leq 4 \exp(\frac{-(1-\delta)^2 rs}{4}) \ . \tag{6}$$

Proof: For $1 \leq i \leq s$, $1 \leq j \leq r$ let X_{ij} denote the complex valued random variable $e_p(h_i \cdot f_j)$. The X_{ij} are clearly independent and $\|X_{ij}\|_\infty = 1$, hence (6) follows from the Chernoff bound.

□

The following result uses an idea of Alon, Lubotzky and Wigderson [ALW01].

Proposition 3.2 *If* rank $T_f = r$ *then*

$$\Pr(B_\delta(f)) \leq 8 \exp(\frac{-(1-2\delta)^2 rs}{4}) \ .$$

Proof: Let $\tau_1, \ldots, \tau_r \in G$ such that $\tau_1 f, \ldots, \tau_r f$ are linearly independent in $\mathbf{F}_p[G]$. Then

$$\frac{1}{sn} \sum_{\sigma \in G} \sum_{i=1}^{s} e_p(\sigma h_i \cdot f) = \frac{1}{rsn} \sum_{\sigma \in G} \sum_{i=1}^{s} \sum_{j=1}^{r} e_p(\tau_j^{-1} \sigma h_i \cdot f) =$$

$$\frac{1}{n} \sum_{\sigma \in G} (\frac{1}{rs} \sum_{i=1}^{s} \sum_{j=1}^{r} e_p(\sigma h_i \cdot \tau_j f)) \ .$$

It follows that if $(h_1, \ldots, h_s) \in B_\delta(f)$ then

$$(\sigma h_1, \ldots, \sigma h_s) \in C_{2\delta}(\tau_1 f, \ldots, \tau_r f)$$

for at least $\frac{n}{2}$ elements σ in G. Hence

$$\Pr(B_\delta(f)) \leq 2 \ \Pr(C_{2\delta}(\tau_1 f, \ldots, \tau_r f)) \leq 8 \exp(\frac{-(1-2\delta)^2 rs}{4}) \ .$$

□

Proof of Theorem 1.2: Keeping the notation of section 2 let $\mathrm{Irr}(G; \mathbf{F}_p) = \{\rho_1, \ldots, \rho_t\}$ where ρ_i is of dimension $d_i e_i$, and

$$\mathbf{F}_p[G] \cong \prod_{i=1}^{t} M_{d_i}(\mathbf{F}_{p^{e_i}}) \ . \tag{7}$$

Let $m = m(G;\mathbf{F}_p)$, $s = \frac{4}{(1-2\delta)^2}(m + 2\log_2 p + 7)$, $\lambda = 4p^2 \exp(-\frac{(1-2\delta)^2 s}{4})$. Choose $h_1, \ldots, h_s$ uniformly at random from $\mathbf{F}_p[G]$. The probability that $A(h_1, \ldots, h_s) = \cup_{i=1}^s G h_i$ is not δ-balanced is

$$\Pr(\bigcup_{0\neq f\in\mathbf{F}_p[G]} B_\delta(f)) \leq \sum_{0\neq f\in\mathbf{F}_p[G]} \Pr(B_\delta(f)) \leq$$

$$8\sum_{r\geq 1} |V_r(\mathbf{F}_p)| \exp(\frac{-(1-2\delta)^2 rs}{4}) \ = 8\gamma(\exp(\frac{-(1-2\delta)^2 s}{4}) - 8 \leq$$

$$8\prod_{i=1}^{t}(\sum_{k_i=0}^{d_i} 4p^{k_i(2d_i-k_i)e_i} \exp(\frac{-(1-2\delta)^2 s k_i e_i d_i}{4}) - 8 \leq$$

$$8\prod_{i=1}^{t}(\sum_{k_i=0}^{\infty} \lambda^{d_i e_i k_i}) - 8 = 8\prod_{i=1}^{t}(1-\lambda^{d_i e_i})^{-1} - 8 =$$

$$8\prod_{l\geq 1}(1-\lambda^l)^{-|\{i:d_i e_i = l\}|} - 8 \leq 8\exp(2\sum_{l\geq 1}(\lambda 2^m)^l) - 8 <$$

$$8\exp(2\sum_{l=1}^{\infty} 30^{-l}) - 8 < 1 \ .$$

It follows that there exist $h_1, \ldots, h_s$ such that $A(h_1, \ldots, h_s)$ is $\delta-$balanced. To make the failure probability arbitrarily small, note that the above argument shows that if $s = \frac{4}{(1-2\delta)^2}(m + 2\log_2 p + z)$ (for any z) then the probability that $A(h_1, \ldots, h_s)$ is not $\delta-$balanced is $O(2^{-z})$.

□

3.1 Groups whose algebras have few expanding orbits

1. The symmetric group S_n has $\exp(O(\sqrt{n}))$ complex irreducible representations and only two are of dimension $< n-1$. It follows that $m(S_n;\mathbf{F}_p) \leq m(S_n;\mathbf{C}) = O(1)$. By Theorem 1.2 $\mathbf{F}_p[S_n]$ contains $\frac{1}{3}-$balanced sets which are unions of $O(\log p)$ orbits.

2. The special linear group $\mathrm{SL}_2(q)$ has $\sim q$ complex representations of dimension $\sim q$, hence again $m(\mathrm{SL}_2(q);\mathbf{F}_p) = O(1)$. By Theorem 1.2 $\mathbf{F}_p[\mathrm{SL}_2(q)]$ contains $\frac{1}{3}-$balanced sets which are unions of $O(\log p)$ orbits.

3. Let $C_n = \langle x \rangle$ denote the cyclic group of odd order n, and let ω be a primitive $n-$th root of unity in $\overline{\mathbf{F}_2}$. The characters $\{\chi_k\}_{k=0}^{n-1}$ of C_n over $\overline{\mathbf{F}_2}$ are given by $\chi_k(x^j) = \omega^{kj}$. The cardinality of the orbit of χ_k under the Galois group $\mathrm{Gal}(\overline{\mathbf{F}_2}/\mathbf{F}_2)$ is equal to the order of 2 in the multiplicative group of $\mathbf{Z}_{\frac{n}{\gcd(k,n)}}$. It follows that for $k \geq 1$

$$|\mathrm{Orbit}(\chi_k)| \geq \log_2(\frac{n}{\gcd(k,n)} + 1)$$

hence

$$|\{1 \leq k \leq n-1 : |\mathrm{Orbit}(\chi_k)| = l\}| \leq 2^l - 2$$

and

$$r_d(C_n;\mathbf{F}_2) = 1 + \sum_{l=1}^{d} \frac{|\{k \;:\; |\mathrm{Orbit}(\chi_k)| = l\}|}{l} \leq$$

$$1 + \sum_{l=1}^{d} \frac{2^l - 2}{l} \leq 2^d - 1 \ .$$

Therefore $m(C_n;\mathbf{F}_2) \leq 1$ and $\mathbf{F}_2[C_n]$ contains $O(\frac{1}{(1-2\delta)^2})$ orbits whose union is δ-balanced.

3.2 Groups whose algebras require many orbits to expand

In this section we show that Theorem 1.2 is nearly sharp for $G = \mathbf{F}_2^n$.

Proposition 3.3 *For sufficiently large n, no union of $s = \frac{\delta n}{10}$ orbits in $\mathbf{F}_3[\mathbf{F}_2^n]$ is $\delta-$balanced.*

We need the following Ramsey type result of Brown and Buhler [BB82] .

Claim 3.4 *If $C \subset \mathbf{F}_2^n$ satisfies $|C| \geq 2^{\frac{(2^d-1)n}{2^d}+2}$, then C contains an affine $d-$dimensional subspace.* $\square$

Proof of Proposition 3.3: We regard an element $h \in \mathbf{F}_3[\mathbf{F}_2^n]$ as a function $h : \mathbf{F}_2^n \to \mathbf{F}_3$. The action of $x \in \mathbf{F}_2^n$ on $h \in \mathbf{F}_3[\mathbf{F}_2^n]$ is thus given by $h^x(y) = h(x+y)$. For $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbf{F}_2^n$ let $x \bullet y = \sum_{i=1}^{n} x_i y_i \in \mathbf{F}_2$ denote the standard inner product in $\mathbf{F}_2^n$.

Let $h_1, \ldots, h_s \in \mathbf{F}_3[\mathbf{F}_2^n]$ with $s \geq \frac{\delta n}{10}$. We have to show that for some $0 \neq f \in \mathbf{F}_3[\mathbf{F}_2^n]$

$$|\frac{1}{s}\sum_{i=1}^{s}\sum_{x\in\mathbf{F}_2^n} e_3(h_i^x \cdot f)| > (1-\delta)2^n \ .$$

For $1 \leq i \leq s$ write the Fourier expansion

$$h_i(y) = \sum_{z\in\mathbf{F}_2^n} a_{iz}(-1)^{z\bullet y}$$

with coefficients $a_{iz} \in \mathbf{F}_3$. There clearly exist $b_1, \ldots, b_s \in \mathbf{F}_3$ and a subset $C \subset \mathbf{F}_2^n$ of cardinality $|C| \geq 3^{-s}2^n$ such that

$$a_{iz} = b_i \quad \text{for all} \quad 1 \leq i \leq s \ , \ z \in C \quad .$$

Let $d = \lceil \log_2(\frac{4}{\delta}) \rceil$. If n is large enough then $3^{-s}2^n \geq 2^{\frac{(2^d-1)n}{2^d}+2}$ hence there exists a $d-$dimensional linear subspace $U \subset \mathbf{F}_2^n$ and a $v \in \mathbf{F}_2^n$ such that $L = v + U \subset C$. Let

$$U^\perp = \{x \in \mathbf{F}_2^n \ : \ x \bullet u = 0 \ \text{ for all } \ u \in U\}$$

and define $f \in \mathbf{F}_3[\mathbf{F}_2^n]$ by

$$f(y) = \begin{cases} (-1)^{y\bullet v} & y \in U^\perp \\ 0 & y \notin U^\perp \end{cases} \ .$$

Then for any $1 \leq i \leq s$ and $x \in \mathbf{F}_2^n$

$$h_i^x \cdot f = \sum_{y\in\mathbf{F}_2^n} h_i(x+y)f(y) = \sum_{y\in U^\perp}(-1)^{v\bullet y}\sum_{z\in\mathbf{F}_2^n} a_{iz}(-1)^{(x+y)\bullet z} =$$

$$\sum_{z\in\mathbf{F}_2^n} a_{iz}(-1)^{x\bullet z}\sum_{y\in U^\perp}(-1)^{y\bullet(v+z)} = 2^{n-d}\sum_{z\in v+U} a_{iz}(-1)^{x\bullet z} =$$

$$2^{n-d}b_i\sum_{z\in v+U}(-1)^{x\bullet z} = 2^n b_i f(x) \ .$$

In particular $h_i^x \cdot f = 0$ for all $x \notin U^\perp$. It follows that

$$| \ \frac{1}{s}\sum_{i=1}^{s}\sum_{x\in\mathbf{F}_2^n} e_3(h_i^x \cdot f) \ | = | \ 2^n - |U^\perp| + \frac{1}{s}\sum_{i=1}^{s}\sum_{x\in U^\perp} e_3(h_i^x \cdot f) \ | \geq$$

$$2^n - 2|U^\perp| = 2^n(1-2^{-d+1}) \geq 2^n(1-\frac{\delta}{2}) \ .$$

$\square$

4 Counting Representations

In this section we prove Theorem 1.4, showing an exponential upper bound on the growth rate of dimensions of irreducible representations in M_ℓ groups. The proof depends on several results which are described below. Let $\mathcal{F}_\ell$ denote the class of finite groups whose compositions factors do not include an alternating group A_k with $k > \ell$.

Proposition 4.1 *There exists a constant c_1 such that if G is an M_ℓ-group then $G \in \mathcal{F}_{c_1\ell}$.*

Proof: By Jordan's Theorem (see [Is76]) for any ℓ there exists a finite $J(\ell)$ such that any finite subgroup $G \subset \mathrm{GL}(\mathbf{C}^\ell)$ contains a normal Abelian subgroup A such that $|G/A| \leq J(\ell)$. Isaacs [Is84] showed that if G is an M_ℓ-group then every non-Abelian composition factor of G has order bounded by $J(\ell)$. Weisfeiler [We84] nearly sharp estimate $J(\ell) \leq \ell^{a \log \ell + b}(\ell+1)!$ implies that for c_1 sufficiently large $J(\ell) \leq \frac{1}{2}(c_1\ell)!$ hence $G \in \mathcal{F}_{c_1\ell}$.

□

Let $a_m(G)$ denote the number of subgroups of G of index at most m. Pyber and Shalev [PS96] proved the following

Theorem 4.2 *([PS96]) There exists a constant c_2 such that for any $G \in \mathcal{F}_\ell$ with a generating set S and any $m \geq 1$*

$$a_m(G) \leq (c_2 \ell^{|S|-1})^m \quad . \qquad \square \tag{8}$$

Let $\|A\| = (\sum_{i,j} |a_{ij}|^2)^{1/2}$ denote the Hilbert-Schmidt norm of a complex matrix $A = (a_{ij})$. The following observation is due to Wassermann [Wa91].

Lemma 4.3 *[Wa91] Suppose ρ_1 , ρ_2 are two irreducible unitary representations of G on $\mathbf{C}^d$. Suppose there exists a non zero matrix $A \in M_d(\mathbf{C})$ such that for all $s \in S$*

$$\|\rho_1(s)A - A\rho_2(s)\| < \tilde{\kappa}_G(S)\|A\| \ .$$

Then $\rho_1 \simeq \rho_2$.

Proof: The tensor product representation $\rho_1 \otimes \rho_2^*$ is realized on a matrix $X \in M_d(\mathbf{C})$ by

$$\rho_1 \otimes \rho_2^*(g)(X) = \rho_1(g) X \rho_2(g)^* \quad .$$

Suppose $\rho_1 \not\simeq \rho_2$ and let χ_i denote the character of ρ_i. Then the multiplicity of the trivial representation in $\rho_1 \otimes \rho_2^*$ is $(\chi_1\chi_2^*, 1) = (\chi_1, \chi_2) = 0$. It follows that

$$\tilde{\kappa}_G(S)\|A\| \le \| \frac{1}{|S|} \sum_{s \in S} \rho_1 \otimes \rho_2^*(s)(A) - A \| \le$$

$$\frac{1}{|S|} \sum_{s \in S} \|\rho_1 \otimes \rho_2^*(s)(A) - A\| = \frac{1}{|S|} \sum_{s \in S} \|\rho_1(s)A - A\rho_2(s)\| \quad .$$

It follows that $\|\rho_1(s)A - A\rho_2(s)\| \ge \tilde{\kappa}_G(S)\|A\|$ for some $s \in S$, a contradiction.

□

Let $U(n) \subset \mathrm{GL}(\mathbf{C}^n)$ denote the unitary group. A simple volume argument shows the following

Lemma 4.4 *There exists a constant c_3 such that $U(n)$ can be covered by at most $(\frac{c_3}{\epsilon})^{2n^2}$ balls of radius $\frac{\epsilon}{2}\sqrt{n}$ in $M_n(\mathbf{C})$.* □

Let H be a subgroup of G of index m and let $\eta : H \to \mathrm{GL}(W)$ be an n-dimensional unitary representation of H. Let $G = \cup_{j=1}^m g_j H$ be a coset decomposition and for $g \in G$ and $1 \le j \le m$ let $\pi(g, g_j)$ be the unique g_k such that $gg_j \in g_k H$ and let $u(g, g_j) = g_k^{-1} g g_j$. Let V denote the $m-$dimensional vector space with basis $g_1, \ldots, g_d$. The induced representation

$$\rho = \mathrm{ind}_H^G \eta : G \to \mathrm{GL}(V \otimes W)$$

is given by

$$\rho(g)(g_j \otimes w) = \pi(g, g_j) \otimes \eta(u(g, g_j))(w) \quad .$$

In particular, if ψ is another $n-$dimensional representation of H then

$$\|\mathrm{ind}_H^G \eta(g) - \mathrm{ind}_H^G \psi(g)\| = (\sum_{j=1}^m \|\eta(u(g, g_j)) - \psi(u(g, g_j))\|^2)^{1/2} \quad .$$

Proof of Theorem 1.4: Let $\rho_1, \ldots, \rho_t$ denote the complex irreducible representations of G of dimension at most d. We show that

$$t \leq \sum_{\{(m,n):mn\leq d\}} (c_2(c_1\ell)^{|S|-1})^m (\frac{c_3}{\tilde{\kappa}_G(S)})^{2n^2m|S|}$$

$$< (\frac{c}{\tilde{\kappa}_G(S)})^{2\ell d|S|} \ . \tag{9}$$

For each $1 \leq i \leq t$ there exists a subgroup $H_i < G$ of index m_i and a unitary representation $\eta_i : H_i \to \mathrm{GL}(\mathbf{C}^{n_i})$ such that $\rho_i = \mathrm{ind}_{H_i}^G \eta_i$, with $m_i n_i \leq d$ and $n_i \leq \ell$ (the later using the assumption that G is an M_ℓ-group). Suppose (9) does not hold. By Proposition 4.1 and Theorem 4.2 there exists a subgroup $H < G$ of index m, an integer n and subset $I \subset [t]$ of cardinality

$$|I| > (\frac{c_3}{\tilde{\kappa}_G(S)})^{2n^2m|S|}$$

such that $H_i = H$ and $n_i = n$ for all $i \in I$. For $i \in I$ let M_i be the $|S| \ltimes m$ array of $n \ltimes n$ unitary matrices given by

$$M_i(s,j) = \eta_i(u(s,g_j))$$

for $s \in S$ and $1 \leq j \leq m$ (we are using the notation introduced above). By Lemma 4.4 and the pigeon hole principle there exist $i \neq i' \in I$ such that

$$\|M_i(s,j) - M_{i'}(s,j)\| < \tilde{\kappa}_G(S)\sqrt{n}$$

for all $s \in S$ and $1 \leq j \leq m$. It follows that for all $s \in S$

$$\|\rho_i(s) - \rho_{i'}(s)\| = \|\mathrm{ind}_H^G \eta_i(s) - \mathrm{ind}_H^G \eta_{i'}(s)\| =$$

$$(\sum_{j=1}^{m} \|M_i(s,j) - M_{i'}(s,j)\|^2)^{1/2} < \tilde{\kappa}_G(S)\ \sqrt{nm} = \tilde{\kappa}_G(S)\|I_{nm}\|$$

. Applying Lemma 4.3 with $A = I_{nm}$ we obtain that $\rho_i \simeq \rho_{i'}$, a contradiction.
Remarks:

1. The bound is nearly sharp: Let $G = C_p \ltimes \mathbf{F}_2[C_p]$ where p is an odd prime and C_p is the cyclic group of order p. G is a monomial group and it can be shown that G has a generating set S of size $O(\log p)$ and $\tilde{\kappa}_G(S) \geq 1/2$. Hence the bound (2) gives $r_p(G) = \exp(O(p\log p))$ while the exact value of $r_p(G)$ is $2p + \frac{2^p-2}{p}$.

2. The monomial case of Theorem 1.4 which is needed for Theorem 1.7 admits a somewhat simpler proof. Proposition 4.1 and Theorem 4.2 can be respectively replaced by Taketa's Theorem on the solvability of monomial groups (see [Is76]) and by Mann's result [Ma96] on the exponential subgroup growth in solvable groups.

Proof of Theorem 1.5 : Note that $r_d(G; \mathbf{F}_p) \leq r_d(G; \overline{\mathbf{F}_p}) = r_d(G)$ for all d. Hence by Theorem 1.4

$$m(G; \mathbf{F}_p) \leq m(G; \mathbf{C}) = O(\ell |S| \log \frac{1}{\tilde{\kappa}_G(S)})$$

and the result follows from Theorem 1.2 .

□

5 Expanders from Group Algebras

Proposition 1.6 is a direct consequence of the following result of Lubotzky and Weiss

Proposition 5.1 *[LW93] Let S be a generating set of G with $\tilde{\kappa}_G(S) \geq \frac{1}{2}$. Then for any subgroup $H < G$*

$$(H : H^{(1)}) \leq (4\pi)^{|S| \cdot (G:H)} \ . \tag{10}$$

□

Proof of Proposition 1.6 : Let $f(k) = (G : G^{(k)})$. Applying (10) with $H = G^{(k)}$ we obtain

$$f(k+1) = f(k) \cdot (G^{(k)} : G^{(k+1)}) \leq f(k) \cdot (4\pi)^{|S| f(k)} \ .$$

Since $f(n) = |G|$, this implies that $|S| = \Omega(\log^{(n)} |G|)$.

□

We now prove Theorem 1.7, which shows that Proposition 1.6 is nearly sharp. We first recall some properties of semi-direct products and their representations (see e.g. [Is76]) . Let H act on the left on an Abelian group N and let $G = H \ltimes N$ be the corresponding semi-direct product. The induced action of H on the character group $\widehat{N}$ is given by $h(\chi)(n) = \chi(h^{-1}(n))$. Let $K < H$ be the stabilizer of some $\chi \in \widehat{N}$, and let $\phi : K \to \mathrm{GL}(W)$ be an irreducible representation of K. Define $\tilde{\phi} : K \ltimes N \to \mathrm{GL}(W)$ by $\tilde{\phi}(kn) = \chi(n)\phi(k)$. Then $\mathrm{ind}_{K \ltimes N}^{G} \tilde{\phi} \in \mathrm{Irr}(G)$ and all $\rho \in \mathrm{Irr}(G)$ arise this way.

Claim 5.2 *If $(|H|, |N|) = 1$ and all subgroups of H are monomial then all subgroups of $G = H \ltimes N$ are monomial.*

Proof: First we prove that any subgroup $G_1 < G$ is conjugate to a subgroup of the form $H_1 \ltimes N_1$, where $H_1 < H$ and $N_1 < N$ is invariant under H_1. Indeed let φ denote the projection from G_1 to H and let $N_2 = \ker \varphi < N$. Clearly $(|N_2|, |G_1/N_2|) = 1$ hence by the Schur-Zassenhaus Theorem (see [Asc00]) there exists an $M < G_1$ such that $M \cap N_2 = \{1\}$ and $MN_2 = G_1$. By Taketa's Theorem H and therefore G are solvable. Since $M < G$ and $(|M|, |N|) = 1$ it follows by P. Hall's Theorem (see [Asc00]) that $gMg^{-1} < H$ for some $g \in G$. Let $H_1 = gMg^{-1}$, $N_1 = gN_2g^{-1}$, then $gG_1g^{-1} = H_1 \ltimes N_1$.

It therefore suffices to show that G itself is monomial. Let $\rho \in \mathrm{Irr}(G)$ then ρ is of the form $\mathrm{ind}_{K \ltimes N}^{G} \tilde{\phi}$ described above. By the monomiality of $K < H$ there exists an $L < K$ and a $1-$dimensional $\psi \in \mathrm{Irr}(L)$ such that $\phi = \mathrm{ind}_{L}^{K}(\psi)$. Let $\tilde{\psi} \in \mathrm{Irr}(L \ltimes N)$ be given by $\tilde{\psi}(ln) = \chi(n)\psi(l)$ then $\tilde{\phi} = \mathrm{ind}_{L \ltimes N}^{K \ltimes N} \tilde{\psi}$ hence $\rho = \mathrm{ind}_{L \ltimes N}^{G} \tilde{\psi}$.

$\square$

Next we describe a special case of the Zig-zag construction of Reingold, Vadhan and Wigderson [RVW00] used in [ALW01]. Let $G = H \ltimes N$ be a semi-direct product. Suppose S is a symmetric generating multiset (which for simplicity we assume contains the identity as well) of H with Kazhdan constant $\tilde{\kappa}_H(S)$, and $A \subset N$ is a symmetric set such that

$$B = \mathrm{Orbit}_H(A) = \cup_{h \in H} h^{-1} A h$$

generates N with Kazhdan constant $\tilde{\kappa}_N(B)$. Let

$$T = SAS = \{ s_1 a s_2 \ : \ s_1, s_2 \in S \ , \ a \in A \ \}.$$

The following theorem, which states that G is expanding if H and N are, is stated here in terms of the Kazhdan constants, while in the references it is stated in terms of the 2nd largest (in absolute value) eigenvalues of the random walk matrix, but the two are identical as explained in section 1.2.

Theorem 5.3 *([RVW00, ALW01]) T generates G and*

$$\tilde{\kappa}_G(T) \geq f(\tilde{\kappa}_H(S), \tilde{\kappa}_N(B))$$

where f is a function which satisfies $f(\lambda,\mu) > 0$ whenever $\lambda,\mu > 0$.

Proof of Theorem 1.7 : Arguing by induction we show that if S_{n-1} is a symmetric generating set of G_{n-1} and $\tilde{\kappa}_{G_{n-1}}(S_{n-1}) \geq 1/2$ then G_n contains a symmetric generating set S_n with $\tilde{\kappa}_{G_n}(S_n) \geq 1/2$ and cardinality $|S_n| \leq O(|S_{n-1}|^c)$ for some constant c to be specified later.

Let $H = G_{n-1}$ and $N = \mathbf{F}_{p_n}[H]$. Repeated applications of Claim 5.2 imply that H is monomial, hence by Theorem 1.5 there exists a symmetric $A \subset N$ such that $|A| = O(\log p_n + |S_{n-1}|)$ and $B = \mathrm{Orbit}_H A$ satisfies $\tilde{\kappa}_N(B) \geq \frac{1}{3}$. Theorem 5.3 then implies that $G_n = H \ltimes N$ contains a generating set T of cardinality $|T| \leq |A||S_{n-1}|^2 = O(|S_{n-1}|^3)$ such that $\tilde{\kappa}_{G_n}(T) \geq f(1/2, 1/3) = \epsilon$.

Let T^c denote (the multiset of) all words of length c in the elements of T. It is easy to check that

$$\tilde{\kappa}_{G_n}(T^c) \geq 1 - (1 - \tilde{\kappa}_{G_n}(T))^c \ .$$

Let $c = \lceil \frac{4}{\epsilon} \rceil$, and set $S_n = T^c$. It follows that $\tilde{\kappa}_{G_n}(S_n) \geq \frac{1}{2}$ and $|S_n| \leq O(|S_{n-1}|^c)$. Starting the process with $S_0 = G_0 = \mathbf{F}_2$ we obtain $|S_n| = \exp(\exp(O(n)))$. Since $|G_n|$ is bigger then the $n-$th iterated exponential it follows that $|S_n| \leq \log^{(n-\log^* n)} |G_n|$ for large enough n.

$\square$

6 Explicit Construction of Expanding Orbits

Proof of Theorem 1.8: The members of G are all functions $ax + b$ with $a, b \in \mathbf{F}_p$, $a \neq 0$, acting on the coordinates $x \in \mathbf{F}_p$. Let χ_T be the character associated with a set $T \in \mathbf{F}_p$. Similarly, identify each vector in S with the set of 1's in it. We want to prove that for every $T \neq \emptyset$ we have

$$\sum_{A \in S} (-1)^{|A \cap T|} \leq .99 \cdot 2|G|$$

Clearly, it suffices if either one of the following two hold:

$$(i) \ \sum_{A \in Gv} (-1)^{|A \cap T|} \leq .98 \cdot |G|$$

$$(ii) \quad \sum_{A \in Gu} (-1)^{|A \cap T|} \leq .98 \cdot |G|$$

Since v is a singleton vector, condition (i) is satisfied for every T that is not too small or large, namely $\frac{p}{100} \leq |T| \leq \frac{99p}{100}$. But note that since the support of u is even, condition (ii) is the same for T and $\bar{T}$. Thus proving that condition (ii) holds for all small sets $|T| \leq p/100$ will complete the proof.

Let us rewrite condition (ii) as

$$(ii) \quad \sum_{a,b} (-1)^{|I \cap aT+b|} \leq .98|G|$$

Let us give some intuition first. The key to the proof will be that the functions in G are good hash functions, and thus well disperse the elements of any small set T. The dispersion means that most elements of the set aT for a random a are "isolated". We say that an element $y \in aT$ is $c-isolated$ if there are no other elements from aT in the intervals of length $c/2$ centered at y and $y + (p-1)/2$. Note that if y is isolated, the shifts $y + b$ near the edges of the interval I will cause a cancellation of c in the sum above (the change in parity of the intersection with I in these values of b depends solely on whether y is in I or not, which happens exactly half the time. Choosing $c = \Omega(p/|T|)$, and making sure that the above happens for most elements of aT, for most choices of a will complete the proof.

We will omit floor and ceiling notation, since rounding does not affect the calculations in any significant way.

Let $t = |T|$ and let $c = p/100t$. Denote by I_0 the union of two intervals $[1, c/2] \cup [(p-1)/2+1, (p-1+c)/2]$. For $0 \leq j \leq (p-1/c-1$ let $I_j = I_0 + jc/2$. Note that the $k = (p-1)/c$ sets I_j are form a partition $\mathbf{F}_p$ (except 0) into equal size parts. Assume for simplicity that $0 \notin T$. Thus the random mapping $x \to I(ax)$ which maps $x \in \mathbf{F}_p^*$ to $j \in [k]$ if $ax \in I_j$ is a nearly 2-universal mapping (see [CW79]), namely we have for a random $0 \neq a \in \mathbf{F}_p$ both $Pr_a[I(ax) = j] = 1/k$ for every x, j and for $x' \neq x$ $Pr_a[I(ax) = I(ax')] \leq \frac{3k}{2}$.

For a fixed a, let BAD_a contain all $x \in T$ which is not alone in its interval, namely for some other x' we have $I(ax) = I(ax')$. Similar to [FKS84] we can upper bound the expectation $E_a[|BAD_a|$ by twice the number of colliding pairs x, x', which is at most $\frac{3t^2}{2k} \leq t/50$.

By Markov's inequality, the fraction of a's for which $|BAD_a| > t/10$ is at most $3/20$. An identical argument shows that if we define new (shifted by

$c/4$) intervals, $I'_j = I_j + c/4$, at most $3/20$ of the a's will have the analogous $|BAD'_a| > t/10$. But note that an element x which is neither in BAD_a nor in BAD'_a satisfied that ax is c-isolated. So we have just proved that for each of .7 of all a's, at least .8 of all x satisfy that ax are c-isolated. This yield a bound of .1 on the expression (ii), which concludes the proof.

Acknowledgements

We are grateful to Pierre Deligne, Alex Lubotzky and Peter Sarnak for insightful discussions. This research was partially supported by NSF grant number CCR-9987845.

References

[A86] N. Alon, Eigenvalues and expanders, *Combinatorica* 6(1986), 83-96.

[AM84] N. Alon and V.D. Milman, Eigenvalues, expanders and superconcentrators, Proc. 25^{th} Annual Symp. on Foundations of Computer Science (FOCS), Singer Island, Florida, IEEE(1984), pp. 320-322. Also: λ_1, Isoperimetric Inequalities for Graphs and Superconcentrators, *J. Combinatorial Theory Ser. B* 38 (1985), pp. 73-88.

[ALW01] N. Alon, A. Lubotzky and A. Wigderson, Semi-direct product in groups and Zig-zag product in graphs: connections and applications. Proc. of the 42nd FOCS, 2001.

[Asc00] M. Aschbacher, *Finite group theory*, Cambridge University Press, Cambridge, 2000.

[BB82] T. C. Brown and J. P. Buhler, A density version of a geometric Ramsey theorem, *J. Combin. Theory Ser. A* **32**(1982) 20-34.

[CW79] L. Carter and M. Wegman, Universal Classes of Hash Functions, *J. Computer and System Sciences* **18**(1979) 143-154.

[GG81] O. Gabber and Z. Galil, Explicit Construction of Linear Sized Superconcentrators, *J. Comp. and Sys. Sci* 22 (1981), pp. 407-420.

[HRV93] P. de la Harpe, A. G. Robertson and A. Valette, On the spectrum of the sum of generators for a finitely generated group, *Israel J. of Math.* **81**(1993) 65-96.

[FKS84] M. Fredman and J. Komlós and E. Szemerédi, Storing a Sparse Table with O(1) Worst Case Access Time, *Journal of the ACM* **31**(1984) 538-544.

[Is76] I.M. Isaacs, *Character Theory of Finite Groups*, Academic Press 1976.

[Is84] I.M. Isaacs, Generalizations of Taketa's theorem on the solvability of M-groups, *Proc. Amer. Math. Soc.* **91**(1984) 192-194.

[LPS88] A. Lubotzky, R. Philips, P. Sarnak, Ramanujan Graphs, *Combinatorica* 8 (1988), 261-277.

[L94] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Progress in Math. 125, Birkhaüser Verlag, Basel 1994.

[LW93] A. Lubotzky, B. Weiss, Groups and expanders, in: *Expanding Graphs* (ed. J. Friedman), DIMACS Ser. Discrete Math. Theoret. Compt. Sci. 10 pp. 95–109, Amer. Math. Soc., Providence, RI 1993.

[Ma96] A. Mann, Positively finitely generated groups, *Forum Math.* **8**(1996) 429-469.

[Mar73] G.A. Margulis, Explicit Construction of Concentrators, *Problems of Inform. Transmission* (1973) 325-332.

[Mar88] G. A. Margulis, Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and superconcentrators, Problems of Information Transmission 24(1988) 39-46.

[PS96] L. Pyber and A. Shalev, Groups with super-exponential subgroup growth, *Combinatorica* **16**(1996) 527-533.

[RVW00] O. Reingold, S. Vadhan and A. Wigderson, Entropy waves, the zig-zag grpah product, and a new constant-degree expanders and extractors, *Proc. of the 41st FOCS* (2000), pp. 3–13.

[Tan84] R.M. Tanner, Explicit Construction of Concentrators from Generalized N-gons, *SIAM J. Alg. Discr. Meth.* 5 (1984) 287-293.

[Wa91] S. Wassermann, C^*-algebras associated with groups with Kazhdan's property T, *Ann. Math.* **134**(1991) 423-431.

[We84] B. Weisfeiler, Post-classification of Jordan's theorem on finite linear groups, *Proc. Nt. Acad. Sci. U.S.A* **81**(1984) 5278-5279.