Finite Simple Groups as Expanders

Martin Kassabov
Department of Math
Cornell University
Ithaca, NY 14853
USA.

Alexander Lubotzky*
Institute of Mathematics
Hebrew University
Jerusalem, 91904
Israel.

Nikolay Nikolov
New College
Oxford, OX1 3BN
UK.

Abstract

We prove that there exist $k \in \mathbb{N}$ and $0 < \varepsilon \in \mathbb{R}$ such that every non-abelian finite simple group G, which is not a Suzuki group, has a set of k generators for which the Cayley graph $\mathrm{Cay}(G; S)$ is an ε-expander.

Introduction

Let X be a finite graph and $0 < \varepsilon \in \mathbb{R}$. The graph X is called an ε-expander graph if for every subset A of the vertices of X with $|A| \leq \frac{1}{2}|X|, |\partial A| \geq \varepsilon |A|$, where ∂A denotes the boundary of A, i.e., the vertices of distance 1 from A.

Expander graphs play an important role in computer science and combinatorics and many efforts has been dedicated to their constructions (cf. [12],the references therein and [18]). Many of these constructions are of Cayley graphs and in particular various families of finite simple groups were shown to be expanding families.

We will say that a family $\mathfrak{G}$ of groups is a family of expanders (uniformly), if there exists $k \in \mathbb{N}$ and $0 < \varepsilon \in \mathbb{R}$ such that every group $G \in \mathfrak{G}$, has a subset S of k generators for which $\mathrm{Cay}(G; S)$ is an ε-expander. Until recently all such families were of bounded Lie rank (cf. [12, 21]), a fact which has raised the speculation that this is the only possibility (see [15] and [9]).

It is easy to see that expander graphs have logarithmic diameter. In [1] it was shown that every non-abelian finite simple group has a set S of 7 generators for which the Cayley graph $\mathrm{Cay}(G; S)$ has a diameter bounded by $C \log(|G|)$ for an absolute constant C. It was conjectured there that one can even make all finite simple groups expanders in a uniform way although, as observed by Y. Luz (see [15]), the generators used in [1] do not give rise to expanders.

The main goal of this note is to announce an almost complete proof of this conjecture:

*Supported by NSF and BSF (US–Israel). This work was done while visiting the IAS in Princeton, supported by the Ambrose Monell Foundation and The Ellentuck Fund.

Theorem 1 *There exist $k \in \mathbb{N}$ and $0 < \varepsilon \in \mathbb{R}$ such that every non-abelian finite simple group G, which is not a Suzuki group, has a set S of k generators for which $\mathrm{Cay}(G;S)$ is an ε-expander. Moreover the constants k and ε can be estimated.*

We believe that the above theorem holds also for the Suzuki groups but our (diverse) methods do not apply to them. What makes them exceptional is the fact that they do not contain copies of $\mathrm{SL}_2(\mathbb{F}_p)$ or $\mathrm{PSL}_2(\mathbb{F}_p)$ like essentially all the other finite simple groups (see below for more details).

The proof of the Theorem is the accumulation of the works [7, 6, 5, 17] and [11] in the following chronological order:
In [7] it was proved, extending the work of Shalom [21], that for $d \geq 3$ and $k \geq 0$ the group $\mathrm{SL}_d(\mathbb{Z}[x_1, \ldots, x_k])$ has property (τ), i.e., its finite quotients are expanders. It was then further shown in [6] that if $R = \mathbb{Z}\langle x_1, \ldots, x_k\rangle$ is the free non-commutative ring then suitable finite quotients of $\mathrm{EL}_d(R)$ are also expanders uniformly (where $\mathrm{EL}_d(R)$ denotes the subgroup of the multiplicative group of $\mathrm{Mat}_d(R)$ generated by the elementary matrices). This includes, in particular, the groups $\mathrm{EL}_3(\mathrm{Mat}_n(\mathbb{F}_q)) \simeq \mathrm{SL}_{3n}(\mathbb{F}_q)$ and thus $\mathrm{SL}_{3n}(\mathbb{F}_q)$ are uniformly expanders for all n and for all prime powers q. For every $d \geq 3$, the group $\mathrm{SL}_d(\mathbb{F}_q)$ is a bounded product of copies of $\mathrm{SL}_{3n}(\mathbb{F}_q)$ for $n = \lfloor d/3 \rfloor$, which implies that the family of groups $\{\mathrm{SL}_d(\mathbb{F}_q) \mid d \geq 3, q \text{ prime power}\}$ form a family of expanders.

It was then shown in [17] that every finite simple classical group of Lie type is a bounded product of copies of $\mathrm{SL}_d(\mathbb{F}_q)$ and its central quotients. This can be combined with the previous results to yield that all classical groups of Lie type of sufficiently high rank are expanders.

The alternating groups $\mathrm{Alt}(n)$ for $n \geq 5$ are also expanders in a uniform way. This is proved in [5]. The argument here is more involved since $\mathrm{Alt}(n)$ contains copies of $\mathrm{SL}_d(\mathbb{F}_q)$ but it is not boundedly generated by such groups. The proof, therefore, goes by decomposing the regular representation of $\mathrm{Alt}(n)$ into two components - on the first $\mathrm{Alt}(n)$ acts "like" it is bounded generated by some copies of powers of $\mathrm{SL}_d(\mathbb{F}_q)$ and on the second component the eigenvalues estimates of [19] are applied (for details, see §6 below). This method is influenced by the work of Roichman [20]. We are using here the well known representation-theoretic reformulation of the expanding property - see §1.

On the other hand it is shown in [11] that the family $\mathrm{SL}_2(\mathbb{F}_q)$, q a prime power, is also a family of expanders. This is proved by a combination of Selberg's Theorem (cf. [12, §4]) with the *explicit* construction of Ramanujan graphs as given in [13]. In fact, a more careful analysis there can also give the general result for the family $\mathrm{SL}_d(\mathbb{F}_q)$ for all $d \geq 2$ and all prime powers q together, using the theory of Ramanujan complexes (cf. [14]) and their explicit construction in [13].
The case of $\mathrm{SL}_2(\mathbb{F}_q)$ is the crucial new case of [11]. It is further shown there, using some model theoretic results of Hrushovski and Pillay [4], that for a fixed r, all finite simple groups of Lie type and of rank at most r, with the

exception of the Suzuki groups, are bounded products of copies of $\mathrm{SL}_2(\mathbb{F}_q)$'s. One therefore deduces that the groups of Lie type and rank $\leq r$ are expanders uniformly. This exactly complements the results of [6] and [17] and all together gives that all finite simple groups of Lie type, with the possible exception of the Suzuki groups, are expanders uniformly.

By the classification of the finite simple groups (CFSG) every (non-abelian) finite simple group is either alternating or of Lie type or one of finitely many sporadic groups. Thus Theorem 1 follows from the works described above.

The layout of the current note would not follow the chronological story. We recall and make in §1 some observations regarding the representation theoretic reformulation of the problem. In §2 we describe the proof for SL_2, while sections 3 and 4 give two proofs for the case of $\mathrm{SL}_d, (d \geq 3)$ first via Ramanujan's complexes and second via $\mathrm{EL}_3(\mathbb{Z}\langle x_1, \ldots, x_k\rangle)$. In section 5 we use the results for $\mathrm{SL}_d(\mathbb{F}_q)$ to construct expanding generating sets in all simple groups of Lie type (with the exception of the Suzuki groups). In §6 we describe the proof for $\mathrm{Alt}(n)$, or equivalently for $\mathrm{Sym}(n)$ - the symmetric groups, which is a case of great special interest.

1 A representation theoretic interpretation

As is well known (cf. [12] and references therein) the expanding property of $\mathrm{Cay}(G; S)$ is equivalent to representation theoretic properties. The one which will be most convenient for us to use is:

Proposition 2 *A family $\mathrm{Cay}(G_i; S_i)$ of Cayley graphs are ε-expanders for some $\varepsilon > 0$ iff there exist $0 < \alpha \in \mathbb{R}$ such that the following holds:*

For every $i \in \mathbb{N}$, every unitary representation (V, φ) of G_i, every $0 \neq v \in V$ and every $0 < \delta \in \mathbb{R}$, if $|\varphi(s)v - v| < \delta$ for each $s \in S$, then $|\varphi(g)v - v| < \alpha\delta$ for each $g \in G$.

(i.e., a vector v which is "S-almost invariant" is also "G-almost invariant".)

Another interpretation is via the normalized adjacency matrix of the graph $X = \mathrm{Cay}(G; S)$: Let $k = |S \cup S^{-1}|$ and $\Delta = \frac{1}{k}A$ where A is the adjacency matrix of X. Then all the eigenvalues of Δ are in $[-1, 1]$. The second to largest eigenvalue will be denoted $\lambda(X)$ and we have:

Proposition 3 *A family $X_i = \mathrm{Cay}(G_i; S_i)$ is a family of ε-expanders for some $\varepsilon > 0$ if $\lambda(X_i) < 1 - \delta$ for some $\delta > 0$ and for all i.*

Note that in Proposition 3 we do not assume that the sets S_i are of bounded size. If S_i are bounded then the converse is also true.

Finally, we will make the following observations which will be used several times: If S_1 is a "bounded product" of a set S_2 i.e., every element of S_1 is a product of a bounded number of elements of S_2, then an S_2-almost invariant vector is also S_1-almost invariant. This implies for example that if G is a bounded product of a bounded number of subgroups $H_1, H_2, \ldots, H_\ell$ and each H_i is an expander (w.r.t. some set of generators S_i) then G is an expander w.r.t. their union $S = \cup S_i$.

In addition, if H_i are expanders with respect to some generating sets S_i, and each H_i is embedded in a group G, which is an exapnder w.r.t. the union $\cup H_i$ then G is also an expander w.r.t. to $\cup S_i$.

2 The $\mathrm{SL}_2(\mathbb{F}_{p^k})$ case

In this section we will show, following [11], that $\mathrm{PSL}_2(q)$ can be made into expanders uniformly for every prime power $q = p^\alpha$.

It is known that:

2.1. The family of groups $\mathrm{SL}_2(\mathbb{F}_p)$, p prime, with respect to the generators $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ form a family of expanders. For a proof, based on Selberg's theorem $\lambda_1 \geq \frac{3}{16}$, see [12, §4].

2.2. For a fixed prime p, the groups $\mathrm{SL}_2(\mathbb{F}_{p^k})$, $k \in \mathbb{N}$, have a subset S_p of $p+1$ generators for which the Cayley groups $X = \mathrm{Cay}(SL_2(p^k); S_p)$ are Ramanujan graphs, i.e., $\lambda(X) \leq \frac{2\sqrt{p}}{p+1}$. This means, in particular, that they form a family of expanders with a common expanding factor $\varepsilon > 0$, even if we let both p and k vary. The problem is that the number of generates is unbounded when $p \to \infty$.

The result of 2.2 was first proved by Morgenstern [16], and it relies on the Drinfeld's solution to the characteristic p Ramanujan conjecture for GL_2. However, for our purpose we need the explicit construction of Ramanujan graphs (as special cases of Ramanujan complexes) as given in [13]. In the construction there, a symmetric set of $p+1$ generators S'_p for $\mathrm{SL}_2(\mathbb{F}_{p^k})$ is given as the $p+1$ conjugates of a fixed element C by a non-split torus H of $\mathrm{SL}_2(\mathbb{F}_p)$, i.e., $S'_p = \{h^{-1}C^{\pm 1}h \mid h \in H\}$. Now,

$$\lambda(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_{p^k}); S'_p)) \leq \frac{2\sqrt{p}}{p+1} < \frac{19}{20}$$

therefore these graphs are expanders by Proposition 3 uniformly for all p and all k.

At the same time $\mathrm{Cay}(SL_2(p); \{A, B\})$ are expanders by 2.1. Altogether this implies that $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_{p^k}); \{A, B, C\})$ are expanders. Indeed, if (V, φ) is a representative of $G = \mathrm{SL}_2(\mathbb{F}_{p^k})$ and $v \in V$ is S-almost invariant for the set $S = \{A, B, C\}$, then v is $\mathrm{SL}_2(\mathbb{F}_p)$-almost invariant and hence is also S'_p-almost invariant, because $S'_p \subset \mathrm{SL}_2(\mathbb{F}_p) \cdot C \cdot \mathrm{SL}_2(\mathbb{F}_p)$, and hence G-almost invariant.

This shows that $\mathrm{SL}_2(\mathbb{F}_{p^k})$ are uniformly expanders with 3 generators.

3 $\mathrm{SL}_d(\mathbb{F}_{p^k})$ via Ramanujan complexes

One can generalize the proof for SL_2 described in §2 to SL_d for every d. We sketch the proof below – for full details see [11].

Let $F = \mathbb{F}_q$ be the field of order $q = p^k$, for some prime p. Let $E = \mathbb{F}_{q^d}$ be the unique field extension of degree d. The natural map $E^* \to \mathrm{GL}_d(\mathbb{F}_q)$ given by letting E^* act on E by multiplication, induces an isomorphism of

$$\{x \in E^* \mid \mathrm{Norm}_{E/F}(x) = 1\} \text{ onto } H \leq \mathrm{SL}_d(\mathbb{F}_q),$$

where H is a non-split maximal torus of order $\frac{q^d-1}{q-1}$. In [13] it was shown that for a suitable choice of $D \in \mathrm{SL}_d(\mathbb{F}_q)$, the Caley graphs $\mathrm{Cay}(\mathrm{SL}_d(\mathbb{F}_q); S')$ are expanders when $S' = \{h^{-1}Dh \mid h \in H\}$. What is really proved there is that the adjacency operator of this Cayley graph is the sum of the first and the last of the $d-1$ Hecke operators on the Cayley complex $\mathrm{SL}_d(\mathbb{F}_q)$, which is a Ramanujan complex, see [14]. The eigenvalue bound on these Hecke operators implies that

$$\lambda(\mathrm{Cay}(\mathrm{SL}_d(\mathbb{F}_q); S')) \leq \frac{2dq^{(d-1)/2}}{(q^d-1)/(q-1)}$$

and in particular these are expanders.

We mention that the proof here (when $d \geq 3$) does not need the full power of the Ramanujan bound. A weaker bound

$$\lambda(\mathrm{Cay}(\mathrm{SL}_d(\mathbb{F}_q); S')) \leq \frac{1}{\sqrt{q}} + o(1) \leq \frac{19}{20}$$

which is sufficient for out purposes, can be deduced from the infinite dimensional representation theory of the group $\mathrm{SL}_d(\mathbb{F}_q((t)))$.

Assume now that d is even, $d = 2m$. Then the map $E^* \hookrightarrow \mathrm{GL}_d(\mathbb{F}_q)$ described above factors through:

$$E^* = \mathbb{F}^*_{q^{2m}} \hookrightarrow \mathrm{GL}_2(q^m) \hookrightarrow \mathrm{GL}_{2m}(q) = GL_d(q),$$

which shows that $H \leq \mathrm{SL}_d(\mathbb{F}_q)$ is contained in a copy of $\mathrm{SL}_2(\mathbb{F}_{q^m})$.

Take now the expanding generating set $\{A, B, C\}$ of $\mathrm{SL}_2(\mathbb{F}_{q^m})$ from § 2 with D to construct a 4 generator set for $\mathrm{SL}_d(\mathbb{F}_q)$.

We claim that $\mathrm{SL}_d(\mathbb{F}_q)$ are expanders w.r.t. these 4 generators. Indeed, again an $S = \{A, B, C, D\}$-almost invariant vector is $\mathrm{SL}_2(\mathbb{F}_q)$-almost invariant and then it is $H \cdot D \cdot H$-almost invariant hence also S'-almost invariant and thus $G = \mathrm{SL}_d(\mathbb{F}_q)$-almost invariant as required.

This covers the case of even d. For odd d, the group $\mathrm{SL}_d(\mathbb{F}_q)$ is a product of 5 copies of $\mathrm{SL}_{d-1}(\mathbb{F}_q)$ and hence it is also an expander.

4 $\mathrm{SL}_d(\mathbb{F}_{p^k})$ for $(d \geq 3)$ via $\mathrm{EL}_3(R)$

A different proof for the case of SL_d has been given in [6] (prior to the proof in [11], which is described in §3.) This proof borrows ideas from the work of Shalom [21], where he gave a new proof of Kazhdan's result [8] that $\mathrm{SL}_3(\mathbb{Z})$ has property (T). Shalom's proof has two ingredients:

4.1. The group $\Lambda = \mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ has a relative Kazhdan property (T) relative to $\mathbb{Z}^2$, i.e., if (V, φ) is a unitary representation space of Λ with almost invariant vector, w.r.t. a fixed set of generators, then this vector is $\mathbb{Z}^2$-almost invariant.

4.2. The group Λ has several obvious embeddings into $\mathrm{SL}_3(\mathbb{Z})$. The copies of $\mathbb{Z}^2$ in these embeddings (which include the root subgroups) boundedly generate[1] $\mathrm{SL}_3(\mathbb{Z})$ by a result of Carter and Keller [2].

Parts 4.1 and 4.2 together imply that if V is a unitary representation of $\Gamma = \mathrm{SL}_3(\mathbb{Z})$ and $v \in V$ is an almost invariant vector (w.r.t. some generating set) it will be Γ-almost invariant and therefore the group Γ has property (T).

A similar argument to 4.1 works also for $\Lambda = \mathrm{SL}_2(R_0) \ltimes R_0^2$, when R_0 is the polynomial ring in k variables over $\mathbb{Z}$. However, it is not known if the bounded generation of 4.2 holds in this case, which would imply that $\mathrm{SL}_3(R_0)$ has property (T). Still, by analyzing the congruence kernel of $\mathrm{SL}_3(R_0)$, it is deduced in [7] that $\Gamma = \mathrm{SL}_3(R_0)$ has property (τ), i.e. all of its finite factors are expanders (w.r.t. a fixed set of generators of Γ).

A step further is taken in [6]: it is shown there that part 4.1 holds even if one takes the non-commutative free ring $R = \mathbb{Z}\langle x_1, \ldots, x_k \rangle$, i.e., $\Lambda = R^2 \times \mathrm{EL}_2(R)$ has the property (T) relative to R^2. It will be quite surprising if $\Gamma = \mathrm{EL}_3(R)$ is boundedly generated by images of R^2 under different embedding of Λ in Γ, however this holds uniformly for many quotients $\overline{R}$ of R, probably even for all finite quotients. For example if $\overline{R} = \mathrm{Mat}_n(\mathbb{F}_q)$ or $\overline{R} = \mathrm{Mat}_n(\mathbb{F}_q)^{\times s}$ for $s \leq q^{n^2}$, then $\overline{R}$ is an image of $\mathbb{Z}\langle x_1, x_2, x_3 \rangle$ and $\mathrm{EL}_3(\overline{R})$ is boundedly generated by its elementary matrices in a way which is independent of n, q and s. All this implies that the groups $\mathrm{EL}_3(\mathrm{Mat}_n(\mathbb{F}_q)) = \mathrm{SL}_{3n}(\mathbb{F}_q)$ and $\mathrm{EL}_3(\mathrm{Mat}_n(\mathbb{F}_q)^{\times s}) = \mathrm{SL}_{3n}(\mathbb{F}_q)^{\times s}$ are expanders uniformly.

For a general $d \geq 3$, one notes again that $\mathrm{SL}_d(\mathbb{F}_q)$ is a bounded product of a bounded number of copies of $\mathrm{SL}_{3n}(\mathbb{F}_q)$ for $n = \lfloor d/3 \rfloor$. We can therefore deduce that $\mathrm{SL}_d(\mathbb{F}_q)$ are expanders for all $d \geq 3$ and every prime power q.

One of the advantages of this construction is that it also produces expanders in very large powers of the group $\mathrm{SL}_d(\mathbb{F}_q)$, which are essential for constructing expanding generating sets in the alternating groups, see §6.

[1] For our purposes it is sufficient that the quotient groups $\mathrm{SL}_3(\mathbb{F}_p)$ are uniformly boundedly generated by the elementary matrices. This result follows easily from the standard row and column reduction algorithm for matrices.

5 Simple groups of Lie type

The following two theorems show how to deduce the (almost) general case of finite simple groups of Lie type from the case of $\mathrm{SL}_d(\mathbb{F}_q)$ described in §2–§4.

Theorem 4 ([17]) *There exists a constant C such that every finite simple group G of classical type is a product of length at most C of at most C subgroups of G which are quotients of $\mathrm{SL}_d(\mathbb{F}_q)$ (for some $d \geq 2$ and q).*

Theorem 5 ([11]) *Given $r \in \mathbb{N}$, there exists a constant $C(r)$ with the following property: Suppose G is a finite simple group of Lie type of Lie rank at most r, which is not a Suzuki group. Then G is a product of length at most $C(r)$ of some $C(r)$ subgroups of G which are all quotients of $\mathrm{SL}_2(\mathbb{F}_q)$ for some q's.*

As explained in §1, once a group G is a product of boundedly many expander groups, it is also an expander. So Theorem 1 is now proved for all groups of Lie type except for the Suzuki groups. The reason for the Suzuki groups to be excluded is the fact that they do not contain copies of $\mathrm{SL}_d(\mathbb{F}_q)$ or $\mathrm{PSL}_d(\mathbb{F}_q)$ for any $d \geq 2$ and prime power q. In fact, the order of a Suzuki group is not divisible by 3 while $|\mathrm{SL}_d(\mathbb{F}_q)|$ is.

The proof of Theorem 4 is by a detailed analysis of the subgroup structure of simple groups of Lie type:

The essential point is that arbitrary connected Dynkin diagram becomes one of type A_d after a few vertices are deleted. In this way we can find a quasisimple quotient G_1 of $\mathrm{SL}_{d+1}(\mathbb{F}_q)$ inside G (in fact it is a Levi factor of a suitable parabolic subgroup).

If U (resp. U_1) is a suitable unipotent subgroup of G (resp G_1) then [17] proves that U is a product of at most 14 conjugates of U_1. (using that the positive root system of G parameterizing U is "close" to the root system A_d of U_1.) A theorem of M. Liebeck and L. Pyber in [10] now gives that G is a product of at most 13 conjugates of U and hence a product of at most $13 \times 14 = 182$ conjugates of G_1.

A very detailed and laborious analysis of this kind will also lead to a similar proof of Theorem 5 with explicit bounds for $C(r)$ but this is not the way this theorem is proved in [11].

Instead, the author there appeals to a model theoretic method developed by Hrushovski and Pillay [4]. There it is shown that "definable" subgroups of $\mathrm{GL}_n(F)$ over pseudo-algebraically closed field F are very much like Zariski closed subgroups over algebraically closed field. In particular, if a definable subgroup H is generated by finitely many definable subgroups $L_1, \ldots, L_c$ then it is a bounded product of them. Now, it follows from the Lang-Weil Theorem that ultra-products of finite fields are pseudo-algebraically closed (see [3]). As elementary statements are true in an ultra product iff they are true in almost all factors – one can get "bounded results" over finite fields. This scheme is applied to show that all the finite simple groups (except the Suzuki groups) contain "definable" subgroups isomorphic to $\mathrm{SL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$ and hence are generated by them in a bounded way (when the rank is bounded).

6 The Alternating groups

Last but not least is the case of the alternating groups $\mathrm{Alt}(n)$ or equivalently the symmetric groups $\mathrm{Sym}(n)$. For its special importance, we restate it:

Theorem 6 ([5]) *There exist $k \in \mathbb{N}$ and $0 < \varepsilon \in \mathbb{R}$ such that for every $n \in \mathbb{N}$ the symmetric group $\mathrm{Sym}(n)$ has an explicit set of generators S_n of size at most k such that $\mathrm{Cay}(\mathrm{Sym}(n); S_n)$ is an ε-expander.*

The main idea of the proof in [5] is as follows: Let first consider the alternating groups $\mathrm{Alt}(n)$. Assume first that $n = d^6$ and $d = 2^{3k} - 1$ for some k. Based on ideas and results from [6] (see §4 above) it is shown first that the Cayley graphs of the groups $\Delta_k = \mathrm{SL}_{3k}(\mathbb{F}_2)^{d^5}$ with respect to some generating set F_k of size at most 20 are expanders for all k and $d = 2^{3k} - 1$.

Now, thinking of the set $\{1, \dots, n\}$ as the points in a 6-dimensional cube of size d, and remembering that $\mathrm{SL}_{3k}(\mathbb{F}_2)$ acts transitively on a set of size d (via its defining linear action on $\mathbb{F}_2^{3k}$), we can construct 6 different embeddings π_i of Δ_k into $\mathrm{Alt}(n)$, where the image under π_i of each copy of $\mathrm{SL}_{3k}(\mathbb{F}_2)$ in Δ_k acts on the points on a line parallel to the i-th coordinate axis in the cube. Denote $S_n = \cup_i \pi_i(F_k)$ and $E = \cup_i \pi_i(\Delta_k)$. We will show that the Cayley graphs of $\mathrm{Alt}(n)$ with respect to S_n form a family of expanders. Using that F_k is an expanding generating set in Δ_k it suffices to show that the existence of E-almost invariant vector v in any unitary representation V of $\mathrm{Alt}(n)$ implies the existence of an invariant vector.

We decompose V as a sum of two representations $V_1 \oplus V_2$, where V_1 is the sum of all irreducible representations of $\mathrm{Alt}(n)$ in V corresponding to partitions $\lambda \vdash n$, where the first row λ_1 is small (less than $n - d^{5/4}$) and V_2 contains all others. A similar decomposition is used by Roichman in [20] to show that the Cayley graphs of $\mathrm{Alt}(n)$ with respect to conjugacy classes have some expanding properties. We will use two different arguments to show that the projection v_1 of v in V_1 is small and that projection v_2 in V_2 is close to an invariant vector:

6.1. Using the definition of the set E, it is shown that a bounded power of E acts transitively on "nearly all" ordered ℓ-tuples of points in the cube for some ℓ of size approximately $d^5/(3\log d)$. Also a bounded power of E contains a permutation which acts as ℓ-cycle. Thus the vector v, and therefore v_1, is almost invariant by "nearly all" elements in the conjugacy class C_ℓ of ℓ-cycles in $\mathrm{Alt}(n)$. Here "nearly all" means a subset of proportion tending to 1, as k and n tend to infinity. This implies that v_1 is almost invariant under the action of the operator

$$L = \frac{1}{|C_\ell|} \sum_{s \in C_\ell} s.$$

The operator L acts as a multiplication by $\chi_\lambda(C_\ell)/\chi_\lambda(id)$ on the irreducible representation V_λ corresponding to the partition λ, where χ_λ is the character of V_λ. At this point one can appeal to methods and results of Roichman [19], who studied normalized character values of the symmetric groups. Roichman's results gives that $|\chi_\lambda(C_\ell)/\chi_\lambda(id)| \ll 1$, for any $\lambda \vdash n$, provided that the first row λ_1 is small. Therefore $||Lv_1|| \ll ||v_1||$, which together with the almost invariance of v_1 under L, implies that the vector v_1 is short.

6.2. Using that all irreducible representations in V_2 corresponds to partitions with $\lambda_1 \geq n - d^{5/4}$, one can view the linear span W of the orbit of v_2 in V_2 as part of the induced representation to $\mathrm{Alt}(n)$ of the trivial representation of $\mathrm{Alt}(n - d^{5/4})$. This induced representation has a basis $\mathfrak{B}$, whose elements corresponds to the ordered $d^{5/4}$-tuples of points in the cube. The size of the basis $\mathfrak{B}$ is significantly smaller that the size of E and it can be shown that the random walk on $\mathfrak{B}$ defined by E mixes in just several steps. This together with the almost invariance of v_2 under E, implies that v_2 is close to an invariant vector.

This finishes the sketch of the proof for the case $\mathrm{Alt}(n)$ for $n = (2^{3k} - 1)^6$ for some k. The case of general n follows from the observation that $\mathrm{Alt}(n)$ can be written as a product of a bounded number of copies of $\mathrm{Alt}(n_k)$ for $n_k = (2^{3k}-1)^6$ embedded in $\mathrm{Alt}(n)$. Finally, any expanding generating set of $\mathrm{Alt}(n)$ gives an expanding generating set in $\mathrm{Sym}(n)$ by adjoining one odd permutation.

References

[1] L. Babai, W. M. Kantor, and A. Lubotzky, *Small-diameter Cayley graphs for finite simple groups*, European J. Combin. **10** (1989), no. 6, 507–522. MR1022771 (91a:20038)

[2] David Carter and Gordon Keller, *Bounded elementary generation of* $\mathrm{SL}_n(\mathcal{O})$, Amer. J. Math. **105** (1983), no. 3, 673–687. MR704220 (85f:11083)

[3] Michael D. Fried and Moshe Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2005. MR2102046 (2005k:12003)

[4] E. Hrushovski and A. Pillay, *Definable subgroups of algebraic groups over finite fields*, J. Reine Angew. Math. **462** (1995), 69–91. MR1329903 (97f:20059)

[5] Martin Kassabov, *Symmetric Groups and Expander Graphs*, `arXiv:math.GR/0505624`.

[6] ———, *Universal lattices and unbounded rank expanders*, `arXiv:math.GR/0502237`.

[7] Martin Kassabov and Nikolay Nikolov, *Universal lattices and Property Tau*, `arXiv:math.GR/0502112`.

[8] D. A. Každan, *On the connection of the dual space of a group with the structure of its closed subgroups*, Funkcional. Anal. i Priložen. **1** (1967), 71–74. MR0209390 (35 #288)

[9] John D. Lafferty and Daniel Rockmore, *Fast Fourier analysis for* SL_2 *over a finite field and related numerical experiments*, Experiment. Math. **1** (1992), no. 2, 115–139. MR1203870 (94f:11131)

[10] Martin W. Liebeck and L. Pyber, *Finite linear groups and bounded generation*, Duke Math. J. **107** (2001), no. 1, 159–171. MR1815254 (2001m:20081)

[11] Alexander Lubotzky, *Finite simple groups of Lie type as expanders*, in preparation.

[12] ———, *Discrete groups, expanding graphs and invariant measures*, Progress in Mathematics, vol. 125, Birkhäuser Verlag, Basel, 1994. MR1308046 (96g:22018)

[13] Alexander Lubotzky, Beth Samuels, and Uzi Vishne, *Explicit constructions of Ramanujan complexes of type* A_d, European J. Combin. **26** (2005), no. 6, 965–993. MR2143204

[14] ———, *Ramanujan complexes of type* A_d, Israel J. of Math. (to appear).

[15] Alexander Lubotzky and B. Weiss, *Groups and expanders*, Expanding graphs (Princeton, NJ, 1992), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 10, Amer. Math. Soc., Providence, RI, 1993, pp. 95–109. MR1235570 (95b:05097)

[16] Moshe Morgenstern, *Existence and explicit constructions of* $q+1$ *regular Ramanujan graphs for every prime power* q, J. Combin. Theory Ser. B **62** (1994), no. 1, 44–62. MR1290630 (95h:05089)

[17] Nikolay Nikolov, *A product decomposition for the classical quasisimple groups*, `arXiv:math.GR/0510173`.

[18] Omer Reingold, Salil Vadhan, and Avi Wigderson, *Entropy waves, the zig-zag graph product, and new constant-degree expanders*, Ann. of Math. (2) **155** (2002), no. 1, 157–187. MR1888797 (2003c:05145)

[19] Yuval Roichman, *Upper bound on the characters of the symmetric groups*, Invent. Math. **125** (1996), no. 3, 451–485. MR1400314 (97e:20014)

[20] ———, *Expansion properties of Cayley graphs of the alternating groups*, J. Combin. Theory Ser. A **79** (1997), no. 2, 281–297. MR1462559 (98g:05070)

[21] Yehuda Shalom, *Bounded generation and Kazhdan's property (T)*, Inst. Hautes Études Sci. Publ. Math. (1999), no. 90, 145–168 (2001). MR1813225 (2001m:22030)