Finite simple groups as expanders

Martin Kassabov[†], Alexander Lubotzky[‡], and Nikolay Nikolov[§¶]

[†]Department of Mathematics, Cornell University, Ithaca, NY 14853; [‡]Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel; and [§]New College, Oxford OX1 3BN, United Kingdom

Edited by Robion C. Kirby, University of California, Berkeley, and approved February 21, 2006 (received for review November 30, 2005)

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 Cay(G; S) is an ε-expander.

expander graphs | Ramanujan complexes

Let X be a finite graph and $0 < \varepsilon \in \mathbb{R}$. Then X is called an ε-expander if for every subset A of the vertices of X with $|A| \leq (1/2)|X|$ we have $|\partial A| \geq \varepsilon|A|$, 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. ref. 1, the references therein, and ref. 2). Many of these constructions are of Cayley graphs, and in particular various infinite families of finite simple groups have been shown to be expanding families.

A finite group G is called an ε-expander with respect to a generating subset S if the Cayley graph Cay(G; S) is an ε-expander. We will say that an infinite family $\mathfrak{G}$ of groups is a family of expanders 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 with respect to (w.r.t.) which G is an ε-expander. In this situation we also say that the groups $G \in \mathfrak{G}$ are expanders "uniformly." Until recently all known such families consisting of simple groups were of bounded Lie rank (cf. refs. 1 and 3), a fact that has raised speculation that this is the only possibility (see refs. 4 and 5).

It is easy to see that the diameter of each graph X_i from an expander family $\{X_i\}$ is most $c \log|X_i|$ (where c is a constant). In ref. 6 it was shown that every non-abelian finite simple group has a set S of seven generators for which the Cayley graph 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 uniformly, although, as observed by Y. Luz (see ref. 4), the generators used in ref. 6 do not give rise to expanders.

The main goal of this note is to announce a proof of almost the whole of this conjecture.

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* Cay(G; S) *is an ε-expander.*

In fact careful estimates using variations of some of the arguments below yield $k < 1{,}000$ and $\varepsilon > 10^{-10}$.

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 $SL_2(\mathbb{F}_p)$ or $PSL_2(\mathbb{F}_p)$ like all the other finite simple groups (see below for more details).

The proof of *Theorem 1* is the accumulation of the works (refs. 7–10 and A.L., unpublished results) in the following chronological order.

In ref. 7 it was proved, extending the work of Shalom (3), that for $m \geq 3$ and $k \geq 0$ the group $SL_m(\mathbb{Z}[x_1, \ldots, x_k])$ has property (τ), i.e., its finite quotients are expanders. It was then further shown in ref. 8 that if $R = \mathbb{Z}\langle x_1, \ldots, x_k\rangle$ is a free noncommutative ring, then suitable finite quotients of $EL_m(R)$ are also expanders uniformly, provided $m \geq 3$ [where $EL_m(R)$ denotes the subgroup of the multiplicative group of $Mat_m(R)$ generated by the elementary matrices]. This includes, in particular, the groups $EL_3(Mat_n(\mathbb{F}_q)) \simeq SL_{3n}(\mathbb{F}_q)$, and thus $SL_{3n}(\mathbb{F}_q)$ are uniformly expanders for all n and for all prime powers q. For every $d \geq 3$, the group $SL_d(\mathbb{F}_q)$ is a bounded product of copies of $SL_{3n}(\mathbb{F}_q)$ for $n = \lfloor d/3 \rfloor$, which implies (using *Lemma 1* below) that the groups $\{SL_d(\mathbb{F}_q) \mid d \geq 3, q \text{ prime power}\}$ form a family of expanders.

It was then shown in ref. 10 that every finite simple classical group of Lie type is a bounded product of copies of $SL_d(\mathbb{F}_q)$ and its central quotients. This fact can be combined with the previous results to yield that all classical groups of Lie type of sufficiently high rank are expanders uniformly.

The alternating groups Alt(n) [or equivalently the symmetric groups Sym(n)] for $n \geq 5$ are also expanders in a uniform way. This result is proved in ref. 9. The argument here is more involved because Alt(n) contains copies of $SL_d(\mathbb{F}_q)$, but it is not boundedly generated by such groups. The proof instead goes by decomposing the regular representation of Alt(n) into two components. On the first component Alt(n) acts as if it is boundedly generated by some copies of powers of $SL_d(\mathbb{F}_q)$. On the second component one applies the eigenvalue estimates of ref. 11. The idea of this decomposition comes from work of Roichman (12).

On the other hand, it is shown by A.L. (unpublished results) that the family $SL_2(\mathbb{F}_q)$, q a prime power, is also a family of expanders. This result is proved by a combination of Selberg's Theorem (cf. ref. 1 and *Section 4*) with the explicit construction of Ramanujan graphs as given in ref. 13. In fact, a similar method (using the theory of Ramanujan complexes cf. ref. 14 and their explicit construction in ref. 13) also gives that the groups $SL_d(\mathbb{F}_q)$ for all $d \geq 2$ and all prime powers q are expanders uniformly.

The case of $SL_2(\mathbb{F}_q)$ is the crucial new case of A.L. (unpublished results). It is further shown there, using some model theoretic results of Hrushovski and Pillay (15), 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 $SL_2(\mathbb{F}_q)$'s. One therefore deduces that the groups of Lie type and rank $\leq r$ are expanders uniformly. This case exactly complements the results of refs. 8 and 10 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 does not reflect the chronological story. We recall and make in *Section 1* some observations regarding the representation theoretic reformulation of the problem. In *Section 2* we describe the proof for SL_2, while *Sections 3* and *4* give two proofs for the case of SL_d, ($d \geq 3$): first, via Ramanujan complexes and second, via $EL_3(\mathbb{Z}\langle x_1, \ldots, x_k\rangle)$. In *Section 5* we use the results for $SL_d(\mathbb{F}_q)$ to construct expanding

Conflict of interest statement: No conflicts declared.

This paper was submitted directly (Track II) to the PNAS office.

Abbreviation: w.r.t., with respect to.

¶To whom correspondence should be addressed. E-mail: nikolay.nikolov@new.ox.ac.uk.

www.pnas.org/cgi/doi/10.1073/pnas.0510337103

generating sets in all simple groups of Lie type (with the exception of the Suzuki groups). In *Section 6* we describe the proof for Alt(n), which is a case of great special interest.

1. A Representation Theoretic Interpretation

As is well known (cf. ref. 1, Chap. 4), the expanding property of Cay(G; S) is equivalent to representation theoretic properties. We need some notation.

The normalized adjacency matrix of a k-regular graph X is defined to be $\Delta = 1/k \cdot A$ where A is the adjacency matrix of X. Then all the eigenvalues of Δ are in $[-1, 1]$. The second largest eigenvalue is denoted $\lambda(X)$.

Let $I(\alpha, G, S)$ denote the following statement:

For every unitary representation (V, φ) *of* G, *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").*

Proposition 1 below can be deduced from the proofs of propositions 4.2.4 and 4.2.5 and theorem 4.3.2 of ref. 1, noting that the "nonnormalized spectral gap" $\lambda_1(X)$ there is equal to $k(1 - \lambda(X))$ under our definition.

Proposition 1. *The following hold:*

(i) (a) For each $\alpha > 0$ *there is* $\varepsilon > 0$ *such that a Cayley graph* $X =$ Cay(G; S) *is an* ε*-expander if* $I(\alpha, G, S)$ *holds.*
(b) For each $\delta > 0$ *there is* $\alpha > 0$ *such that if* $X =$ Cay(G, S) *is a Cayley graph and* $\lambda(X) < 1 - \delta$ *then* $I(\alpha, G; S)$ *holds.*
(ii) Moreover, if $k = |S|$ *is bounded then the implications in (i) can be reversed.*

We shall repeatedly use the following easy lemma.

Lemma 1 (9). *Let* G *be a finite group generated by a collection of subgroups* $\{H_i\}$ *and let* ε_1, $\delta > 0$. *Assume that each subgroup* H_i *is generated by a subset* S_i *such that* $|\cup_i S_i| \leq k$ *and that each graph* Cay(H_i; S_i) *is an* ε_1*-expander. Moreover, assume that the graph* $Y =$ Cay(G; $\cup_i H_i$) *satisfies* $\lambda(Y) < 1 - \delta$.

Then there exists $\varepsilon > 0$ *depending on* ε_1, δ *and* k *such that the Cayley graph* Cay(G; $\cup_i S_i$) *is an* ε*-expander.*

For the proof take any unitary representation (V, φ) of G with a $\cup_i S_i$-almost invariant vector v. Restricting the representation to each H_i we see that v is H_i-almost invariant. The last assumption of *Lemma 1* implies that v is then G-almost invariant and by *Proposition 1*, Cay(G; $\cup_i S_i$) is an expander.

This lemma 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 ε_0-expander (w.r.t. some set of generators S_i), then G is an ε-expander w.r.t. their union $S = \cup S_i$.

2. The $SL_2(\mathbb{F}_{p^k})$ Case

In this section we will show, following A.L. (unpublished results), that $PSL_2(q)$ can be made into expanders uniformly for every prime power $q = p^\alpha$. It is known that:

Fact 1: The family of groups $SL_2(\mathbb{F}_p)$, p prime, w.r.t. the generators

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

form a family of expanders. For a proof, based on Selberg's theorem $\lambda_1 \geq 3/16$, see ref. 1, Section 4.

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

The result of *Fact 2* was first proved by Morgenstern (16), and it relies on 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 ref. 13. In the construction there, a symmetric set of $p + 1$ generators S'_p for $SL_2(\mathbb{F}_{p^k})$ is given as the $p + 1$ conjugates of a fixed element C by a fixed nonsplit torus H of $SL_2(\mathbb{F}_p)$, i.e., $S'_p = \{h^{-1}C^{\pm 1}h \mid h \in H\}$. Now

$$\lambda(\text{Cay}(SL_2(\mathbb{F}_{p^k}); S'_p)) \leq \frac{2\sqrt{p}}{p+1} < \frac{19}{20},$$

therefore these graphs are ε-expanders by *Proposition 1*, for some $\varepsilon > 0$ independent of k and p. However, the generating sets S'_p are not bounded.

At the same time Cay($SL_2(p)$; $\{A, B\}$) are expanders uniformly by *Fact 1*. All together, these facts imply that Cay($SL_2(\mathbb{F}_{p^k})$; $\{A, B, C\}$) are expanders by *Lemma 1*: Indeed, if (V, φ) is a representation of $G = SL_2(\mathbb{F}_{p^k})$ and $v \in V$ is S-almost invariant for the set $S = \{A, B, C\}$, then v is $SL_2(\mathbb{F}_p)$-almost invariant and hence is also S'_p-almost invariant, because $S'_p \subset SL_2(\mathbb{F}_p) \cdot C \cdot SL_2(\mathbb{F}_p)$, and hence v is G-almost invariant.

This argument shows that $SL_2(\mathbb{F}_{p^k})$ are uniformly expanders with three generators.

3. $SL_d(\mathbb{F}_{p^k})$ via Ramanujan Complexes

One can generalize the proof for SL_2 described in *Section 2* to SL_d for every d. We sketch the proof below (details available from A.L. upon request).

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 $E^* \to GL_d(\mathbb{F}_q)$ given by letting E^* act on E by multiplication, induces an isomorphism of

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

where H is a nonsplit maximal torus of order $(q^d - 1)/(q - 1)$. In ref. 13 it was shown that there exists an $\varepsilon > 0$ such that for a suitable choice of $D \in SL_d(\mathbb{F}_q)$, the Cayley graphs Cay($SL_d(\mathbb{F}_q)$; S') are ε-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 $SL_d(\mathbb{F}_q)$, which is a Ramanujan complex, see ref. 14. The eigenvalue bound on these Hecke operators implies that

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

and in particular these are ε-expanders by *Proposition 1*.

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

$$\lambda(\text{Cay}(SL_d(\mathbb{F}_q); S')) \leq \frac{1}{\sqrt{q}} + o(1) \leq \frac{19}{20},$$

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

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

$$E^* = \mathbb{F}^*_{q^{2m}} \hookrightarrow GL_2(q^m) \hookrightarrow GL_{2m}(q) = GL_d(q),$$

which shows that $H \leq SL_d(\mathbb{F}_q)$ is contained in a copy of $SL_2(\mathbb{F}_{q^m})$.

Take now the expanding generating set $\{A, B, C\}$ of $SL_2(\mathbb{F}_{q^m})$ from *Section 2* with D to obtain a generating set S of four elements for $SL_d(\mathbb{F}_q)$.

We claim that $SL_d(\mathbb{F}_q)$ are a family of expanders w.r.t. these four generators. By *Lemma 1* again, an $S = \{A, B, C, D\}$-almost invariant vector is $SL_2(\mathbb{F}_{q^m})$-almost invariant, and then it is $H{\cdot}D{\cdot}H$-almost invariant hence also S'-almost invariant and thus $G = SL_d(\mathbb{F}_q)$-almost invariant as required.

This argument covers the case of even d. For odd d, the group $SL_d(\mathbb{F}_q)$ is a product of four copies of $SL_{d-1}(\mathbb{F}_q)$, and we can apply *Lemma 1*.

4. $SL_d(\mathbb{F}_{p^k})$ for ($d \geq 3$) via $EL_3(R)$

A different proof for the case of SL_d has been given in ref. 8 [prior to the proof of A.L. (unpublished results), which is described in *Section 3*]. This proof builds on the work of Shalom (3), where he gave a new proof of Kazhdan's result (17) that $SL_3(\mathbb{Z})$ has property (T). Shalom's proof has two ingredients.

Part 1: The group $\Lambda = SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ has a relative Kazhdan property (T) relative to $\mathbb{Z}^2$, i.e., if (V, φ) is a unitary representation space of Λ with an almost invariant vector w.r.t. the set of four natural generators, then this vector is $\mathbb{Z}^2$-almost invariant.

Part 2: The group Λ is isomorphic to a maximal parabolic subgroup of $SL_3(\mathbb{Z})$. Conjugating with the Weyl group gives rise to six obvious embeddings of Λ in $SL_3(\mathbb{Z})$. The images of $\mathbb{Z}^2$ in these embeddings (which include all root subgroups) boundedly generate $SL_3(\mathbb{Z})$ by a result of Carter and Keller (18).

Parts 1 and *2* together imply that if V is a unitary representation of $\Gamma = SL_3(\mathbb{Z})$ 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 *Part 1* works also for $\Lambda = SL_2(R_0) \ltimes R_0^2$, when R_0 is the polynomial ring in k variables over $\mathbb{Z}$. However, it is not known if the bounded generation of *Part 2* holds in this case, which would imply that $SL_3(R_0)$ has property (T). Still, by analyzing the congruence kernel of $SL_3(R_0)$, it is deduced in ref. 7 that $\Gamma = SL_3(R_0)$ 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 ref. 8: it is shown there that *Part 1* holds even if one takes the noncommutative free ring $R = \mathbb{Z}\langle x_1, \ldots, x_k\rangle$, i.e., $\Lambda = EL_2(R) \ltimes R^2$ has property (T) relative to R^2.

It will be quite surprising if the analogue of the Carter and Keller result holds for $\Gamma = EL_3(R)$, i.e., if Γ is boundedly generated by its root subgroups. However, this fact holds for many quotients $\bar{R}$ of R: If $\bar{R} = Mat_n(\mathbb{F}_q)$ or $\bar{R} = Mat_n(\mathbb{F}_q)^s$ for $s \leq q^{n^2}$, then $\bar{R}$ is an image of $\mathbb{Z}\langle x_1, x_2, x_3\rangle$ and $EL_3(\bar{R})$ is boundedly generated by its elementary matrices in a way that is independent of n, q, and s. This result implies that the groups $EL_3(Mat_n(\mathbb{F}_q)) = SL_{3n}(\mathbb{F}_q)$ and $EL_3(Mat_n(\mathbb{F}_q)^s) = SL_{3n}(\mathbb{F}_q)^s$ are a family of expanders.

For a general $d \geq 3$, one notes again that $SL_d(\mathbb{F}_q)$ is a bounded product of a bounded number of copies of $SL_{3n}(\mathbb{F}_q)$ for $n = \lfloor d/3 \rfloor$. We can therefore deduce by *Lemma 1* that $SL_d(\mathbb{F}_q)$ form a family of 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 $SL_d(\mathbb{F}_q)$, which are essential for constructing expanding generating sets in the alternating groups (see *Section 6*).

5. Simple Groups of Lie Type

The following two theorems show how to reduce the case of finite simple groups of Lie type (minus the Suzuki groups) to the case of $SL_d(\mathbb{F}_q)$ described in *Sections 2–4*.

Theorem 2 (10). *There exists a constant C such that every finite simple group G of classical type is a product of at most C subgroups of G which are quotients of $SL_d(\mathbb{F}_q)$ (for some $d \geq 2$ and q).*

Theorem 3 (A.L., unpublished results). *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 at most $C(r)$ subgroups each of which is a quotient of $SL_2(\mathbb{F}_q)$ for a suitably chosen field $\mathbb{F}_q$.*

As explained in *Lemma 1*, once a group G is a product of boundedly many groups that are ε-expanders, its Cayley graph is an ε'-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 $SL_d(\mathbb{F}_q)$ or $PSL_d(\mathbb{F}_q)$ for any $d \geq 2$ and prime power q. In fact, the order of a Suzuki group is not divisible by 3, whereas $|SL_d(\mathbb{F}_q)|$ is.

The proof of *Theorem 2* is based on the fact that an arbitrary connected Dynkin diagram of high rank becomes one of type A_d after a vertex is deleted. In this way we can find a quasisimple quotient G_1 of $SL_{d+1}(\mathbb{F}_q)$ inside G (in fact it is a Levi factor of a suitable parabolic subgroup).

If U (resp. U_1) is a maximal unipotent subgroup of G (resp G_1) then ref. 10 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 Liebeck and Pyber in ref. 19 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 3* with explicit bounds for $C(r)$, but this is not the way this theorem is proved by A.L. (unpublished results).

Instead, the author there appeals to a model theoretic method developed by Hrushovski and Pillay (15). There, it is shown that "definable" subgroups of $GL_n(F)$ 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 ultraproducts of finite fields are pseudo-algebraically closed (see ref. 20). As elementary statements are true in an ultraproduct if 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 $SL_2(\mathbb{F}_q)$ or $PSL_2(\mathbb{F}_q)$ 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 $Alt(n)$. For its special importance, we restate it as follows.

Theorem 4 (9). *There exist $l \in \mathbb{N}$ and $0 < \varepsilon \in \mathbb{R}$ such that for every $n \in \mathbb{N}$ the alternating group $Alt(n)$ has an explicit set of generators S_n of size at most l such that $Cay(Alt(n); S_n)$ is an ε-expander. The same holds also for the symmetric groups $Sym(n)$.*

The main idea of the proof in ref. 9 is as follows. Assume first that $n = d^6$ and $d = 2^{3k} - 1$ for some k. Based on ideas and results from ref. 8 (see *Section 4*) it is shown first that the Cayley graphs of the groups $\Delta_k = SL_{3k}(\mathbb{F}_2)^{d^5}$ w.r.t. some generating set F_k of size at most 20 are ε_0-expanders for all k and $d = 2^{3k} - 1$ (for some fixed $\varepsilon_0 > 0$).

Now, thinking of the set $\{1, \ldots, n\}$ as the points in a six-dimensional cube of size d, and remembering that $SL_{3k}(\mathbb{F}_2)$ acts transitively on a set of size d (via its defining linear action on $\mathbb{F}_2^{3k}$), we can construct six different embeddings π_i of Δ_k into $Alt(n)$, where the image under π_i of each copy of $SL_{3k}(\mathbb{F}_2)$ in Δ_k acts on the points on a line parallel to the ith 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 $Alt(n)$ with respect to S_n form a family of expanders. Using that F_k is an expanding generating set in Δ_k by *Lemma 1* it suffices to show that the existence of an E-almost

invariant vector v in any unitary representation V of $\mathrm{Alt}(n)$ implies the existence of an $\mathrm{Alt}(n)$-almost 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 not too big (less than $n - d^{5/4}$) and V_2 contains all others. A similar decomposition is used by Roichman in ref. 12 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.

Argument 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 that 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 fact 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 the results of Roichman (11), who studied normalized character values of the symmetric groups. Roichman's results give 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.

Argument 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 fact, together with the almost invariance of v_2 under E, implies that v_2 is close to an invariant vector.

This argument 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 $\mathrm{Alt}(n)$. By adding any odd permutation to S_n, we see that the symmetric groups $\mathrm{Sym}(n)$ also form a family of expanders.

A.L. was supported by the National Science Foundation and the Binational Science Foundation (U.S. and Israel). This work was done while visiting the Institute for Advanced Study at Princeton University, supported by the Ambrose Monell Foundation and the Ellentuck Fund.

1. Lubotzky, A. (1994) *Discrete Groups, Expanding Graphs and Invariant Measures*, Progress in Mathematics (Birkhäuser, Basel), Vol. 125.
2. Reingold, O., Vadhan, S. & Wigderson, A. (2002) *Ann. Math.* **155,** 157–187.
3. Shalom, Y. (1999) *Inst. Hautes Études Sci. Publ. Math.* **90,** 145–168.
4. Lubotzky, A. & Weiss, B. (1992) *Groups and Expanders: Expanding Graphs*, DIMACS Series for Discrete Mathematics and Theoretical Computer Science (Am. Math. Soc., Providence, RI), Vol. 10, pp. 95–109.
5. Lafferty, J. D. & Rockmore, D. (1992) *Exp. Math.* **1,** 115–139.
6. Babai, L., Kantor, W. M. & Lubotzky, A. (1989) *Eur. J. Combin.* **19,** 507–522.
7. Kassabov, M. & Nikolov, N. (March 14, 2006) *Invent. Math.* 10.1007/s00222-005-0498-0.
8. Kassabov, M. (2005) arXiv: math.GR/0502237.
9. Kassabov, M. (2005) arXiv: math.GR/0505624.
10. Nikolov, N. (2006) *J. Group Theory*, in press.
11. Roichman, Y. (1996) *Invent. Math.* **125,** 451–485.
12. Roichman, Y. (1997) *J. Combin. Theory Ser. A* **79,** 281–297.
13. Lubotzky, A., Samuels, B. & Vishne, U. (2005) *Eur. J. Combin.* **26,** 965–993.
14. Lubotzky, A., Samuels, B. & Vishne, U. (2005) *Isr. J. Math.* **149,** 267–300.
15. Hrushovski, E. & Pillay, A. (1995) *J. Reine Angew. Math.* **462,** 69–91.
16. Morgenstern, M. (1994) *J. Combin. Theory Ser. B* **62,** 44–62.
17. Každan, D. A. (1967) *Funkcional. Anal. Priložen* **1,** 71–74.
18. Carter, D. & Keller, G. (1983) *Am. J. Math.* **105,** 673–687.
19. Liebeck, M. W. & Pyber, L. (2001) *Duke Math. J.* **107,** 159–171.
20. Fried, M. D. & Jarden, M. (2005) *Field Arithmetic*, Results in Mathematics and Related Areas: 3rd Series, A Series of Modern Surveys in Mathematics (Springer, Berlin), Vol. 11.