ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 11, Pages 47–56 (June 9, 2005)
S 1079-6762(05)00146-0

SYMMETRIC GROUPS AND EXPANDERS

MARTIN KASSABOV

(Communicated by Efim Zelmanov)

ABSTRACT. We construct explicit generating sets F_n and $\tilde{F}_n$ of the alternating and the symmetric groups, which turn the Cayley graphs $\mathcal{C}(\mathrm{Alt}(n), F_n)$ and $\mathcal{C}(\mathrm{Sym}(n), \tilde{F}_n)$ into a family of bounded degree expanders for all sufficiently large n. These expanders have many applications in the theory of random walks on groups and in other areas of mathematics.

A finite graph Γ is called an ϵ-expander for some $\epsilon \in (0,1)$ if for any subset $A \subseteq \Gamma$ of size at most $|\Gamma|/2$ we have $|\partial(A)| > \epsilon|A|$ (where $\partial(A)$ is the set of vertices of $\Gamma \backslash A$ of edge distance 1 to A). The largest such ϵ is called the expanding constant of Γ. Constructing families of ϵ-expanders with bounded valency is an important practical problem in computer science, because such graphs have many nice properties — for example, these graphs are highly connected, have a logarithmic diameter and the random walks mix rapidly. For an excellent introduction to the subject we refer the reader to the book [19] by A. Lubotzky.

Using counting arguments it can be shown that almost any 5 regular graph is a 1/5-expander. However, constructing explicit examples of families of expander graphs is a difficult problem.

The first explicit construction of a family of expanders was done by G. Margulis in [23], using Kazhdan's property T of $\mathrm{SL}_3(\mathbb{Z})$. Currently there are several different construction of expanders. With the exception of a few recent ones based on the zigzag products of graphs (see [2, 25, 28]), all constructions are based on group theory and use some variant of property T (property τ, Selberg's property, etc.).

Kazhdan's property T is not very interesting for a given finite group G (all finite groups have property T), but the related Kazhdan constant with respect to some generating set F is. Given an infinite collection of finite groups G_i, it is a challenge to prove or disprove the existence of uniform Kazhdan constants with respect to properly chosen generating sets. Problem 3 below is a reformulation of this question.

The original definition of property T uses the Fell topology of the unitary dual; see [13]. Here we will use an equivalent definition (only for discrete groups) which also addresses the notion of Kazhdan constants.

Received by the editors March 16, 2005.
2000 *Mathematics Subject Classification.* Primary 20B30; Secondary 05C25, 05E15, 20C30, 20F69, 60C05, 68R05, 68R10.
Key words and phrases. Expanders, symmetric groups, alternating groups, random permutations, property T, Kazhdan constants.

Definition 1. Let G be a discrete group generated by a finite set S. Then G has Kazhdan's property T if there exists $\epsilon > 0$ such that for every unitary representation $\rho: G \to U(\mathcal{H})$ on a Hilbert space $\mathcal{H}$ without G invariant vectors and every vector $v \neq 0$ there exists some $s \in S$ such that $\|\rho(s)v - v\| > \epsilon\|v\|$. The largest ϵ with this property is called the *Kazhdan constant* for G with respect to S and is denoted by $\mathcal{K}(G; S)$.

For a group G the property T is independent on the choice of the generating set S; however, the Kazhdan constant depends also on the generating set.

There is a well-known connection between property T and expander graphs:

Theorem 2 ([19], Theorem 4.3.2)**.** *Let G be a discrete group having property T, and let S be a finite generating set of G. Then there exists an $\epsilon = \epsilon(S) > 0$ such that the Cayley graphs $\mathcal{C}(G_i, S_i)$ (and all their quotients) of the finite images of G_i of G (with respect to the images S_i of S) form a family of ϵ-expanders. The largest $\epsilon_0(S)$ with this property is related to the Kazhdan constant $\mathcal{K}(G, S)$, in particular we have $\epsilon_0(S) \geq \mathcal{K}(G; S)^2/4$.*

Using this approach and property T of $\mathrm{SL}_n(\mathbb{Z})$ one can make the Cayley graphs of $\mathrm{SL}_n(\mathbb{F}_p)$ for fixed $n \geq 3$ a family of expanders.[1] Until recently the only way to prove Kazhdan's property T was via representation theory of high rank Lie groups. These methods are not quantitative and do not lead to estimates for the Kazhdan constants and the corresponding expanding constants of the resulting Cayley graphs.

A breakthrough in this direction is due to Y. Shalom [29], who used the bounded generation of the $\mathrm{SL}_n(\mathbb{Z})$ and M. Burger's estimate (see [6]) of the relative Kazhdan constant of $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ to obtain a lower bound for the Kazhdan constant of $\mathrm{SL}_n(\mathbb{Z})$. His methods were refined in [8] to give the exact asymptotic of the Kazhdan constant of $\mathrm{SL}_n(\mathbb{Z})$ with respect to the set of all elementary matrices. This yields an asymptotically exact estimate for the expansion constant of the form n^{-1} of the Cayley graphs of $\mathrm{SL}_n(\mathbb{F}_p)$ with respect to the set of all elementary matrices. It is interesting to note that if the size of the matrices increases, then the resulting Cayley graphs do not form an expander family, even though the degree of these graphs goes to infinity.

Using the relative property T of the pair $\mathrm{SL}_2(R) \ltimes R^2, R^2$ for finitely generated noncommutative rings R, the Cayley graphs of $\mathrm{SL}_n(\mathbb{F}_q)$ for any prime power q and all $n \geq 3$ can be made expanders simultaneously by choosing a suitable generating set; see [10]. An important building block in this construction is that the group $\mathrm{SL}_n(\mathbb{F}_q)$ can be written as a product of 20 abelian subgroups and this number is independent of n and q.

The examples lead to the following problem:

Problem 3. Let G_i be an infinite family of finite groups. Is it possible to make their Cayley graphs expanders using suitably chosen generating sets?

Currently there is no theory which can give a satisfactory answer to this question. The answer is known only in a few special cases: If the family of finite groups comes from a finitely generated infinite group with property T (or its weaker versions), then the answer is YES. Also if all groups in the family are "almost" abelian, then

[1] The Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ can also be made expanders although the group $\mathrm{SL}_2(\mathbb{Z})$ does not have property T or even τ; see [16].

the answer is NO (see [17]), and this is practically the only case where a negative answer is known.

Motivated by the above remark A. Lubotzky conjectured [18] that Problem 3 should have a positive answer in the case of finite simple groups:

Conjecture 4. There exist constants $L > 0$ and $\epsilon > 0$ such that any nonabelian finite simple group G has a generating set F such that $|F| \leq L$ and the Cayley graphs $\mathcal{C}(G; F)$ form a family of ϵ-expanders. Equivalently, we have that $\mathcal{K}(G; F) > \epsilon$ (with a different constant ϵ).

This conjecture is supported by several results — it is known (see [5] and [12]) that for any nonabelian finite simple group there exists a 4 element generating set such that the diameter of the corresponding Cayley graph is logarithmic in the size of the group.

As with many similar results, one expects that the proof of Conjecture 4 will use the classification of the finite simple groups. It seems that almost all finite simple groups of Lie type groups can be made expanders using an idea from [10]. The alternating groups form the only other infinite family of finite simple groups, and it was believed that this is the most difficult case of the Lubotzky conjecture.

The methods from [10] cannot be applied directly to the symmetric/alternating groups because these groups cannot be written as a product of a fixed number of abelian subgroups — the size of $\mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$ is approximately n^n, and every abelian subgroup has at most 2^n elements; see [1]. This suggests that the groups $\mathrm{Alt}(n)$ are "further from the abelian groups" than all other finite simple groups, and therefore they should have more expanding properties. Unfortunately, this also significantly complicates the construction of expanders based on the alternating groups.

The main result announced in the paper can be viewed as a major step toward proving Conjecture 4. Theorem 7, together with the results from [10], proves the Lubotzky conjecture in all but a few cases; see [11] for details.

If one allows unbounded generating sets, there are only a few partial results known. A classical result of N. Alon and Y. Roichman (and its improvements in [14] and [15]) says that any group is an ϵ-expander[2] with respect to a random large generating set:

Theorem 5 ([3]). *For any $\epsilon > 0$ there exists $c(\epsilon) > 0$ such that the Cayley graph of any finite group G is an ϵ-expander with respect to a random generating set of size $c(\epsilon) \log |G|$.*

The bound $c(\epsilon) \log |G|$ is the optimal one in the class of all finite groups, because the large abelian groups are not expanders with respect to small generating sets. It is believed that if the group G is far from being abelian, the bound $c \log |G|$ can be improved. Note that Theorem 5 implies a version of Conjecture 4, where the size of the generating set is allowed to increase.

Theorem 5 also gives that the Cayley graphs of the alternating groups $\mathrm{Alt}(n)$ are expanders with respect to a random generating set of size $n \log n$. This was the best known result in this direction, and even there were no known explicit sets of

[2]There are two different definitions of ϵ-expanders, which are equivalent for graphs of bounded degree but not in general: A "weak" one corresponding to Definition 1, and a "strong" one using the spectral gap of the Laplacian. The random Cayley graphs obtained from Theorem 5 are expanders in both definitions.

size less than $n^{\sqrt{n}}$ which make the Cayley graphs expanders. In view of the main results in this paper it is very interesting to understand the expanding properties of the Cayley graphs of $\mathrm{Alt}(n)$ and other finite simple groups with respect to a random generating set of a small (even bounded) size.

One of the main results announced in this paper answers affirmatively an old question, which has been asked several times in the literature; see [4, 19, 20, 22]:

Theorem 6. *There exist constants $L > 0$, $\epsilon > 0$ and an infinite sequence n_s with the property: There exists a constructible generating set F_{n_s} of size at most L of the alternating group $\mathrm{Alt}(n_s)$ such that the Cayley graphs $\mathcal{C}(\mathrm{Alt}(n_s); F_{n_s})$ form a family of ϵ-expanders.*

From the proof of Theorem 6, it can be seen that the sequence n_i does not grow too fast, which leads to the following generalization:

Theorem 7. *There exist constants $L > 0$ and $\epsilon > 0$, with the property: For any n there exist explicit generating sets F_n and $\tilde{F}_n$ of the alternating group $\mathrm{Alt}(n)$ and the symmetric group $\mathrm{Sym}(n)$ respectively such that the Cayley graphs $\mathcal{C}(\mathrm{Alt}(n); F_n)$ and $\mathcal{C}(\mathrm{Sym}(n); \tilde{F}_n)$ form a family of ϵ-expanders. Moreover all generating sets F_n and $\tilde{F}_n$ have at most L elements.*

Theorem 7 has interesting applications: It provides one of the few constructions of an expander family of Cayley graphs $\mathcal{C}(G_i, S_i)$ such that the groups G_i are not quotients of some infinite group having a variant of Kazhdan's property T.[3] It also provides a supporting evidence for the conjecture that the automorphism groups of the free groups have property τ; see [7] and [21].

Theorem 7 implies that the expanding constant of $\mathrm{Alt}(n)$ with respect to the set $F_n^{10^{10}}$ is large enough.[4] The size of the set $F_n^{10^{10}}$ is independent of n, and if n is sufficiently large, then $|F_n^{10^{10}}| < 10^{-30} n^{1/30}$. The last inequality allows us to use the expander $\mathcal{C}(\mathrm{Alt}(n); F_n^{10^{10}})$ as a "seed" graph for the Rozenman, Shalev, and Widgerson recursive construction of expanders; see [28]. This construction produces a family of expander graphs based on the Cayley graphs of the automorphism group of large n-regular rooted tree of depth k. A slight modification of this construction gives another recursive expander family based on $\mathrm{Alt}(n^k)$ for a fixed large n and different k's.

Theorem 7 gives that the Cayley graphs $\mathcal{C}(\mathrm{Alt}(n); F_n)$ and $\mathcal{C}(\mathrm{Sym}(n); \tilde{F}_n)$ have many expanding properties which imply that the random walks on $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$, generated by F_n and $\tilde{F}_n$ respectively, have mixing time of approximately $\log |\mathrm{Alt}(n)| = n \log n$ steps.

Sketch of the proof of Theorem 6. This sketch describes all main steps in the construction and omits the proofs of several technical claims. The proofs of these claims are relatively easy and follow from standard combinatorial and probabilistic arguments. A complete proof of Theorem 6 can be found in [9].

[3]For any infinite family of finite groups G_i the existence of generating sets S_i such that the Cayley graphs $\mathcal{C}(G_i, S_i)$ are a family of expanders is equivalent to the existence of a finitely generated subgroup of $\prod G_i$ which has a variant of property T. The main point here is that we prove that the Cayley graphs are expanders without using the representation theory of this infinite group.

[4]More precisely we have that the spectral gap of the Laplacian of the Cayley graph is very close to 1.

We start with a very brief explanation of the main idea: Let ρ be a representation of $\mathrm{Alt}(N)$ with almost invariant vector v with respect to some generating set F (to be chosen later), where $N = k^d$ for some k and d. We will use two different arguments to show that ρ contains an invariant vector.

First, we show that the vector v is almost invariant with respect to the union of several abelian groups. After that we will split the representation ρ into two components — one corresponding to partitions λ with $\lambda_1 < N - h$ and second one containing all other partitions for some suitably chosen h. The decomposition of the regular representation of $\mathrm{Alt}(N)$ into two components depending on the first part of the partition λ comes from [27]. In this paper, Roichman uses a similar argument to show that the Cayley graphs of the symmetric/alternating group with respect to a conjugacy class with a large number of nonfixed points have certain expanding properties.

We will show that the projection of the vector v in the first representation is small provided that $h \gg K$. Also, if $h \ll N^{1/4}$, the projection of v in the second one is close to an invariant vector.[5] In order to satisfy these restrictions we need that $N \gg K^4$, i.e., $d > 4$. In order to simplify the argument a little, we also require that d is even, which justifies our choice of $d = 6$ and $N = K^6$. Also we need that $K \ll h \ll K^{3/2}$; therefore, we choose $h = K^{5/4}$ and define $\mathcal{H}_1$ to be the subrepresentation of $\mathcal{H}$ corresponding to all partitions with $\lambda_1 < N - K^{5/4}$. As an additional assumption, we require that $K+1$ is a power of some prime number and we use $K = 2^{3s} - 1$ for a sufficiently large s.[6]

We will think that the alternating group $\mathrm{Alt}(N)$ acts on a set of N points which are arranged into a 6-dimensional cube of size K, and we will identify these points with ordered 6-tuples of nonzero elements from the field $\mathbb{F}_{2^{3s}}$.

Let $\rho : \mathrm{Alt}(N) \to U(\mathcal{H})$ be a fixed unitary representation of the alternating group, and let $v \in \mathcal{H}$ be an ϵ-almost invariant unit vector for some generating set F. We will fix the set F and the number ϵ later. Without loss of generality, we may assume that $\mathcal{H}$ is generated by the orbit of the vector v.

Let H_s denote the group $\mathrm{SL}_{3s}(\mathbb{F}_2)$. The group H_s has a natural action on the set $V \setminus \{0\}$ of K nonzero elements of a vector space V of dimension $3s$ over $\mathbb{F}_2$. The elements of H_s act by even permutations on $V \setminus \{0\}$, because H_s is a simple group and does not have $\mathbb{Z}/2\mathbb{Z}$ as a factor. If we identify V with $\mathbb{F}_{2^{3s}}$, then the existence of a generator for the multiplicative group of $\mathbb{F}_{2^{3s}}$ implies that some element in $H_s = \mathrm{GL}_{2s}(\mathbb{F}_2)$ acts as a K-cycle on $V \setminus \{0\}$.[7]

Let Γ be the direct product of K^5 copies of the group H_s. The group Γ can be embedded into $\mathrm{Alt}(N)$ in 6 different ways, which we denote by π_i, $i = 1, \dots, 6$. The image of each copy of H_s under π_i acts as $\mathrm{SL}_{3s}(\mathbb{F}_2)$ on a set of $K = 2^{3s} - 1$ points where all coordinates but the ith one are fixed. It is clear that Γ contains an abelian subgroup $\overline{\Gamma}$ isomorphic to $(\mathbb{Z}/K\mathbb{Z})^{\times K^5}$.

---

[5] We believe that the argument also works even in the case $h \ll N^{1/2}$; however, we are unable to prove it. If such generalization is true, it will allow us to use $d = 4$, which will improve the estimates for the Kazhdan constants by a factor of 10.

[6] It can be shown that $s > 15$ suffices; however, the estimate depends on the constants involved in the character estimates from [26], which are not in the literature.

[7] We can use some other family of groups instead of $\{H_s\}_s$ — the only requirements for groups in $\{H_s\}_s$ are that they act transitively on a set of $K(s)$ points (where $K(s) \to \infty$ as $s \to \infty$) and that $\left\{H_s{}^{\times K(s)^5}\right\}_s$ can be made a bounded degree expanders. For example, we can use the groups $\mathrm{SL}_3(\mathbb{F}_p)$ acting on $\mathbb{F}_p{}^3 \setminus \{0\}$ or on the projective plane $P^2\mathbb{F}_p$ for different primes p.

Using Theorem 5 from [10], we can find a small generating set S of the group H_s such that the Kazhdan constant $\mathcal{K}(H_s; S) > 1/400$. This allows us to construct a generating set $\tilde{S}$ with 40 elements of Γ with similar properties, i.e., the Kazhdan constant

$$\mathcal{K}(\Gamma; \tilde{S}) > 1/500.$$

Now we can define the generating set F_N of $\mathrm{Alt}(N)$ such that the Kazhdan constant $\mathcal{K}(\mathrm{Alt}(N); F_N)$ can be estimated — the set F_N will be the union of the images of $\tilde{S}$ under the embeddings π_i:

$$F_N = \bigcup_i \pi_i(\tilde{S}).$$

The group generated by the set F_N contains the 6 images of Γ and therefore is the whole alternating group $\mathrm{Alt}(N)$. From now on, we will assume that the vector $v \in \mathcal{H}$ is ϵ-almost invariant with respect to the set F_N defined above.

Using the Kazhdan constant of $\mathcal{K}(\Gamma; \tilde{S})$, it can be seen that if v is an ϵ-almost invariant vector with respect to the set F_N in some representation ρ of $\mathrm{Alt}(N)$, then v is close to a Γ_i invariant vector, i.e.,

$$\|\rho(\pi_i(g))v - v\| \leq 10^3 \epsilon \|v\|,$$

for all $g \in \Gamma$ and any $i = 1, \ldots, 6$. If the diameters of the Cayley graphs of $\mathcal{C}(\mathrm{Alt}(N), \bigcup \Gamma_i)$ were bounded independently on N, this would gives us that the representation ρ has an invariant vector, provided that ϵ is small enough. Unfortunately this is not the case, because the size of $\bigcup \Gamma_i$ is small compared to $\mathrm{Alt}(N)$, i.e., the ratio $\ln |\mathrm{Alt}(N)| / \ln |\bigcup \Gamma_i|$ is not bounded.

Let $\overline{\Gamma_i}$ denote the image of $\overline{\Gamma}$ under the embedding π_i and let C be the union of $\overline{\Gamma_i}$. Thus, we may assume that the vector v is almost invariant with respect to the set C.

As mentioned before we will break the representation ρ into two components. The space $\mathcal{H}$ decomposes as a sum of irreducible representations

$$\mathcal{H} = \bigoplus_\lambda c_\lambda M^\lambda,$$

where the sum is over all partitions λ of N, M^λ denotes the irreducible representations corresponding to the partition λ, and c_λ is the multiplicity of M^λ in $\mathcal{H}$, which is either 0 or 1, since $\mathcal{H}$ is generated by 1 element. Let $\mathcal{H}_1$ be the sum of all irreducible subrepresentations of $\mathcal{H}$ which correspond to the partitions $\lambda = [\lambda_1, \lambda_2, \ldots]$ of N with

$$\lambda_1 < N - K^{5/4},$$

and let $\mathcal{H}_2$ be the orthogonal complement of $\mathcal{H}_1$ in $\mathcal{H}$.

This allows us to decompose the almost invariant vector v as $v = v_1 + v_2$, where $v_i \in \mathcal{H}_i$. We will use two different arguments to show that the vector v_1 is small and that v_2 is close to an invariant vector in $\mathcal{H}_2$.

Using the definition of the set C, it can be seen that C^{440} acts almost transitively on the set of all ordered tuples of $K^5/10$ points. Here C^{440} denotes the set of all products of less than 440 elements from the set C, and by almost transitivity we mean that if we are given 2 ordered tuples, then with large probability κ (approaching 1 as $s \to \infty$), there exists an element in C^{440} which sends one tuple to the other. Therefore, the set C^{440} contains almost all elements in some conjugacy class B of permutations in $\mathrm{Alt}(N)$ with at least $K^5/10$ nonfixed points.

The vector v is almost preserved by any element of C, which implies that v is moved little by most of the elements inside the conjugacy class B, i.e., $\|\rho(g)v - v\| \leq 440 \times 1000\epsilon$ for any $g \in B \cap C^{440}$. This gives

$$\begin{aligned}\left\| \frac{1}{|B|} \sum_{g \in B} \rho_1(g) v_1 - v_1 \right\| &\leq \frac{1}{|B|} \sum_{g \in B} \|\rho(g)v - v\| \\ &\leq 2(1-\kappa)\|v_1\| + \frac{1}{|B|} \sum_{g \in B \cap C^{440}} \|\rho(g)v - v\| \\ &< \frac{\|v_1\|}{6} + 4.5 \times 10^5 \epsilon,\end{aligned}$$

provided that κ is sufficiently close to 1. The decomposition of $\mathcal{H}_1$ as

$$\mathcal{H}_1 = \bigoplus_{\lambda} c_\lambda M^\lambda$$

gives a decomposition of the vector $v_1 = \sum v_\lambda$. The set B is a conjugacy class; therefore, $\frac{1}{|B|} \sum_{g \in B} \rho(g) v_\lambda = \bar{\chi}_\lambda(B) v_\lambda$ for any vector v_λ in an irreducible representation M^λ. Here $\bar{\chi}_\lambda(B)$ is the normalized character of the representation M^λ, defined as $\bar{\chi}_\lambda(B) := \chi_\lambda(B)/\dim M^\lambda$. Thus we have

$$\left\| \frac{1}{|B|} \sum_{g \in B} \rho_1(g) v_1 \right\| \leq \|v_1\| \max_{\lambda} |\bar{\chi}_\lambda(B)|,$$

where the maximum is taken over all partitions which appear in the representation ρ_1, i.e., all partitions λ with $\lambda_1 < N - K^{5/4}$. There are various estimates of the values of the normalized characters of the symmetric/alternating groups. Applying the bounds from [26], Theorem 1 yields

$$\begin{aligned}\max_{\lambda} |\bar{\chi}_\lambda(B)| &\leq \max_{\lambda} \left\{ \max\{\lambda_1/N, q\}^{c\,\mathrm{supp}|B|} \right\} \\ &\leq \left(1 - \frac{K^{\frac{5}{4}}}{K^6}\right)^{\frac{cK^5}{10}} \leq \exp\left(-\frac{cK^{\frac{1}{4}}}{10}\right) < \frac{1}{3},\end{aligned}$$

where c and q are universal constants. The last inequalities are valid only if K is large enough. The two inequalities above imply that

$$\|v_1\| < 9 \times 10^5 \epsilon. \tag{1}$$

The above argument does not work for the representation $\mathcal{H}_2$, because the first part of the partition λ can be close to N. This means that the sum

$$\lambda_2 + \lambda_3 + \cdots < K^{5/4}$$

is small. Therefore, $\mathcal{H}_2$ can be embedded in the representation M arising from the action of $\mathrm{Alt}(N)$ on the set of all ordered tuples of size $K^{5/4}$. Let E denote the set of ordered tuples of size $K^{5/4}$ which is a basis of M.

We have $K^{K^5} \gg N^{K^{5/4}}$, i.e., the number of elements in the set C is much larger than the size of the set E. Using this inequality and the definition of the set S, it can be shown that the random walk on the set E, where the moves are given by the permutations from some subset $\widetilde{C} \subset C^6$, mixes in a few steps independent of N. Therefore, if we define the operator Δ on M by

$$\Delta := \frac{1}{|\widetilde{C}|} \sum_{g \in \widetilde{C}} \rho_2(g),$$

then Δ^8 has a single eigenvalue 1 with eigenvectors the invariant vectors in M, and all other eigenvalues are less than $1/2$ in absolute value. Thus we have:

$$||\Delta^8 v_2 - v_2|| \geq \frac{1}{2}||v_2 - v_{||}||,$$

where $v_{||}$ is the projection of v_2 onto the space of all invariant vectors in M. On the other hand,

$$||\Delta^8 v_2 - v_2|| \leq 8||\Delta v_2 - v_2|| \leq \frac{8}{|\widetilde{C}|} \sum_{g \in \widetilde{C}} ||\rho_2(g) v_2 - v_2|| \leq 48 \times 1000\epsilon,$$

which gives that

$$||v_2 - v_{||}|| < 10^5 \epsilon. \tag{2}$$

The inequalities (1) and (2) imply that

$$||v - v_{||}|| \leq ||v_1|| + ||v_2 - v_{||}|| < 10^6 \epsilon.$$

In particular, if ϵ is small enough, then $||v - v_{||}|| < 1$ and the vector $v_{||}$ is not zero, which shows that there exist invariant vectors in the representation $\mathcal{H}$. Thus, we have shown that

$$\mathcal{K}(\mathrm{Alt}(N); F_N) \geq 10^{-6},$$

which concludes the proof of Theorem 6. □

Proof of Theorem 7. By Theorem 6 the alternating groups $\mathrm{Alt}(n_s)$ are expanders with respect to some generating set F_{n_s} for $n_s = \left(2^{3s} - 1\right)^6$. The sequence $\{n_s\}_s$ grows exponentially; therefore, for any sufficiently large n there exists s such that $1 < n/n_s < 10^6$. The group $\mathrm{Alt}(n)$ can be written as a product of a fixed number (less than 10^8) of copies of $\mathrm{Alt}(n_s)$ embedded in $\mathrm{Alt}(n)$. Using the images of the sets F_{n_s} one can construct a generating set F_n such that

$$\mathcal{K}\left(\mathrm{Alt}(n); F_n\right) \geq 10^{-15}$$

and $|F_n| \leq 10^{10}$, which completes the proof of the first part of Theorem 7. The construction of the generating sets $\tilde{F}_n$ of the symmetric groups is similar. □

The generating set S of $\mathrm{SL}_{3s}(\mathbb{F}_2)$ can be defined so that all elements of S are involutions. This allows us to construct an expanding generating set F_n that consists only of involutions.

The bounds for the size of the generating set F_n and the Kazhdan constant in the proof of Theorem 7 can be significantly improved — it is possible to construct a 10 element generating set $\bar{F}_n$ consisting of involutions such that $\mathcal{K}\left(\mathrm{Alt}(n); \bar{F}_n\right) \geq 10^{-8}$, provided that n is large enough. N. Nikolov [24] suggested that it is possible to further improve the bound for the Kazhdan constant by using the groups $\mathrm{SL}_3(\mathbb{F}_q)$ instead of $\mathrm{SL}_{3s}(\mathbb{F}_2)$, but this will double the size of the generating set.

Acknowledgements

I wish to thank Alex Lubotzky and Nikolay Nikolov for their encouragement and useful discussions during the work on this project. I am also very grateful to Yehuda Shalom and Efim Zelmanov for introducing me to the subject.

References

[1] M. Abért, *Symmetric groups as products of abelian subgroups*, Bull. London Math. Soc. **34** (2002), no. 4, 451–456. MR1897424 (2002m:20006)

[2] N. Alon, A. Lubotzky, and A. Wigderson, *Semi-direct product in groups and zig-zag product in graphs: connections and applications (extended abstract)*, 42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001), IEEE Computer Soc., Los Alamitos, CA, 2001, pp. 630–637. MR1948752

[3] N. Alon and Y. Roichman, *Random Cayley graphs and expanders*, Random Structures Algorithms **5** (1994), no. 2, 271–284. MR1262979 (94k:05132)

[4] L. Babai, G. Hetyei, W. M. Kantor, A. Lubotzky, and Á. Seress, *On the diameter of finite groups*, 31st Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990), IEEE Comput. Soc. Press, Los Alamitos, CA, 1990, pp. 857–865. MR1150735

[5] 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)

[6] M. Burger, *Kazhdan constants for* $\mathrm{SL}(3,\mathbb{Z})$, J. Reine Angew. Math. **413** (1991), 36–67. MR1089795 (92c:22013)

[7] R. Gilman, *Finite quotients of the automorphism group of a free group*, Canad. J. Math. **29** (1977), no. 3, 541–551. MR0435226 (55:8186)

[8] M. Kassabov, *Kazhdan constants for* $\mathrm{SL}_n(\mathbb{Z})$, `arXiv:math.GR/0311487`.

[9] M. Kassabov, *Symmetric groups and expanders*, in preparation.

[10] M. Kassabov, *Universal lattices and unbounded rank expanders*, `arXiv:math.GR/0502237`.

[11] M. Kassabov and N. Nikolov, *Finite simple groups and expanders*, in preparation.

[12] M. Kassabov and T. R. Riley, *Diameters of Cayley graphs of* $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$, `arXiv:math.GR/0502221`.

[13] D. A. Kazhdan, *On the connection of the dual space of a group with the structure of its closed subgroups*, Funktsional. Anal. i Prilozhen. **1** (1967), 71–74. MR0209390 (35:288)

[14] Z. Landau and A. Russell, *Random Cayley graphs are expanders: a simple proof of the Alon-Roichman theorem*, Electron. J. Combin. **11** (2004), no. 1, Research Paper 62, 6 pp. (electronic). MR2097328

[15] P. Loh and L. Schulman, *Improved expansion of random cayley graphs*, Disc. Math. and Theor. Comp. Sci. **6** (2004), 523–528. MR2097328

[16] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277. MR963118 (89m:05099)

[17] A. 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)

[18] A. Lubotzky, *private communication.*

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

[20] A. Lubotzky, *Cayley graphs: eigenvalues, expanders and random walks*, Surveys in combinatorics, 1995 (Stirling), London Math. Soc. Lecture Note Ser., vol. 218, Cambridge Univ. Press, Cambridge, 1995, pp. 155–189. MR1358635 (96k:05081)

[21] A. Lubotzky and I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363 (electronic). MR1815215 (2003d:60012)

[22] A. Lubotzky and A. Żuk, *On property* τ, preprint. `http://www.ma.huji.ac.il/ alexlub/BOOKS/On%20property/On%20property.pdf`

[23] G. A. Margulis, *Explicit constructions of expanders*, Problemy Peredachi Informatsii **9** (1973), no. 4, 71–80. MR0484767 (58:4643)

[24] N. Nikolov, *private communication.*

[25] O. Reingold, S. Vadhan, and A. Wigderson, *Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors (extended abstract)*, 41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000), IEEE Comput. Soc. Press, Los Alamitos, CA, 2000, pp. 3–13. MR1931799

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

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

[28] E. Rozenman, Aner Shalev, and Avi Wigderson, *A new family of Cayley expanders*, Proceedings of the 36th Annual ACM Symposium on Theory of Computing, 445–454 (electronic), ACM, New York, 2004. MR2121630

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

Department of Mathematics, Cornell University, Ithaca, New York 14853-4201
E-mail address: kassabov@math.cornell.edu