Expansion in $SL_d(\mathbf{Z}/q\mathbf{Z})$, q arbitrary

Jean Bourgain[*]and Péter P. Varjú[†]

July 2, 2010

Abstract

Let S be a fixed finite symmetric subset of $SL_d(\mathbf{Z})$, and assume that it generates a Zariski-dense subgroup G. We show that the Cayley graphs of $\pi_q(G)$ with respect to the generating set $\pi_q(S)$ form a family of expanders, where π_q is the projection map $\mathbf{Z} \to \mathbf{Z}/q\mathbf{Z}$.

1 Introduction

Let $\mathcal{G}$ be a graph, and for a set of vertices $X \subset V(\mathcal{G})$, denote by ∂X the set of edges that connect a vertex in X to one in $V(\mathcal{G})\backslash X$. Define

$$c(\mathcal{G}) = \min_{X \subset V(\mathcal{G}),\ |X| \le |V(\mathcal{G})|/2} \frac{|\partial X|}{|X|},$$

where $|X|$ denotes the cardinality of the set X. A family of graphs is called a family of expanders, if $c(\mathcal{G})$ is bounded away from zero for graphs $\mathcal{G}$ that belong to the family. Expanders have a wide range of applications in computer science (see e.g. Hoory, Linial and Widgerson [19] for a recent survey on expanders) and recently they found remarkable applications in pure mathematics as well (see Bourgain, Gamburd and Sarnak [7] and Long, Lubotzky and Reid [22]). For further motivation, we refer to these papers.

Let G be a group and let $S \subset G$ be a symmetric (i.e. closed for taking inverses) set of generators. The Cayley graph $\mathcal{G}(G,S)$ of G with respect to the generating set S is defined to be the graph whose vertex set is G, and in which two vertices $x, y \in G$ are connected exactly if $y \in Sx$. Let q be a positive integer, and denote by $\pi_q : \mathbf{Z} \to \mathbf{Z}/q\mathbf{Z}$ the residue map. π_q induces maps in a natural way in various contexts, we always denote these maps by π_q. Consider a fixed symmetric $S \subset SL_d(\mathbf{Z})$ and assume that it generates a group G which is Zariski-dense in SL_d. The purpose of this paper is to show that for any such fixed set S and for q running through the integers, the family of Cayley graphs $\mathcal{G}(SL_d(\mathbf{Z}/q\mathbf{Z}), \pi_q(S))$ is an expander family. More precisely we prove

[*] Supported by the NSF grants DMS-0808042 and DMS-0835373

[†] Supported by the Fulbright Science and Technology Award 15073240

Theorem 1. *Let $S \subset SL_d(\mathbf{Z})$ be finite and symmetric. Assume that S generates a subgroup $G < SL_d(\mathbf{Z})$ which is Zariski dense in SL_d.*

Then $\mathcal{G}(\pi_q(G), \pi_q(S))$ form a family of expanders, when S is fixed and q runs through the integers. Moreover, there is an integer q_0 such that $\pi_q(G) = SL_d(\mathbf{Z}/q\mathbf{Z})$ if q is prime to q_0.

We remark that if G is not Zariski dense, then $\pi_q(S)$ does not generate $SL_d(\mathbf{Z}/q\mathbf{Z})$ for any q. Several papers are devoted to the study of this problem, see [4]–[7], [28], each obtaining the above statement in some special cases. More precisely, [4] established the case when $d = 2$ and q is prime, [5]–[6] deals with moduli $q = p^m$ the powers of fixed prime p, and [7] settled the case when $d = 2$ and q is square-free. In [28] the statement was proved for any d when q restricted to the set of square-free integers under the assumption that there is a $\delta > 0$ depending on d such that for any prime p and for any generating set $A \subset SL_d(\mathbf{Z}/p\mathbf{Z})$, we have

$$|A.A.A| \geq \min\{|A|^{1+\delta}, SL_d(\mathbf{Z}/p\mathbf{Z})\}. \tag{1}$$

Here, and everywhere in this paper we write $A.B$ for the set of all products gh where $g \in A$ and $h \in B$. Helfgott proved (1) first for $d = 2$ [16, Key Proposition] and later for $d = 3$ [17, Main Theorem]. Very recently Breuillard, Green and Tao; and Pyber and Szabó obtained this result in great generality, in particular for arbitrary d. For further details we refer to the papers [9] and [24]. Therefore combining the result of [9] or [24] with [28], we now have unconditionally the following

Theorem A (Breuillard-Green-Tao;Pyber-Szabó;Varjú)**.** *Let $S \subset SL_d(\mathbf{Z})$ be finite and symmetric. Assume that S generates a subgroup $G < SL_d(\mathbf{Z})$ which is Zariski dense in SL_d.*

Then there is an integer q_0 such that $\mathcal{G}(SL_d(\mathbf{Z}/q\mathbf{Z}), \pi_q(S))$ form a family of expanders when S is fixed and q ranges over square-free integers prime to q_0.

We are going to use the above theorem as a black box in our proof as well as the following result. Consider a group $G < SL_d(\mathbf{R})$. We say that it is strongly irreducible, if any subspace of $\mathbf{R}^d$ which is invariant under some finite index subgroup of G is either of dimension 0 or d. We say that G is proximal if there is an element $g \in G$ with a unique eigenvalue of maximal modulus, and this eigenvalue is of multiplicity one. If $G < SL_d(\mathbf{Z})$, then we can study its action on the torus $\mathbf{R}^d/\mathbf{Z}^d$. Bourgain, Furman, Lindenstrauss and Moses [3] proved a strong quantitative estimate about the equidistribution of orbits of this action.

Theorem B (Bourgain, Furman, Lindenstrauss, Moses)**.** *Let $G < SL_d(\mathbf{Z})$ be strongly irreducible and proximal, and let ν be a probability measure supported on a finite set of generators of G.*

Then for any $0 < \lambda < \lambda_1(\nu)$ there is a constant $C = C(\nu, \lambda)$ so that if for some $a \in \mathbf{R}^d/\mathbf{Z}^d$ and $b \in \mathbf{Z}^d \backslash \{0\}$, we have

$$\int_g e(\langle ga, b\rangle) d\nu^{(l)}(g) > t > 0, \quad \text{with} \quad l > C \log(2\|b\|/t),$$

then a admits a rational approximation

$$\|a - p/q\| < e^{-\lambda l} \quad \text{with} \quad |q| < (2\|b\|/t)^C.$$

Here $\nu^{(l)}$ denotes the l-fold convolution of the measure ν, and $e(x)$ is the usual shorthand for the function $e^{2\pi i x}$.

We point out that our argument is independent of the papers [5]–[6], hence we give an alternative proof for the case when the moduli $q = p^m$ are the powers of a fixed prime. We also remark that in a subsequent paper of Salehi Golsefidy and the second author [25], Theorem A will be generalized to the case when G is not Zariski dense, but the connected component of its Zariski closure is perfect. The only difficulty which prevents us from relaxing the requirement of Zariski density in Theorem 1 is that the adjoint representation, for which we apply Theorem B, is neither irreducible nor proximal in general. It is an open problem if the Cayley graphs of $SL_n(\mathbf{Z}/q\mathbf{Z})$ form an expander family when the generators are arbitrary, not necessarily the projections of a fixed subset of $SL_n(\mathbf{Z})$. A partial result in this direction is given in [8]. Expanding properties of groups of Lie type with respect to random generators are studied in [10]–[11].

2 Notation and outline of the proof

We introduce some notation that will be used throughout the paper. We use Vinogradov's notation $x \ll y$ as a shorthand for $|x| < Cy$ with some constant C. Let G be a discrete group. The unit element of any multiplicatively written group is denoted by 1. For given subsets A and B, we denote their product-set by

$$A.B = \{gh \,|\, g \in A, h \in B\},$$

while the k-fold iterated product-set of A is denoted by $\prod_k A$. We write $\widetilde{A}$ for the set of inverses of all elements of A. We say that A is symmetric if $A = \widetilde{A}$. The number of elements of a set A is denoted by $|A|$. The index of a subgroup H of G is denoted by $[G : H]$. Occasionally (especially when a ring structure is present) we write groups additively, then we write

$$A + B = \{g + h \,|\, g \in A, h \in B\}$$

for the sum-set of A and B, $\sum_k A$ for the k-fold iterated sum-set of A and 0 for the unit element.

If μ and ν are complex valued functions on G, we define their convolution by

$$(\mu * \nu)(g) = \sum_{h \in G} \mu(gh^{-1})\nu(h),$$

and we define $\widetilde{\mu}$ by the formula

$$\widetilde{\mu}(g) = \mu(g^{-1}).$$

We write $\mu^{(k)}$ for the k-fold convolution of μ with itself. As measures and functions are essentially the same on discrete sets, we use these notions interchangeably, we will also use the notation

$$\mu(A) = \sum_{g\in A} \mu(g).$$

A probability measure is a nonnegative measure with total mass 1. Finally, the normalized counting measure on a finite set A is the probability measure

$$\chi_A(B) = \frac{|A \cap B|}{|A|}.$$

We write $\Gamma = SL_d(\mathbf{Z})$ and denote by Γ_q the kernel of $\pi_q : SL_d(\mathbf{Z}) \to SL_d(\mathbf{Z}/q\mathbf{Z})$

The proof of Theorem 1 follows the same lines as in any of the papers [4]–[7], [28]. This approach goes back to Sarnak and Xue [26]; and Bourgain and Gamburd [4]. The new ingredient is the following

Proposition 2. *Let $S \subset \Gamma$ be symmetric, and assume that it generates a group G which is Zariski-dense in SL_d. Then for any $\varepsilon > 0$ there is a $\delta > 0$ such that the following hold. If $A \subset \Gamma$ is symmetric and Q and l are integers satisfying*

$$\chi_S^{(l)}(A) > Q^{-\delta}, \quad l > \delta^{-1}\log Q \quad \text{and} \quad |\pi_Q(A)| < |\Gamma/\Gamma_Q|^{1-\varepsilon}, \tag{2}$$

then $|A.A.A| > |A|^{1+\delta}$.

For the reader's convenience we include an outline how Proposition 2 implies Theorem 1. More details can be found in any of the papers [4]–[7], [28], in particular see sections 3.1 and 5 in [28]. One ingredient is [28, Lemma 15] that we recall now, because it will be also used later. It is based on the noncommutative version of the Balog–Szemerédi–Gowers theorem, and is essentially contained in [4].

Lemma C (Bourgain, Gamburd)**.** *Let μ and ν be two probability measures on an arbitrary group G and let $K > 2$ be a number. If*

$$\|\mu * \nu\|_2 > \frac{\|\mu\|_2^{1/2}\|\nu\|_2^{1/2}}{K}$$

then there is a symmetric set $S \subset G$ with

$$\frac{1}{K^R\|\mu\|_2^2} \ll |S| \ll \frac{K^R}{\|\mu\|_2^2},$$

$$|\textstyle\prod_3 S| \ll K^R|S| \quad \text{and}$$

$$\min_{g\in S} (\widetilde{\mu} * \mu)(g) \gg \frac{1}{K^R|S|},$$

where R and the implied constants are absolute.

Proof of Theorem 1. First we note that by the Tits alternative [27, Theorem 3], there is a free subgroup $G' < G$ that is Zariski dense in SL_d. In light of [19, Claim 11.19], it is enough to prove the theorem for any set of generators of G', in particular we can assume that S generates a free group.

Denote by $T = T_q$ the convolution operator by $\chi_{\pi_q(S)}$ in the regular representation of Γ/Γ_q. I.e. we write $T(\mu) = \chi_{\pi_q(S)} * \mu$ for $\mu \in l^2(\Gamma/\Gamma_q)$. We will show that there are constants $c < 1$ and $C \geq 1$ independent of q such that T has at most C eigenvalues larger than c. If $\mu \in l^2(\Gamma/\Gamma_q)$ is constant on cosets of $G/(G\cap\Gamma_q)$, then $T(\mu) = \mu$, hence $[\Gamma/\Gamma_q : G/(G\cap\Gamma_q)] < C$. Consider $\Gamma/\Gamma_{q_1\cdots q_k}$ for such relatively prime integers q_i for which $[\Gamma/\Gamma_{q_i} : G/(G\cap\Gamma_{q_i})] > 1$. Our claim implies $k < C$, so if q_0 is the product of a maximal family of such q_i, then $\pi_q(S)$ indeed generates Γ/Γ_q when q is prime to q_0. Moreover, consider the subspace $l_0^2(G/(G\cap\Gamma_q)) \subset l^2(\Gamma/\Gamma_q)$, i.e. the space of functions supported on $G/(G\cap\Gamma_q)$ with integral 0. This space is invariant for T and by a result of Dodziuk [13]; Alon [1]; and Alon and Milman [2] (see also [19, Theorem 2.4]) $\mathcal{G}(G/(G\cap\Gamma_q), \pi_q(S))$ is a family of expanders if and only if we have $\lambda < c < 1$ for all eigenvalues of T on $l_0^2(G/(G\cap\Gamma_q)) \subset l^2(\Gamma/\Gamma_q)$ for some constant c independent of q. This follow from our claim, since all eigenvalues of T_{q_1} is an eigenvalue of T_{q_2} when $q_1|q_2$, and the second eigenvalue of a connected graph is less than 1.

Consider an eigenvalue λ of T, and let μ be a corresponding eigenfunction. Consider the irreducible representations of Γ/Γ_q; these are subspaces of $l^2(\Gamma/\Gamma_q)$ invariant under T. We can assume that the irreducible representation ρ that contains μ is faithful, otherwise we can consider the quotient by the kernel, and we can replace q by a smaller integer. By [5, Lemma 7.1] any faithful representation of $SL_2(\mathbf{Z}/q\mathbf{Z})$ is of dimension at least $q/3$. Considering the restriction of a faithful representation of Γ/Γ_q to an appropriate subgroup isomorphic to $SL_2(\mathbf{Z}/q\mathbf{Z})$, we can get the same bound. This in turn implies that the multiplicity of λ in T is at least $q/3$, since the regular representation $l^2(\Gamma/\Gamma_q)$ contains $\dim(\rho)$ irreducible components isomorphic to ρ.

Using this bound for the multiplicity, we can bound $\lambda^{(2l)}$ by computing the trace of T^{2l} in the standard basis:

$$\lambda^{2l} \leq \frac{3}{q}\mathrm{Tr}(T^{2l}) = \frac{3}{q}|\Gamma/\Gamma_q|\|\pi_q[\chi_S^{(l)}]\|_2^2,$$

where $\|\cdot\|_2$ denotes the l^2 norm over the finite set Γ/Γ_q. This proves the theorem, if we can show that

$$\|\pi_q[\chi_S^{(l)}]\|_2 \ll |\Gamma/\Gamma_q|^{-1/2+1/10d^2}$$

for some $l \ll \log q$. For this, we first note that there is an integer $l_0 \geq c_0 \log q$ (if q is large enough) such that all entries of all elements of $\prod_{2l_0} S$ is less then q. Then for $g \in \prod_{2l_0} S$, $\pi_q(g) = 1$ implies $g = 1$. By Kesten's bound [20] we get

$$\pi_q[\chi_S^{(2l_0)}](1) \leq \left(\frac{4|S|-4}{|S|^2}\right)^{l_0}. \tag{3}$$

This in turn implies
$$\|\pi_q[\chi_S^{(2l_0)}]\|_2 \ll |\Gamma/\Gamma_q|^{\varepsilon}$$
for some $\varepsilon > 0$ depending on c_0 and $|S|$. Next we claim that there is a $\delta = \delta(\varepsilon) > 0$ such that if
$$\|\pi_q[\chi_S^{(2l)}]\|_2 > |\Gamma/\Gamma_q|^{-1/2+1/10d^2},$$
with $l > \delta^{-1}\log q$ then
$$\|\pi_q[\chi_S^{(4l)}]\|_2 < \|\pi_q[\chi_S^{(2l)}]\|_2^{1+\delta}. \tag{4}$$
Applying this repeatedly we can get the theorem.

Assume to the contrary that (4) does not hold. Then using Lemma C, we get that there is a symmetric set $A \subset \Gamma$ with
$$\chi_S^{(4l)}(A) > q^{-\delta_2} \quad \text{and} \quad |\pi_q(A)| < |\Gamma/\Gamma_q|^{1-1/10d^2}$$
and $|A.A.A| < |A|^{1+\delta_2}$, where we can make δ_2 arbitrarily small if the δ for which (4) does not hold is small enough. This contradicts to Proposition 2. □

The rest of the paper is devoted to the proof of Proposition 2. From now on S, A, Q, l, and ε will be fixed and we assume that they satisfy the hypothesis of the proposition. We also assume that δ is sufficiently small, and it will depend on S and ε. We aim to prove that
$$|\pi_Q(A.A\ldots A)| \geq |\Gamma/\Gamma_Q|^{1-\varepsilon/2},$$
where the number of factors in the product set $A.A\ldots A$ is bounded by a constant depending on S and ε. This proves the proposition, since by [16, Lemma 2.2] we have
$$|\textstyle\prod_l A| < \left(\frac{|A.A.A|}{|A|}\right)^{l-2}|A|. \tag{5}$$

There are some key properties of the groups Γ/Γ_Q that we will use in several places in the paper. These were also exploited in the papers [4], [5], [12] and [14]. For on integer q, denote by $\mathfrak{sl}_d(\mathbf{Z}/q\mathbf{Z})$ the $d\times d$ matrices with trace 0 and entries in $\mathbf{Z}/q\mathbf{Z}$, and we write $[u,v] = uv - vu$ for the Lie-bracket of $u, v \in \mathfrak{sl}_d(\mathbf{Z}/q\mathbf{Z})$. For $g \in \Gamma$ and integers $q_1|q_2$, write
$$\Psi_{q_1}^{q_2}(g) = \pi_{q_2/q_1}\left(\frac{g-1}{q_1}\right).$$
It is an easy calculation to check that if $q_2|q_1^2$, then
$$\Psi_{q_1}^{q_2} : \Gamma_{q_1}/\Gamma_{q_2} \to \mathfrak{sl}_d(\mathbf{Z}/(q_2/q_1)\mathbf{Z})$$
is a bijection and satisfies the following identities:
$$\Psi_{q_1}^{q_2}(xy) = \Psi_{q_1}^{q_2}(x) + \Psi_{q_1}^{q_2}(y), \tag{6}$$
$$\Psi_{q_1}^{q_2}(gxg^{-1}) = \pi_{q_2/q_1}(g)\Psi_{q_1}^{q_2}(x)\pi_{q_2/q_1}(g^{-1}), \tag{7}$$

for integers $q_1|q_2|q_1^2$, $x, y \in \Gamma_{q_1}$ and $g \in \Gamma$, furthermore

$$\Psi_{q_1 q_2}^{q_1 q_2 q_3}(xyx^{-1}y^{-1}) = [\Psi_{q_1}^{q_1 q_3}(x), \Psi_{q_2}^{q_2 q_3}(y)], \tag{8}$$

for integers q_1, q_2, q_3 with $q_3|q_1$ and $q_3|q_2$ and for $x \in \Gamma_{q_1}$ and $y \in \Gamma_{q_2}$.

We introduce some further notation that will be used henceforth. Write

$$Q = \prod_{p|Q} p^{m_p}$$

for the factorization of Q. If $q|Q$ and $p|q$ is a prime, we write

$$E_p(q) = \max_{m:p^m|q} \frac{m}{m_p} \quad \text{and} \quad w(q) = \sum_{p|q} m_p \log p.$$

Intuitively, $w(q)$ measures, "how large piece" of Q we can recover from q by taking a sufficiently high power of it. Finally if a is an integer, or more generally a vector or matrix with integral entries, then we write $q\|a$ if $q|a$ and $pq \nmid a$ for any prime $p|q$.

3 Primes with small exponents

In this section we prove Proposition 2 in the case, when the exponents of the prime factors of Q are bounded. Set

$$Q_s = \prod_{p|Q:m_p \le L} p,$$

where L is an integer whose value will be set later depending on ε, S and Q, but it can be bounded by a constant depending on ε and S only. We prove

Proposition 3. *Let $S \subset \Gamma$ be symmetric, and assume that it generates a group G which is Zariski-dense in SL_d. Then for any $\varepsilon_1 > 0$ there is a $\delta_1 > 0$ such that the following hold. If $A \subset \Gamma$ is symmetric and Q and l are sufficiently large integers satisfying*

$$\chi_S^{(l)}(A) > Q^{-\delta_1} \quad \text{and} \quad l > \delta_1^{-1} \log Q$$

then there is an integer $q_0 < Q^{\varepsilon_1}$ such that

$$(\textstyle\prod_{C(d,L)} A).\Gamma_{Q_s^L} \supset \Gamma_{q_0^L}$$

holds for any integer L.

In this section we assume that any prime divisor of Q_s is larger than a sufficiently large constant. The general case follow from this, if we make q_0 bigger. This proposition can be quite easily deduced from Theorem A, but we also need two Lemmata about the groups Γ/Γ_{p^2}.

Lemma 4. *Let p be a prime, $\psi : \Gamma/\Gamma_p \to \Gamma/\Gamma_{p^2}$ be any function such that $\pi_p \circ \psi = Id$. Choose two elements $x, y \in \Gamma/\Gamma_p$ at random independently with uniform distribution. Then the probability of $\psi(xy) = \psi(x)\psi(y)$ is less than p^{-c} for some absolute constant $c > 0$.*

Proof. Assume that the Lemma fails for some $c > 0$. We will get a contradiction if c is small enough. Denote by ν the push-forward of χ_{Γ/Γ_p} by ψ. Then $\nu * \nu(\operatorname{supp} \nu) \geq p^{-c}$. Hence

$$\|\nu * \nu\|_2 > p^{-c}|\Gamma/\Gamma_p|^{-1/2} = p^{-c}\|\nu\|_2.$$

By Lemma C, there is a symmetric $S \subset \Gamma/\Gamma_{p^2}$ such that $|S| < p^{Rc}|\Gamma/\Gamma_p|$, $\widetilde{\nu} * \nu(S) > p^{-Rc}$ and $|S.S.S| < p^{Rc}|S|$. Since $\pi_p(\widetilde{\nu} * \nu)$ is the normalized counting measure on Γ/Γ_p, we get $|\pi_p(S)| > p^{-Rc}|\Gamma/\Gamma_p|$. Any nontrivial representation of Γ/Γ_p is of dimension at least $p/3$, hence by a theorem of Gowers (see also [23, Corollary 1]) we have $\pi_p(S.S.S) = \Gamma/\Gamma_p$. Since there is no subgroup of Γ/Γ_{p^2} which is isomorphic to Γ/Γ_p, there is an element $x_0 \in (\prod_9 S) \cap \Gamma_p \backslash \Gamma_{p^2}$. The stabilizer of $\Psi_p^{p^2}(x_0)$ in Γ/Γ_p acting by conjugation on $\mathfrak{sl}_d(\mathbf{Z}/p\mathbf{Z})$ is a proper subgroup, hence is of index at least $p/3$. This shows using (7) that

$$|(\textstyle\prod_{15} S) \cap \Gamma_p| \geq |\{gx_0g^{-1} : g \in S.S.S\}| > p/3$$

and $|\prod_{18} S| > p|\Gamma/\Gamma_p|/3$. If c is sufficiently small, then in light of (5), this contradicts to $|S.S.S| < p^{Rc}|S|$ and $|S| < p^{Rc}|\Gamma/\Gamma_p|$. □

Some ideas of the proof of the following lemma is taken from [12].

Lemma 5. *Let p be a prime which is larger than a constant depending on d, and let $x \in \mathfrak{sl}_d(\mathbf{Z}/p\mathbf{Z})$ be nonzero. Then*

$$\textstyle\sum_{100d^2}\{gxg^{-1}, -gxg^{-1} : g \in \Gamma/\Gamma_p\} = \mathfrak{sl}_d(\mathbf{Z}/p\mathbf{Z}).$$

Proof. In this proof we use some special notation that we do not need elsewhere. We write $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. If x is a $d \times d$ matrix, we write $x(i,j)$ for its (i,j)'th entry, and we write $\operatorname{diag}(x)$ for the vector formed from the diagonal elements of x. If $\alpha_1, \ldots \alpha_d \in \mathbf{F}_p$, then we write $\operatorname{diag}(\alpha_1, \ldots, \alpha_d)$ for diagonal $d \times d$ matrix containing $\alpha_1, \ldots, \alpha_d$ in the diagonal. We write

$$\{\ldots\} = \{gxg^{-1}, -gxg^{-1} : g \in \Gamma/\Gamma_p\}$$

Note that $\sum_k\{\ldots\}$ is closed under conjugation by elements of Γ/Γ_p for any k. Finally, we write $E_{i,j}$ for the matrix whose (i,j)'th entry is 1 and the rest is 0. Note that

$$\{E_{i,j} : i \neq j\} \cup \{E_{i,i} - E_{i+1,i+1} : 1 \leq i < d\}$$

is a basis for $\mathfrak{sl}_d(\mathbf{F}_p)$. Replacing x by a conjugate if necessary, we can assume that $x(1,2) \neq 0$.

We show that

$$\textstyle\sum_{100}\{\ldots\} \supset \mathbf{F}_p \cdot E_{1,2}.$$

Let

$$x_1 = g_1 x g_1^{-1} - g_1^{-1} x g_1 \in \textstyle\sum_2\{\ldots\},$$

for $g_1 = \operatorname{diag}(\lambda^{-d+1}, \lambda, \lambda, \ldots, \lambda)$ with any $\lambda^d \neq \pm 1$. Then $x_1(1,2) \neq 1$ and $x(i,j) = 0$ if $i \neq 1$ or $j \neq 1$ or $i = j = 1$. Next, take

$$x_2 = g_2 x_1 g_2^{-1} + x_1 \in \textstyle\sum_4\{\ldots\},$$

where $g_2 = \operatorname{diag}(-1, -1, 1, 1, \ldots, 1)$. Then $x_2 = a_1 E_{1,2} + a_2 E_{2,1}$ with $a_1 \neq 0$. Choose elements $\lambda_3, \lambda_4, \lambda_5 \in \mathbf{F}_p$ such that $\lambda_3^{-2} + \lambda_4^{-2} + \lambda_5^{-2} = 0$ but $\lambda_3^2 + \lambda_4^2 + \lambda_5^2 \neq 0$. Define g_3, g_4, g_5 by $g_i = \operatorname{diag}(\lambda_i, \lambda_i^{-1}, 1, 1 \ldots, 1)$ and set

$$x_3 = g_3 x_2 g_3^{-1} + g_4 x_2 g_4^{-1} + g_5 x_2 g_5^{-1} \in \textstyle\sum_{12}\{\ldots\}.$$

Then $x_3 = a_3 E_{1,2}$ for some $a_3 \in E_{1,2}$. Now consider an arbitrary $a \in \mathbf{F}_p$ and let $\lambda_6, \lambda_7, \lambda_8 \in \mathbf{F}_p$ be such that $\lambda_6^2 + \lambda_7^2 + \lambda_8^2 = a/a_3$. Observe that

$$aE_{1,2} = g_6 x_3 g_6^{-1} + g_7 x_3 g_7^{-1} + g_8 x_3 g_8^{-1} \in \textstyle\sum_{36}\{\ldots\},$$

where $g_i = \operatorname{diag}(\lambda_i, \lambda_i^{-1}, 1, 1 \ldots, 1)$, which we wanted to show.

Notice that $E_{i,j}$ are conjugate to one another for $i \neq j$, hence we have also

$$\textstyle\sum_{100}\{\ldots\} \supset \mathbf{F}_p \cdot E_{i,j},$$

for $i \neq j$. Finally note that for any $1 \leq i < d$ and $\lambda \in \mathbf{F}_p$, there is $g \in \sum_{100}\{\ldots\}$ such that $\operatorname{diag}(g) = \operatorname{diag}(\lambda E_{i,i} - \lambda E_{i+1,i+1})$. For example

$$\operatorname{diag}((1 - E_{2,1}) E_{1,2} (1 - E_{2,1})^{-1}) = \operatorname{diag}(E_{1,1} - E_{2,2}).$$

This finishes the proof, since

$$\{E_{i,j} : i \neq j\} \cup \{E_{i,i} - E_{i+1,i+1} : 1 \leq i < d\}$$

is a basis for $\mathfrak{sl}_d(\mathbf{F}_p)$. □

Proof of Proposition 3. As in the proof of Theorem 1 we consider the convolution operator $T(\mu) = \chi_{\pi_{Q_s}(S)} * \mu$ on $l^2(\Gamma/\Gamma_{Q_s})$. As we mentioned there, the expander property of the graphs $\mathcal{G}(\Gamma/\Gamma_{Q_s}, \pi_{Q_s}(S))$ is equivalent to the existence of a constant $c > 0$ such that the second largest eigenvalue of T is less than c. Then by Theorem A, if l is a large constant multiple of $\log Q$ (i.e. if δ_1 is small enough), we have

$$\|\chi^{(l)}_{\pi_{Q_s}(S)} - \chi_{\Gamma/\Gamma_{Q_s}}\|_2 < |\Gamma/\Gamma_{Q_s}|^{-1},$$

whence

$$\chi_S^{(l)}(g\Gamma_{Q_s}) < 2|\Gamma/\Gamma_{Q_s}|^{-1}$$

for any $g \in \Gamma$. This implies $|\pi_{Q_s}(A)| > |\Gamma/\Gamma_{Q_s}| Q^{-\delta_1}/2$.

Write $Q_s = p_1 \cdots p_n$ for the factorization of Q_s. One can show (see [7, Lemma 5.2]) that there is a set $A' \subset A$ such that for any $g \in A'$ and for any $0 \leq i < n$ we have

$$|\{x \in \Gamma/\Gamma_{p_{i+1}} |\ \exists h \in A' \ :\ \pi_{p_1 \cdots p_i}(h) = \pi_{p_1 \cdots p_i}(g) \text{ and } \pi_{p_i+1}(h) = x\}| = K_{i+1},$$

where K_i is a sequence of integers satisfying

$$|A'| = \prod_{i=1}^{n} K_i \geq (\prod_{i=1}^{n} (2 \log p_i)^{-1})|A|.$$

This means that

$$q_0 := \prod_{i:K_i<3|\Gamma/\Gamma_{p_i}|/p_i^{1/3}} p_i < Q^{6\delta_1}$$

(if Q is large enough). Since the multiplicity of an irreducible representation of Γ/Γ_p is at least $p/3$ (much better bounds are known in fact, see [18]) we get that

$$A.A.A.\Gamma_{Q_s} \supset A'.A'.A'.\Gamma_{Q_s} \supset \Gamma_{q_0}.$$

This follows from a theorem of Gowers (see also [23, Corollary 1]) which implies that $B_1.B_2.B_3 = \Gamma/\Gamma_p$ if $B_1, B_2, B_3 \subset \Gamma/\Gamma_p$, and $|B_i| > 3|\Gamma/\Gamma_p|/p_i^{1/3}$ for each i. For more details see the argument on page 26 in [28].

Write $Q'_s = Q_s/q_0$. The next step is to show that

$$(\textstyle\prod_{C(d)} A).\Gamma_{{Q'_s}^2} \supset \Gamma_{{q'_0}^2}$$

for a not too large integer q'_0. Let $\psi : \Gamma/\Gamma_{Q'_s} \to \Gamma$ be a map such that $\pi_{Q'_s} \circ \psi = Id$ and

$$\psi(\Gamma/\Gamma_{Q'_s}) \subset A.A.A.$$

We choose two elements $x, y \in \Gamma/\Gamma_{Q'_s}$ independently at random according to the uniform distribution. By Lemma 4, we have

$$\mathbb{E}(\sum_{p|Q'_s:\pi_{p^2}(\psi(x)\psi(y))=\pi_{p^2}(\psi(xy))} \log p) < \sum_{p|Q'_s} p^{-c} \log p < \varepsilon_1 \log Q/2,$$

(if Q is large enough) where $\mathbb{E}$ denotes expectation. Then there is an integer $q'_0 < Q^{\varepsilon_1/2}$ and there are elements $x, y \in \Gamma/\Gamma_{Q'_s}$ such that $\pi_{p^2}(\psi(x)\psi(y)) \neq \pi_{p^2}(\psi(xy))$ for $p|Q'_s/q'_0$. Write $Q''_s = Q'_s/q'_0$ and let

$$z = \Psi_{Q''_s}^{(Q''_s)^2}(\psi(x)\psi(y)\psi(xy)^{-1}).$$

Then $\pi_p(z) \in \mathfrak{sl}_d(\mathbf{Z}/p\mathbf{Z})$ is nonzero for every prime $p|Q''_s$. Using (6) and (7), Lemma 5 shows that

$$(\textstyle\prod_{C(d)} A).\Gamma_{(Q''_s)^2} \supset (\prod_{100d^2}\{g(\psi(x)\psi(y)\psi(xy)^{-1})g^{-1} : g \in A\}).\Gamma_{(Q''_s)^2} = \Gamma_{Q''_s}.$$

It follows from [12, Lemma 3.1 and Lemma 3.2] (see also [14]) that if $A_1, A_2 \subset \Gamma$ are sets with $A_1.\Gamma_{p^{i+k}} = \Gamma_{p^i}$ and $A_2.\Gamma_{p^{j+k}} = \Gamma_{p^j}$, then we have

$$(\textstyle\prod_2\{a_1a_2a_1^{-1}a_2^{-1} : a_1 \in A_1, a_2 \in A_2\}).\Gamma_{p^{i+j+k}} = \Gamma_{p^{i+j}}.$$

Note that if $a_1 \in A_1$ and $a_2 \in A_2$, then $\pi_{p^{i+j+k}}(a_1a_2a_1^{-1}a_2^{-1})$ depends only on $\pi_{p^{i+k}}(a_1)$ and on $\pi_{p^{j+k}}(a_2)$. This implies that if $B_1, B_2 \subset \Gamma$ are symmetric and $B_1.\Gamma_{(Q''_s)^2} = \Gamma_{Q''_s}$ and $B_2.\Gamma_{(Q''_s)^{j+1}} = \Gamma_{(Q''_s)^j}$ for some $j \geq 1$ then

$$(\textstyle\prod_4 B_1.B_2).\Gamma_{(Q''_s)^{j+2}} \supset \Gamma_{(Q''_s)^{j+1}}.$$

Iterating this we can get the proposition. □

4 Primes with large exponents

In this section we prove Proposition 2 in the case, when the exponents of the prime factors of Q are all greater than some fixed constant. Set

$$Q_l = \prod_{p|Q: m_p > L} p^{m_p},$$

where L is an integer whose value will be set later depending on ε, S and Q, but it can be bounded by a constant depending on ε and S only. We prove

Proposition 6. *Let $S \subset \Gamma$ be symmetric, and assume that it generates a group G which is Zariski-dense in SL_d. Then for any $\varepsilon_2 > 0$ and for $1 > c_2 > c_1 > 0$ there is a $\delta_2 > 0$ such that the following hold. Let $A \subset \Gamma$ be symmetric and let Q and l be integers satisfying*

$$\chi_S^{(l)}(A) > Q^{-\delta_2} \quad \text{and} \quad l > \delta_2^{-1} \log Q.$$

Assume that there is an element $x_0 \in A$ with $x_0 \in \Gamma_{Q'}$ for some $Q'|Q$ and there is an integer $q|Q_l$ with $q\|(x_0 - 1)$, $c_1 < E_p(q) < c_2$ for $p|q$, and $w(q) > w(Q_l) - c_2 \log Q$.

Then

$$|\pi_{Q_l}[(\prod\nolimits_{C(S,c_1)} A) \cap \Gamma_{Q'}]| > Q^{-\varepsilon_2 - 2c_2 d^2} Q_l^{d^2-1}.$$

Theorem B, as it is stated, is only useful to estimate Fourier coefficients close to the origin, i.e. those with $\|b\| < Q^{1/C}$. However it implies the following refined version of itself:

Lemma 7. *Let $S \subset \Gamma$ be symmetric and assume that it generates a group $G < \Gamma$ which acts a proximally and strongly irreducibly on $\mathbf{R}^d$. Assume further that any finite index subgroup of G generates the same $\mathbf{R}$-subalgebra of $Mat_d(\mathbf{R})$ as G.*

Then there is a constant c_0 depending only on S such that for any $a, b \in \mathbf{Z}^d$ we have

$$\int e(\langle \frac{ga}{q}, b \rangle) d\chi_S^{(l)}(g) \ll (q/lcm(q,b))^{-c_0},$$

if a is prime to q and $l > C \log q$ for some sufficiently large constant C.

Proof. We assume without loss of generality that b is prime to q. Denote by R the $\mathbf{R}$-subalgebra of $Mat_d(\mathbf{R})$ generated by S. Since R is generated by integral matrices, $\Lambda = Mat_d(\mathbf{Z}) \cap R$ is a lattice in R. Denote by R^* the dual space of R and by Λ^* the dual lattice, i.e. the set of functionals that take integral values on Λ. For $g \in R$ and $\varphi \in R^*$, denote by (g, φ) the pairing between them.

For an element $g \in R$ write l_g and r_g for the left and right multiplications by g in R. Let

$$S' = \{l_g, r_g | g \in S\} \subset SL(\Lambda),$$

where $SL(\Lambda)$ stands for those linear transformations of R with determinant 1 that preserves Λ. Denote by G' the subgroup of $SL(R)$ generated by S'. If $\gamma = l_{g_1} \dots l_{g_k} r_{h_1} \dots r_{h_m}$ is a typical element of G' and $h \in R$, then we write

$$\gamma.h = g_1 \cdots g_k h h_m \cdots h_1.$$

We study the action of G' on R. First we show that the action is irreducible. Assume that V is an invariant subspace, i.e. invariant under left and right multiplications by elements of G. By the very definition, this means that V is an ideal of the algebra R. Since $\mathbf{R}^d$ is a simple R module, i.e. there is no subspace of $\mathbf{R}^d$ invariant under all elements of R, by Wedderburn's theorem (see Lang [21, Corollary XVII.3.5]), R is isomorphic to the endomorphism ring of a vectorspace over a division algebra. Therefore R is simple (see Lang [21, Theorem XVII.5.5]), and V is either $\{0\}$ or R. Hence the action of G' is irreducible. Now we show that it is actually strongly irreducible. Note that G' is naturally isomorphic to the direct product $G \times G$. Then for any finite index subgroup $H' < G'$ there is a finite index subgroup $H < G$ such that $H \times H$ is contained in H' under the above isomorphism. Since H generates the same $\mathbf{R}$-algebra R as G, the same proof shows that the action of H' is irreducible, too.

Next we show that G' acts proximally. Let $g \in G$ be an element which is proximal on $\mathbf{R}^d$, and denote by λ the top eigenvalue, and by v and u^T the corresponding right and left eigenvectors with $gv = \lambda v$ and $u^T g = \lambda u^T$. Now consider the element $\gamma = l_g r_g \in G'$. It is easy to see that on $Mat_d(\mathbf{R})$ it is proximal, and vu^T is an eigenvector corresponding to the top eigenvalue λ^2. We still need to show that vu^T is in the algebra R. For this, note that the rows of $\lambda^{-k} g^k$ tend to scalar multiples of u^T, and the columns tend to scalar multiples of v. Hence $\lim_{n\to\infty} \lambda^{-k} g^k \in R$ is a scalar multiple of vu^T proving the claim.

This shows that we can apply Theorem B for the action of G' on R and for the measure $\nu = \chi_{S'}$. We actually use it for G' acting on R^*. Denote by g^* the adjoint of an element $g \in G'$ acting on R^*. We have

$$\int e((\gamma.1, \frac{\varphi}{q})) d\chi_{S'}^{(m)}(\gamma) = \int e((1, \gamma^*.\frac{\varphi}{q})) d\chi_{S'}^{(m)}(\gamma) \ll q^{-c_0},$$

where 1 is the unit element of R, and $\varphi \in \Lambda^*$ is any functional prime to q, i.e. $\varphi/p \notin \Lambda^*$ for any prime $p|q$. By Theorem B, the failure of this inequality would imply a good rational approximation of φ/q with denominator less than q, a contradiction. By induction it is easy to show that the push-forward of the measure $\chi_{S'}^{(m)}$ under the map $\gamma \mapsto \gamma.1$ is $\chi_S^{(m)}$. We define the functional $\varphi \in \Lambda^*$ by $(g, \varphi) = \langle ga, b \rangle$, where a and b are the same as in the statement of the lemma. Since a ad b are prime to q, so is φ. Then we get

$$\int e((\gamma.1, \frac{\varphi}{q})) d\chi_{S'}^{(m)}(\gamma) = \int e(\langle \frac{ga}{q}, b \rangle) d\chi_S^{(m)}(g)$$

proving the lemma. □

Corollary 8. *Let $S \subset \Gamma$ be symmetric, and assume that it generates a group G which is Zariski-dense in SL_d. Then for any $\varepsilon > 0$ there is a $\delta > 0$ such that the following hold. Let $A \subset \Gamma$ be symmetric and let Q and l be integers satisfying*

$$\chi_S^{(l)}(A) > Q^{-\delta} \quad \text{and} \quad l > \delta^{-1} \log Q.$$

Then for any integer $q|Q$ and for any $v_0 \in \mathfrak{sl}_d(\mathbf{Z}/q\mathbf{Z})$ such that $p \nmid v_0$ for any prime $p|q$, we have

$$|\pi_q[\textstyle\sum_{C(S)}\{gv_0g^{-1} : g \in A\}]| > Q^{-\varepsilon} q^{d^2-1}.$$

Proof. We apply Lemma 7 for the adjoint action of G on the Lie-algebra $\mathfrak{sl}_d(\mathbf{R})$, i.e. $g \in G$ acts by $x \mapsto gxg^{-1}$. Denote by ν the push-forward of $\chi_S^{(l)}$ via the map $g \mapsto \pi_q(gv_0g^{-1})$. Then Lemma 7 gives the following bound for the Fourier coefficients of ν:

$$\widehat{\nu}(b) \ll (q/lcm(q,b))^{-c_0}.$$

Denote by $\nu^{[C]}$ the C-fold additive convolution of ν with itself. Then there is a constant $C = C(S)$ such that

$$(\nu^{[C]})\widehat{\ }(b) \ll (q/lcm(q,b))^{-d^2}.$$

By Parseval

$$\|\nu^{[C]}\|_2^2 \ll q^{-d^2+1} \sum_{q_0|q} q_0^{d^2-1} \cdot q_0^{-2d^2} \ll q^{-d^2+1}.$$

Let now μ be the push-forward of $\chi_S^{(l)}|_A$ (the normalized restriction of $\chi_S^{(l)}$ to A) via the map $g \mapsto \pi_q(gv_0g^{-1})$. Then $\mu(x) < Q^{\delta}\nu(x)$ and hence $\mu^{[C]}(x) < Q^{C\delta}\nu^{[C]}$ for any $x \in \mathfrak{sl}_d(\mathbf{Z}/q\mathbf{Z})$. The above bound for ν gives

$$\|\mu^{[C]}\|_2^2 \ll Q^{C\delta} q^{-d^2+1}.$$

Since

$$\pi_q[\textstyle\sum_{C(S)}\{gv_0g^{-1} : g \in A\}]$$

is the support of $\mu^{[C]}$, the claim follows by Cauchy-Schwartz. □

Lemma 9. *Let $X \subset \mathfrak{sl}_d(\mathbf{Z}/q\mathbf{Z})$ be a set, and assume that $|X| > q^{d^2-1}/K$ for some $K > 2$.*

Then

$$|\textstyle\sum_{d(d-1)/2}[X - X, X - X]| \gg q^{d^2-1}/K^{3d(d-1)}.$$

Proof. Throughout the proof we assume that $2 \nmid q$, the general case requires trivial modifications only. Let $p > 2$ be a prime and for $v \in \mathfrak{sl}_2(\mathbf{Z})$ write

$$A_m(v) = \{(u_1, u_2) \in [\mathfrak{sl}_2(\mathbf{Z}/p^m\mathbf{Z})]^2 | \pi_{p^m}(v) = [u_1, u_2]\}.$$

First we show that if $p^k \| v$, then

$$\begin{aligned} |A_m(v)| &= p^{3m+k} + p^{3m+k-1} - p^{3m-1} - p^{3m-2} \quad \text{if } k < m, \text{ and} \\ |A_m(0)| &= p^{4m} + p^{4m-1} + p^{4m-2} - p^{3m-1} - p^{3m-2}. \end{aligned}$$

This immediately implies the lemma for $d = 2$ even in a stronger form. We will deduce the general case from this in the second half of the proof.

Assume that we have

$$\pi_{p^m}([u_1, u_2]) = \pi_{p^m}(v) \tag{9}$$

for some $u_1, u_2, v \in \mathfrak{sl}_2(\mathbf{Z})$. If $p^l \| u_1$, then we must have $p^l | v$ and

$$\pi_{p^{m-l}}([u_1/p^l, u_2]) = \pi_{p^{m-l}}(v/p^l). \tag{10}$$

Moreover (10) is in fact equivalent to (9), hence we have

$$\begin{aligned} &|A_m(v) \cap \{(u_1, u_2) \in [\mathfrak{sl}_2(\mathbf{Z}/p^m\mathbf{Z})]^2 : p^l \| u_1\}| \\ &= p^{3l} |A_{m-l}(v/p^l) \cap \{(u_1, u_2) \in [\mathfrak{sl}_2(\mathbf{Z}/p^{m-l}\mathbf{Z})]^2 : p \nmid u_1\}|. \end{aligned}$$

For this reason we first concentrate on

$$|A_m(v) \cap \{(u_1, u_2) \in [\mathfrak{sl}_2(\mathbf{Z}/p^m\mathbf{Z})]^2 : p \nmid u_1\}|.$$

With the notation in the proof of Lemma 5, we write

$$\begin{aligned} v &= a_1E_{1,1} - a_1E_{2,2} + a_2E_{1,2} + a_3E_{2,1}, \\ u_1 &= x_1E_{1,1} - x_1E_{2,2} + x_2E_{1,2} + x_3E_{2,1} \quad \text{and} \\ u_2 &= y_1E_{1,1} - y_1E_{2,2} + y_2E_{1,2} + y_3E_{2,1}. \end{aligned}$$

Then we are looking for the number of solutions of the system of equations

$$x_2y_3 - x_3y_2 = a_1 \tag{11}$$

$$2x_1y_2 - 2x_2y_1 = a_2 \tag{12}$$

$$2x_3y_1 - 2x_1y_3 = a_3 \tag{13}$$

in $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbf{Z}/p^m\mathbf{Z}$ with $p \nmid (x_1, x_2, x_3)$. Adding $2x_1$ times (11) and x_3 times (12) to x_2 times (13), we get

$$2x_1a_1 + x_3a_2 + x_2a_3 = 0. \tag{14}$$

On the other hand if (14) holds for some fixed $p \nmid (x_1, x_2, x_3)$, then we always have p^m solutions in (y_1, y_2, y_3). Say if $p \nmid x_1$, the solutions are $y_1 = t$, $y_2 = (a_2 + 2x_2t)/2x_1$ and $y_3 = (2x_3t - a_3)/2x_1$ for $t \in \mathbf{Z}/p^m\mathbf{Z}$. A similar direct calculation shows that (14) has p^{2m+k} solutions in x_1, x_2, x_3, recall that $p^k \| (a_1, a_2, a_3)$. Out of these solutions, $(p^2 - 1)p^{2m-2+k}$ satisfies $p \nmid (x_1, x_2, x_3)$ when $k < m$, and $(p^3 - 1)p^{3m-3}$ when $m = k$. Therefore when $l \le k < m$, we have

$$|A_m(v) \cap \{(u_1, u_2) \in [\mathfrak{sl}_2(\mathbf{Z}/p^m\mathbf{Z})]^2 : p^l \| u_1\}| = p^{3m+k-l} - p^{3m-2+k-l},$$

and the claim follows by summing over $0 \le l \le k$.

Now we show how to deduce the Lemma from the claim. For $1 \le i < j \le d$, denote by $\mathfrak{h}_{i,j} \subset \mathfrak{sl}_d(\mathbf{Z}/q\mathbf{Z})$ the Lie-subalgebra spanned by $E_{i,i} - E_{j,j}, E_{i,j}$ and

$E_{j,i}$. By the pigeon hole principle, for each i,j there is a coset $a+\mathfrak{h}_{i,j}$ such that $|X\cap(a+\mathfrak{h}_{i,j})|>q^3/K$, hence $|(X-X)\cap(a+\mathfrak{h}_{i,j})|>q^3/K$. Write $Y=(X-X)\cap\mathfrak{h}_{i,j}$, and for $q_0|q$ let

$$Y_{q_0}=\{v\in[Y,Y]:q_0|v \text{ but } q_0p\nmid v \text{ for } p|q \text{ prime}\}.$$

Since

$$\prod_{p|q_0 \text{ prime}}\frac{p+1}{p}\ll\log q_0,$$

we have

$$q^6/K^2<|Y|^2<C\sum_{q_0}\log(q_0)q^3q_0|Y_{q_0}|$$

for some constant C by the above claim and the Chinese Remainder Theorem. Clearly $|Y_{q_0}|<(q/q_0)^3$, hence

$$C\sum_{q_0>C'K^2\log K}\log(q_0)q^3q_0|Y_{q_0}|<q^6/2K^2$$

for some constant C'. This gives

$$q^6/2K^2<C\sum_{q_0<C'K^2\log K}\log(q_0)q^3q_0|Y_{q_0}|$$

from where we get

$$[Y,Y]\gg\frac{q^3}{K^4\log^2K}.$$

Since $\mathfrak{sl}_d(\mathbf{Z}/q\mathbf{Z})=\mathfrak{h}_{1,2}+\ldots+\mathfrak{h}_{d-1,d}$, the lemma follows. □

Proof of Proposition 6. Recall the identities (6)–(8). Apply Corollary 8 for $v_0:=\Psi_q^{q^2}(x_0)$, and write

$$B_0:=\prod\nolimits_C\{gx_0g^{-1}:g\in A\},$$

where C is the constant from the corollary. Then $B_0\subset(\prod_{3C}A)\cap\Gamma_{qQ'}$ and $|\pi_{q^2}(B_0)|>Q^{-\varepsilon}q^{d^2-1}$. Define recursively

$$B_i=\prod\nolimits_{d(d-1)/2}\{xyx^{-1}y^{-1}:x\in B_0.\widetilde{B}_0,y\in B_{i-1}.\widetilde{B}_{i-1}\}.$$

Then $B_i\subset\Gamma_{q^{i+1}Q'}$ and we get

$$|\pi_{q^{i+2}}(B_i)|>Q^{-(3d(d-1))^i\varepsilon}q^{d^2-1},$$

if we use Lemma 9 inductively. Note that

$$B_0.B_1\ldots B_{\lceil 1/c_1\rceil}\subset(\prod\nolimits_{C(S,c_1)}A)\cap\Gamma_{Q'}$$

and

$$|\pi_{q^{\lceil 1/c_1\rceil}}(B_0.B_1\dots B_{\lceil 1/c_1\rceil})| > (\prod_i Q^{-(2d(d-1))^i\varepsilon})|\Gamma_q/\Gamma_{q^{\lceil 1/c_1\rceil}}|.$$

The assumptions on q imply

$$\begin{aligned} |\pi_{Q_l}(B_0.B_1\dots B_{\lceil 1/c_1\rceil})| &> (\prod_i Q^{-(2d(d-1))^i\varepsilon})|(\Gamma_{Q_l}\Gamma_{q^{\lceil 1/c_1\rceil}})/\Gamma_{Q_l}|^{-1}|\Gamma_q/\Gamma_{Q_l}| \\ &> (\prod_i Q^{-(2d(d-1))^i\varepsilon})Q^{-2c_2d^2}Q_l^{d^2-1} \end{aligned}$$

and this proves the proposition if we made the choice $\varepsilon = \varepsilon_2/\sum_{i\le\lceil 1/c_1\rceil}(2d(d-1))^i$. □

5 Proof of Proposition 2

Let ε, Q, l, and A be as in the proposition. Similarly to the proof of Theorem 1 (see (3)) we can show that there is a positive constant $c_3 > 0$ depending on S, such that $\chi_S^{(l)}(\Gamma_q) < q^{-c_3}$ for every $q|Q$. In the course of the proof we will use several parameters $\varepsilon_1, \varepsilon_2, c_1, c_2, L$, and L' that depend on each other and on S, ε and Q in a complicated way. We emphasize the crucial property that although the parameters depend on Q, they can be bounded by constants depending only on S and ε. We give now the definition of the parameters, but the reader may want to skip to the next paragraph and refer to the definitions when the parameters are used. First we define a sequence for each parameter recursively. Set $L^{(0)} = 1$, and once $L^{(i)}$ is defined for some $i \ge 0$, we proceed as follows: Let $\varepsilon_1^{(i+1)} = \varepsilon/4L^{(i)}d^2$ and pick $c_2^{(i+1)} < \varepsilon/8d^2$ in such a way that Proposition 3 holds with $\delta_1 = 2c_2^{(i+1)}d^2$ and $\varepsilon_1^{(i+1)}$. Now set $c_1^{(i+1)} = (c_2^{(i+1)})^2c_3/d^2$, $L^{(i+1)} = \lceil 1/c_1^{(i+1)}\rceil$. Now if

$$\prod_{p|Q:L^{(i+1)}>m_p>L^{(i)}} p^{m_p} < Q^{\varepsilon/4d^2}$$

then we stop and set $\varepsilon_1 = \varepsilon_1^{(i+1)}$, $c_1 = c_1^{(i+1)}$, $\varepsilon_2 = \varepsilon/4$, $c_2 = c_2^{(i+1)}$, $L = L^{(i+1)}$, and $L' = L^{(i)}$. Otherwise we continue with computing the next iterate of all parameters. Note that this process always ends in at most $4d^2/\varepsilon$ steps, so the constants are bounded independently of Q. We also assume that δ is sufficiently small and Q is sufficiently large depending on all these parameters. Recall that

$$Q_s = \prod_{p|Q:m_p\le L} p \quad \text{and} \quad Q_l = \prod_{p|Q:m_p>L} p^{m_p},$$

First choose an integer $q_1|Q_l$ such that $c_1 < E_p(q_1) < 2c_1$, which is possible, since $L > c_1^{-1}$, and set $A_1 = (A.A)\cap\Gamma_{q_1}$. If δ is sufficiently small, we have

$$\chi_S^{(l)}(A_1) > q_1^{-d^2} > Q^{-2c_1d^2}.$$

Next, we take an element $g_1 \in A_1$ such that $g_1 \notin \Gamma_q$ for any $q > Q^{c_2^2}$. This is possible, since $\chi_S^{(l)}(\Gamma_q) < q^{-c_3}$ and the number of q's we need to consider is at most $Q^{c_2^2 c_3}$ (if Q is large enough) and we chose our parameters in such a way that $2c_1 d^2 = 2c_2^2 c_3$. This shows that there is an integer $q|Q_l$ with $w(q) > w(Q_l) - c_2 \log Q$ and $c_1 < E_p(q) < c_2$ for $p|q$, and $q\|(g_1 - 1)$. This element g_1 will be used in the construction of x_0 to be used when we apply Proposition 6 below.

Before that, similarly as above, we choose an integer $q_2|Q_l$ such that $c_2 < E_p(q_2) < 2c_2$ and set $A_2 = (A.A) \cap \Gamma_{q_2}$. Note that $\chi_S^{(l)}(A_2) > Q^{-2c_2 d^2}$. We apply Proposition 3 for the set A_2, and we get that

$$(\textstyle\prod_{C(d,L)} A_2).\Gamma_{Q_s^L} \supset \Gamma_{q_0^L}$$

for some $q_0 < Q^{\varepsilon_1}$. This implies

$$\begin{aligned} |\pi_{Q/Q_l}(\textstyle\prod_{C(d,L)} A_2)| &> (\prod_{p|q_0} p^{m_p})^{-d^2} |\Gamma/\Gamma_{Q/Q_l}| \\ &> Q^{-\varepsilon/4} Q^{-L'\varepsilon_1 d^2} |\Gamma/\Gamma_{Q/Q_l}| \\ &= Q^{-\varepsilon/2} |\Gamma/\Gamma_{Q/Q_l}| \qquad (15) \end{aligned}$$

since our choice $\varepsilon_1 = \varepsilon/4L'd^2$ and

$$\prod_{p|Q: L > m_p > L'} p^{m_p} < Q^{\varepsilon/4d^2}.$$

Choose

$$g_2 \in (\textstyle\prod_{2C(d,L)} A_2) \cap \Gamma_{q_2}$$

with $\pi_{Q_s^L/q_0^L}(g_2) = \pi_{Q_s^L/q_0^L}(g_1)$, and take $x_0 = g_1 g_2^{-1}$. Recall that $q\|(g_1 - 1)$ with $c_1 < E_p(q) < c_2$ for $p|q$ and $g_2 \in \Gamma_{q_2}$ with $E_p(q_2) > c_2$ for $p|Q_l$, hence $q\|(x_0 - 1)$. We also have $x_0 \in \Gamma_{Q'}$ with $Q' = Q_s^L/q_0^L$. Now we can apply Proposition 6 for $A \cup \{x_0, x_0^{-1}\}$. Set

$$B = (\textstyle\prod_{C(S,c_1,L)} A) \cap \Gamma_{Q_s^L/q_0^L}.$$

Proposition 6 implies that $|\pi_{Q_l}(B)| > Q^{-\varepsilon_2 - 2c_2 d^2} Q_l^{d^2-1}$, if δ is small enough. Combine this with (15) and we finally get

$$|\pi_Q[\textstyle\prod_{C(S,\varepsilon)} A]| > |\pi_{Q_l}(B)| \cdot |\pi_{Q/Q_l}[\textstyle\prod_{C(d,L)} A]| > Q^{-\varepsilon/2 - \varepsilon_2 - 2c_2 d^2} |\Gamma/\Gamma_Q|.$$

By (5) this implies the proposition, since $\varepsilon_2 < \varepsilon/4$ and $c_2 < \varepsilon/8d^2$ and $|\pi_Q(A)| < |\Gamma/\Gamma_Q|^{1-\varepsilon}$.

References

[1] N. Alon, *Eigenvalues and expanders*, Combinatorica **6** No. 2. (1986), 83–96.

[2] N. Alon and V. D. Milman, λ_1*, isoperimetric inequalities for graphs, and superconcentrators*, J. Combin. Theory Ser. B, **38** No. 1. (1985), 73–88.

[3] J. Bourgain, A. Furman, E. Lindenstrauss, S. Moses, *Stationary measures and equidistribution for orbits of non-abelian semigroups on the torus,* preprint available online: http://www.math.princeton.edu/∼elonl/Publications/BFLM1.PDF

[4] J. Bourgain and A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $SL_2(\mathbb{F}_p)$*,* Ann. of Math. **167** (2008), 625–642.

[5] J. Bourgain and A. Gamburd, *Expansion and random walks in* $SL_d(\mathbb{Z}/p^n\mathbb{Z})$*:I,* J. Eur. Math. Soc. **10** (2008), 987–1011.

[6] J. Bourgain and A. Gamburd, *Expansion and random walks in* $SL_d(\mathbb{Z}/p^n\mathbb{Z})$*:II. With an appendix by J. Bourgain*, J. Eur. Math. Soc. **11** No. 5. (2009), 1057–1103.

[7] J. Bourgain, A. Gamburd and P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. **179** No. 3. (2010), 559–644.

[8] E. Breuillard, A. Gamburd, *Strong uniform expansion in* $\mathrm{SL}(2,p)$, preprint available online: http://arxiv.org/abs/0911.3022

[9] E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*, preprint available online: http://arxiv.org/abs/1005.1881

[10] E. Breuillard, B. Green and T. Tao, *Suzuki groups as expanders*, preprint available online: http://arxiv.org/abs/1005.0782

[11] E. Breuillard, B. Green and T. Tao, *Expansion in simple groups of Lie type*, in preparation

[12] O. Dinai, *Poly-log diameter bounds for some families of finite groups.* Proc. Amer. Math. Soc. **134** No. 11. (2006), 3137–3142.

[13] J. Dodziuk, *Difference equations, isoperimetric inequality and transience of certain random walks*, Trans. Amer. Math. Soc. **284** No. 2. (1984), 787–794.

[14] A. Gamburd, M. Shahshahani, Uniform diameter bounds for some families of Cayley graphs. Int. Math. Res. Not. No. 71. (2004), 3813–3824.

[15] W. T. Gowers, *Quasirandom Groups*, Combin. Probab. Comput. **17** (2008), 363–387.

[16] H. A. Helfgott, *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. **167** (2008), 601–623.

[17] H. A. Helfgott, *Growth in* $SL_3(\mathbb{Z}/p\mathbb{Z})$, preprint, available at http://arxiv.org/abs/0807.2027

[18] M. E. Harris and C. Hering, *On the smallest degrees of projective representations of the groups $PSL(n, q)$*, Canad. J. Math. **23** (1971) 90–102.

[19] S. Hoory, N. Linial and A. Widgerson, *Expander graphs and their applications*, Bull. Amer. Math. Soc., **43** No. 4 (2006), 439–561.

[20] H. Kesten, *Symmetric random walks on groups,* Trans. Amer. Math. Soc., **92** (1959), 336–354.

[21] S. Lang, *Algebra*, Graduate texts in mathematics, **211** Springer-Verlag, New York, 2002.

[22] D. D. Long, A. Lubotzky and A. W. Reid, *Heegaard genus and property τ for hyperbolic 3-manifolds*, J. Topol., **1** (2008), 152–158.

[23] N. Nikolov and L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem*, preprint, available at http://arxiv.org/abs/math/0703343

[24] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type of bounded rank*, preprint available online: http://arxiv.org/abs/1005.1858

[25] A. Salehi Golsefidy and P. P. Varjú, *Expansion in perfect groups*, in preparation

[26] P. Sarnak and X. X. Xue, *Bounds for multiplicities of automorphic representations*, Duke Math. J., **64** no. 1, (1991), 207–227.

[27] J. Tits, *Free subgroups in linear groups*, J. Algebra, **20** (1972), 250–270.

[28] P. P. Varjú, *Expansion in $SL_d(O_K/I)$, I square-free,* preprint available online: http://arxiv.org/abs/1001.3664

J. Bourgain
School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA
e-mail address: bourgain@math.ias.edu

P. P. Varjú
Department of Mathematics, Princeton University, Princeton, NJ 08544, USA and
Analysis and Stochastics Research Group of the Hungarian Academy of Sciences, University of Szeged, Szeged, Hungary
e-mail address: pvarju@princeton.edu