Glasgow Math. J. **57** (2015) 181–200. © Glasgow Mathematical Journal Trust 2014.
doi:10.1017/S0017089514000251.

QUASI-RANDOM PROFINITE GROUPS

MOHAMMAD BARDESTANI
Département de Mathématiques et Statistique,Université de Montréal, CP 6128, succ. Centre-ville, Montréal, QC, Canada H3C 3J7
Current address: *Department of Mathematics and Statistics, University of Ottawa, 585 King Edward, Ottawa, ON K1N 6N5, Canada*
e-mail: mbardest@uottawa.ca

and KEIVAN MALLAHI-KARAI
Jacobs University Bremen, Campus Ring I, 28759 Bremen, Germany
e-mail: k.mallahikarai@jacobs-university.de

(Received 1 October 2012; revised 30 May 2014; accepted 11 August 2014)

Abstract. Inspired by Gowers' seminal paper (W. T. Gowers, *Comb. Probab. Comput*. **17**(3) (2008), 363–387, we will investigate quasi-randomness for profinite groups. We will obtain bounds for the minimal degree of non-trivial representations of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ and $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$. Our method also delivers a lower bound for the minimal degree of a faithful representation of these groups. Using the suitable machinery from functional analysis, we establish exponential lower and upper bounds for the supremal measure of a product-free measurable subset of the profinite groups $\mathrm{SL}_k(\mathbb{Z}_p)$ and $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$. We also obtain analogous bounds for a special subgroup of the automorphism group of a regular tree.

2010 *Mathematics Subject Classification.* 20P05, 20F, 20C33

1. Introduction. A subset A of a group G is called product-free, if the equation $xy = z$ has no solution with $x, y, z \in A$. Babai and Sós [**1**] asked if every finite group G has a product-free subset of size at least $c|G|$ for a universal constant $c > 0$. This question was answered negatively by Gowers in his paper on quasi-random groups [**6**] where he proved that for sufficiently large prime p, the group $G = \mathrm{PSL}_2(\mathbb{F}_p)$ has no product-free subset of size $cn^{8/9}$, where n is the order of G. A feature of this group that plays an essential role in the proof is that the minimal degree of a non-trivial representation of G is $O(p)$. This property of G, called quasi-randomness by Gowers, is due to Frobenius and has been generalized by Landazuri and Seitz [**13**] to other families of finite simple groups of Lie type.

Apart from its intrinsic interest, this theorem has found several important applications. To name a few, Nikolov and Pyber [**15**], used Gowers' theorem to obtain an improved version of a recent theorem of Helfgott [**8**] and Shalev [**20**] on product decompositions of finite simple groups. Gowers' method has also been used in studying the image of the word maps on finite simple groups [**19**, **18**].

The focus of this paper will be quasi-randomness for compact groups and, more specifically, profinite groups. We will be interested in the family $\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))$ where $\mathbf{G}$ is either the special linear or symplectic group. Our goal is to establish a lower bound on the minimal degree of all non-trivial representations and also the minimal degree

of the faithful representations of these groups. We will then introduce the functional analytic ingredients needed to carry over Gowers' argument from finite to compact groups. These together establish that the supremal measure of a product-free set in these groups has an exponential rate of decay (as a function of rank) with explicit lower and upper bounds for the exponential rate. In the same vain, we prove an analogous result for a group of the automorphisms of the k-regular trees. Interestingly, in this case, the bounds are of the form $O(k^c)$ for a constant c. Let us first set the notations and definitions.

DEFINITION 1. *For a group G, the smallest degree among all non-trivial complex representations of G will be denoted by $m(G)$. In other words,*

$$m(G) := \min_{\rho \neq 1} d_\rho, \tag{1}$$

where the minimum is taken over all non-trivial representations of G, and d_ρ denotes for degree of the representation ρ. We say that G is k-quasi-random if $m(G) \geq k$. Similarly, we will denote

$$m_f(G) := \min_{\ker \rho = \{1\}} d_\rho,$$

where the minimum is taken over the set of all faithful representations of G.

REMARK 1. When G is a topological group, all the representations are taken to be continuous.

Our first theorem gives a lower bound for the minimal degree of all non-trivial representations of several classes of classical groups over rings $\mathbb{Z}/(p^n\mathbb{Z})$ for $p \geq 3$. This indeed extends previous work of Landazuri and Seitz, which corresponds to the case $n = 1$ in this theorem.

THEOREM 1. *For every group $\mathbf{G}$ in the first column of the table below the function on the second column (the third column, respectively) gives a lower bound for the degree of any non-trivial representation (any faithful representation, respectively) of the group $\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))$. In other words,*

$$m(\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))) \geq h(\mathbf{G}, p), \quad m_f(\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))) \geq h_f(\mathbf{G}, p, n).$$

In particular, $\mathbf{G}(\mathbb{Z}/(p^n\mathbb{Z}))$ is $O(p^r)$-quasi-random, where r is the rank of $\mathbf{G}$.

$\mathbf{G}$	$h(\mathbf{G}, p)$	$h_f(\mathbf{G}, p, n)$
$\mathbf{SL}_2$	$\frac{1}{2}(p-1)$	$\frac{1}{2}(p^n - p^{n-1})$
$\mathbf{SL}_k$	$p^{k-1} - p^{k-2}$	$(p^n - p^{n-1})p^{(k-2)n}$
$\mathbf{Sp}_{2k}$	$\frac{1}{2}(p-1)p^{k-1}$	$\frac{1}{2}(p^n - p^{n-1})p^{(k-1)n}$

It is worth mentioning that Bourgain and Gamburd [**4**] used a theorem of Clifford to find the following lower bound for $m_f(\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))$:

$$m_f(\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))) \geq \frac{p^{n-2}(p^2-1)}{2}. \tag{2}$$

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

Even though our bound is slightly weaker than the one obtained in [**4**], it is asymptotically equivalent to that. Our method is short and elementary and has also the advantage that it can be easily adapted for other classes of Chevalley groups.

As any continuous finite dimensional representation of a profinite group factors through a finite quotient, the theorem can be rephrased as a statement about the profinite groups:

THEOREM 2. *Let* $\mathbf{G}$ *be one of the groups listed in the table above and* $\mathbf{G}(\mathbb{Z}_p)$ *denote the compact group of p-adic points of* $\mathbf{G}$. *Then the degree of any non-trivial continuous representation of* $\mathbf{G}(\mathbb{Z}_p)$ *is at least* $h(\mathbf{G}, p)$.

Let G be a compact, Hausdorff and second countable topological group and μ denote the Haar measure on G, normalized so that $\mu(G) = 1$. Note that since G is compact, and hence unimodular, a left Haar measure is automatically right invariant. A measurable subset of A is said to be product-free if $A^2 \cap A = \emptyset$. We define the product-free measure as follows:

DEFINITION 2. *Let G be a compact group with normalized Haar measure* μ. *Define the product-free measure of G by*

$$\mathrm{pf}(G) = \sup\{\mu(A) : A \subseteq G \text{ is measurable}, A \cap A^2 = \emptyset\}.$$

We will extend an inequity of Babai–Nikolov–Pyber, known as "mixing inequality", which was originally proven for finite groups. Our method is to consider the compact convolution operator, and then use the spectral theorem for compact operators. Namely we will prove

THEOREM 3 (Mixing inequality). *Let G be a compact, Hausdorff, and second countable topological group such that any non-trivial complex continuous representation of G has dimension at least* $m(G)$. *Let* $f_1, f_2 \in L^2(G)$ *and suppose that at least one of* f_1, f_2 *has mean zero. Then*

$$\|f_1 * f_2\|_2 \leq \sqrt{\frac{1}{m(G)}}\|f_1\|_2\|f_2\|_2. \tag{3}$$

This theorem has an immediate corollary:

COROLLARY 1. *Let G be a compact, Hausdorff and second countable topological group such that any non-trivial complex continuous representation of G has dimension at least* $m(G)$. *Let* $A, B \subseteq G$ *be two measurable sets then,*

$$\|1_A * 1_B - \mu(A)\mu(B)\|_2 \leq \sqrt{\frac{\mu(A)\mu(B)}{m(G)}}. \tag{4}$$

For compact groups, we can establish the following analogue of Gowers' theorem [**6**]:

THEOREM 4. *Suppose G is a compact, Hausdorff and second countable topological group such that any non-trivial complex continuous representation of G has dimension at least* $m(G)$. *If* $A, B, C \subseteq G$ *such that* $\mu(A)\mu(B)\mu(C) > m(G)^{-1}$, *then the set* $AB \cap C$ *has*

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

a positive measure. Moreover, if $m(G)\mu(A)\mu(B)\mu(C) \geq \frac{1}{\eta^2}$ *then*

$$\mu\{(x, y, z) \in A \times B \times C : xy = z\} \geq (1 - \eta)\mu(A)\mu(B)\mu(C). \tag{5}$$

By Theorems 2 and 4 and a method discussed in Section 6 we can establish upper and lower bounds on the product-free measure of some profinite groups.

THEOREM 5. *The product-free measure of the profinite groups* $SL_k(\mathbb{Z}_p)$ *and* $Sp_{2k}(\mathbb{Z}_p)$ *is given by*

$$\begin{aligned}
&\frac{1}{p+1} \leq \mathrm{pf}\left(SL_2(\mathbb{Z}_p)\right) \leq \left(\frac{p-1}{2}\right)^{-1/3}, \\
&\frac{p-1}{p^k-1} \leq \mathrm{pf}\left(SL_k(\mathbb{Z}_p)\right) \leq (p^k - p^{k-1})^{-1/3}, \qquad k \geq 3. \\
&\frac{p-1}{p^{2k}-1} \leq \mathrm{pf}\left(Sp_{2k}(\mathbb{Z}_p)\right) \leq \left(\frac{1}{2}(p-1)p^{k-1}\right)^{-1/3}, \quad k \geq 2
\end{aligned} \tag{6}$$

The upper bounds have the following implication:

COROLLARY 2. *If* A *is a measurable subset of the groups* $G = \mathbf{G}(\mathbb{Z}_p)$ *as defined in Theorem 2 with* $\mu(A) > h(\mathbf{G}, p)^{-1/3}$, *then* $A^3 = G$.

Proof. For every $g \in \mathbf{G}(\mathbb{Z}_p)$, set $B = A$ and $C = gA^{-1}$. Since $\mu(A)\mu(B)\mu(C) = \mu(A)^3 > h(\mathbf{G}, p)^{-1}$, Theorems 2 and 4 show that, $AB \cap C \neq \emptyset$. If $x \in AB \cap C$ then $x = ga_3^{-1} = a_1a_2$ for $a_1, a_2, a_3 \in A$ which proves the claim. □

Using a similar method, we can obtain lower and upper bounds for a particular subgroup A^+_{k+1} of the automorphism group of a rooted regular tree. For the definition of this subgroup we refer the reader to Section 7.

THEOREM 6. *For all* $k \geq 6$ *we have*

$$\frac{1}{k+1} \leq \mathrm{pf}(A^+_{k+1}) \leq \frac{1}{(k-1)^{1/3}}. \tag{7}$$

Using a result of Green and Ruzsa [**7**], we can also compute the exact value of product-free measure of the additive group of p-adic integers. Favouring a consistent terminology, we continue to use product-free (rather than sum-free) for subsets of these additive groups.

THEOREM 7. *The product-free measure of the additive groups of p-adic integers* $\mathbb{Z}_p$ *and power series* $\mathbb{F}_p[[t]]$ *are respectively given by,*

$$\begin{aligned}
\mathrm{pf}(\mathbb{Z}_p) &= \begin{cases} 1/3 + 1/(3p) & \text{if } p \equiv 2 \mod 3 \\ 1/3 & \text{otherwise} \end{cases}. \\
\mathrm{pf}(\mathbb{F}_p[[t]]) &= \begin{cases} 1/3 + 1/(3p) & \text{if } p \equiv 2 \mod 3 \\ 1/3 & \text{if } p = 3 \\ 1/3 - 1/(3p) & \text{if } p \equiv 1 \mod 3 \end{cases}.
\end{aligned} \tag{8}$$

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

This paper is organized as follows: In Section 2, we will recall the definitions and set some notations. Moreover, in those sections we will establish some elementary properties of the product-free measure. In Section 3, we gather some facts about the representation theory of profinite groups. In Section 4, we will prove Theorem 1. Gowers' proof [**6**] uses the language of quasi-random graphs. We will translate his argument to a functional analytic language that is more suitable for dealing with compact groups. This is done in Section 5. In Section 6, we will establish the lower bounds. In Section 7, we will prove Theorem 6. Finally, in Section 8, we will prove Theorem 7.

2. Preliminaries and notations. Groups considered in this paper are all assumed to be compact, Hausdorff and second countable. In general the group operation is denoted multiplicatively; we occasionally make an exception for abelian groups and shift to the additive notation. We use μ for the normalized bi-invariant Haar measure on the group. The corresponding Lebesgue spaces will be denoted by $L^p(G)$ and the respective norm is denoted by $\|\cdot\|_p$. For a subset A of a group G, we use 1_A to denote the characteristic function of A. For subsets A and B, the product set AB is the set of all products of the form ab where $a \in A$ and $b \in B$. We also use the shorthand $A^2 = AA$. The cardinality of a finite set A will be denoted by $|A|$. The finite field with p elements is denoted by $\mathbb{F}_p$. We will be working with the ring of p-adic integers and the ring of formal power series over $\mathbb{F}_p$, denoted respectively by $\mathbb{Z}_p$ and $\mathbb{F}_p[[t]]$. Each one of these groups is equipped with the profinite topology.

Moving to product-free measure. First note that $\mathrm{pf}(G) \leq 1/2$. This follows from the fact that if $A \cap A^2 = \emptyset$ then for each $x \in A$, the sets A and xA are disjoint and have the same Haar measure. One can also easily see that for any non-trivial group G, $\mathrm{pf}(G) > 0$. Let G be a compact group. It is known that the topology of G is given by a bi-invariant metric (see Corollary A4.19 in [**11**].) Let d_G be such a metric and $D = \mathrm{diam}(G)$ be the diameter of G. Let us also denote $f(r) = \mu(B(x, r))$ (note that the bi-invariance of d_G implies that volume of the ball is independent of the centre.) Then we have

PROPOSITION 1. *For any non-trivial group G,* $\mathrm{pf}(G) \geq f(D/3) > 0$.

Proof. Choose $y, z \in G$ such that $d_G(y, z) = D$ and let $x = z^{-1}y$. We have,

$$d_G(x, x^2) = d_G(1, x) = d_G(z, zx) = d_G(z, y) = D.$$

An application of triangle inequality shows that if $u, v \in B(x, D/3)$ then $uv \in B(x^2, 2D/3)$ and hence $uv \notin B(x, D/3)$. This shows that $B(x, D/3)$ is product-free. □

It is worth pointing out that one can give an alternative definition by replacing $A \cap A^2 = \emptyset$ with $\mu(A \cap A^2) = 0$. However, this turns out to be equivalent:

PROPOSITION 2. *Suppose G is an infinite compact group with Haar measure* μ. *Define*

$$\mathrm{pf}_0(G) = \sup\{\mu(A) : A \subseteq G \text{ is measurable}, \mu(A \cap A^2) = 0\}.$$

Then $\mathrm{pf}_0(G) = \mathrm{pf}(G)$.

Proof. It is clear that $\mathrm{pf}(G) \leq \mathrm{pf}_0(G)$. To prove the inverse inequalities, let A be a measurable set with $\mu(A \cap A^2) = 0$. Then $B = A \setminus (A \cap A^2) \subseteq A$ has the same measure as A and $B \cap B^2 \subseteq B \cap A^2 = \emptyset$. This shows that $\mathrm{pf}(G) \leq \mathrm{pf}_0(G)$. □

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

The following lemma is very useful.

LEMMA 1. *Let H be a proper subgroup of a finite group G. Then G contains a subset of density $[G : H]^{-1}$ which is product-free. Similarly, if G is a profinite group and H is a proper open subgroup, then G contains an open product-free set of measure $[G : H]^{-1}$.*

Proof. Let $A = xH$ be a left coset of H other than H. It is easy to see that $A^2 \cap A = \emptyset$. □

3. Complex representations of profinite groups. In this section, we will gather some facts about profinite groups that will be used later. Our final aim in this section is to show that any non-trivial complex continuous representation of $\mathrm{SL}_k(\mathbb{Z}_p)$ (respectively, $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$) factors through a non-trivial representation of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ (respectively, $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$) for some n. In the next section, we will find a lower bound for such a representation.

A topological group which is the projective limit of finite groups, each equipped with the discrete topology, is called a profinite group. Such a group is compact and totally disconnected. The Haar measure for a profinite group G can be easily described as a "limit" of counting measures. More precisely, for an open set $U \subseteq G$ we have,

$$\mu(U) = \lim_i \frac{|\phi_i(U)|}{|G_i|}. \tag{9}$$

We call a family $\mathcal{I}$ of normal subgroups of an arbitrary group G a filter base if for all $K_1, K_2 \in \mathcal{I}$ there is a subgroup $K_3 \in \mathcal{I}$ which is contained in $K_1 \cap K_2$. Now let G be a topological group and $\mathcal{I}$ a filter base of closed normal subgroups, and for $K, L \in \mathcal{I}$ define $K \leq' L$ if and only if L is a subgroup of K. Thus $\mathcal{I}$ is a directed set with respect to the order $\leq'$ and the surjective homomorphisms $q_{KL} : G/L \to G/K$, defined for $K \leq' L$, make the groups G/K into an inverse system. Write $\widehat{G} = \varprojlim(G/K)$. There is a continuous homomorphism $\theta : G \to \widehat{G}$ with kernel $\bigcap_{K\in\mathcal{I}} K$, whose image is dense in $\widehat{G}$. We have the following.

PROPOSITION 3 (See [**21**], proposition 1.2.2). *If G is compact then θ is surjective; if G is compact and $\bigcap_{K\in\mathcal{I}} K = \{id\}$, then θ is an isomorphism of topological groups.*

Moreover we have:

PROPOSITION 4 (See [**21**], proposition 1.2.1). *Let (G, φ_n) be an inverse limit of an inverse system (G_n) of compact Hausdorff topological groups and let L be an open normal subgroup of G. Then* $\ker \varphi_n \leq L$ *for some n.*

For the profinite group $\mathrm{SL}_k(\mathbb{Z}_p)$, consider the following surjective homomorphism

$$0 \longrightarrow K_n \longrightarrow \mathrm{SL}_k(\mathbb{Z}_p) \xrightarrow{\varphi_n} \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow 0, \tag{10}$$

where φ_n is induced by the canonical surjective homomorphism $\mathbb{Z}_p \to \mathbb{Z}/(p^n\mathbb{Z})$. Clearly the set $\mathcal{I}$ consists of K_n is a filter base and $\bigcap K_n = \{I\}$, therefore by Proposition 3 we have

$$\mathrm{SL}_k(\mathbb{Z}_p) = \varprojlim \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})), \quad \mathrm{Sp}_{2n}(\mathbb{Z}_p) = \varprojlim \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})).$$

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

The following proposition is a standard fact in the context of the Galois representation, however for the sake of completeness we will prove it.

PROPOSITION 5. *Let G be a profinite group, and assume $\rho : G \to GL_m(\mathbb{C})$ is a continuous representation. Then the kernel of ρ is an open subgroup, hence* $\mathrm{Im}(\rho)$ *is a finite subgroup of $GL_m(\mathbb{C})$.*

Proof. It is well-known (see [**10**], Chapter II, B.5) that there exists an open neighbourhood of identity $U \subseteq \mathrm{GL}_m(\mathbb{C})$ which does not contain any non-trivial subgroup. Then $V := \rho^{-1}(U)$ is an open subset of G containing the identity. From the properties of profinite groups, we know that V contains an open subgroup, say H. This implies that $\rho(H) = 1$ and hence $H \leq \ker \rho$. Therefore $\ker \rho$ is open, thus $\mathrm{Im}(\rho)$ is finite. □

We can now specialize this to $\mathrm{SL}_k(\mathbb{Z}_p)$. A similar result also holds for the symplectic group $\mathrm{Sp}_{2k}(\mathbb{Z}_p)$.

PROPOSITION 6. *Let $\rho : SL_k(\mathbb{Z}_p) \to GL_m(\mathbb{C})$ be a continuous non-trivial representation. Then ρ factors through a non-trivial representation of $SL_k(\mathbb{Z}/(p^n\mathbb{Z}))$ for some n.*

Proof. By Proposition 5, $\ker \rho$ is an open normal subgroup, which by Proposition 4 contains K_n as introduced in (10) for some $n \geq 1$. Therefore ρ factors through to a non-trivial representation $\bar{\rho} : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \to \mathrm{GL}_m(\mathbb{C})$. □

4. Root functions. We will now turn to establishing the lower bound for the representations of the groups $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ and $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$.

DEFINITION 3. *Let $\mathcal{S}$ be a family of matrices in $M_d(\mathbb{C})$. For a function $r : \mathcal{S} \to \mathbb{C}$, define*

$$V(r) := \{v \in \mathbb{C}^d : Sv = r(S)v \quad \text{for all } S \in \mathcal{S}\}.$$

A map $r : \mathcal{S} \to \mathbb{C}$ will be called a root of $\mathcal{S}$ if $V(r) \neq \{0\}$. Moreover $V(r)$ is called a root subspace.

The following proposition is a special case of Theorem 15 in Section 9.5. of [**9**].

PROPOSITION 7. *Let $\mathcal{S}$ be a commuting family of $d \times d$ unitary matrices. Then $\mathcal{S}$ has only a finite number of roots. If $r_1, \ldots, r_t$ are all the distinct roots of $\mathcal{S}$ then*

1. *$V(r_i)$ is orthogonal to $V(r_j)$ for $i \neq j$.*
2. *$\mathbb{C}^d = V(r_1) \oplus \cdots \oplus V(r_t)$.*

4.1. Root functions for the special linear groups. Consider the following subgroups of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$:

$$L := \left\{ \begin{pmatrix} I_{k-1} & \sigma \\ 0 & 1 \end{pmatrix} : \sigma \in (\mathbb{Z}/(p^n\mathbb{Z}))^{k-1} \right\}, \qquad H := \left\{ \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix} : T \in \mathrm{SL}_{k-1}(\mathbb{Z}/(p^n\mathbb{Z})) \right\}.$$

Notice that L is an abelian subgroup and H normalizes L. Indeed we have

$$\begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I_{k-1} & \sigma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} I_{k-1} & T\sigma \\ 0 & 1 \end{pmatrix}, \tag{11}$$

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

which means that the action by conjugation of H on L is isomorphic to the standard action of $\mathrm{SL}_{k-1}(\mathbb{Z}/(p^n\mathbb{Z}))$ on $(\mathbb{Z}/(p^n\mathbb{Z}))^{k-1}$. Now, let $\rho : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \to \mathrm{GL}_d(\mathbb{C})$ be a non-trivial representation. Note that $\mathcal{S} := \rho(L)$ is a commuting set of $d \times d$ matrices. Next proposition shows that H acts on the root functions and the root subspaces of $\mathcal{S}$.

PROPOSITION 8. *Let r be one of the roots in the decomposition in Proposition 7 and let $h \in H$. For any $s = \rho(l) \in \mathcal{S}$, define $r_h(s) := r(\rho(hlh^{-1}))$. Then r_h is also a root for $\mathcal{S}$, and $V(r_h) = \rho(h^{-1})V(r)$.*

Proof. First note that since H normalizes L, the map r_h is well-defined. For $w \in V(r)$ and $l \in L$, we have

$$\rho(l)(\rho(h^{-1})w) = \rho(h^{-1})(\rho(hlh^{-1})w) = r(\rho(hlh^{-1}))\rho(h^{-1})w = r_h(\rho(l))(\rho(h^{-1})w).$$

This shows that r_h is a root for $\mathcal{S}$, and $\rho(h^{-1})V(r) \subseteq V(r_h)$. To show the equality let $v \in V(r_h)$, then for any $l \in L$ we have $\rho(l)(\rho(h)v) = \rho(h)(\rho(h^{-1}lh)v) = r(\rho(l))(\rho(h)v)$, therefore we have $\rho(h)V(r_h) \subseteq V(r)$. □

Let $e_i = I + E_{in}$, where E_{in} is the matrix with all entries zero except for (i, n)th entry, which is *one*. The group $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ is generated by elementary matrices, and all elementary matrices are conjugate to e_1, defined above. So we have:

LEMMA 2. *If $\rho(e_1) = I$, then ρ is a trivial representation.*

Now let ρ be a faithful representation then we claim the following.

LEMMA 3. *There exists a root r for $\mathcal{S}$, such that $r(\rho(e_1)) = \zeta$, where ζ is a primitive p^n-th root of unity.*

Proof. Let us denote the roots of $\mathcal{S}$ by $r_1, \ldots, r_t$. Assume the contrary that for all $1 \le i \le t$ we have $r_i(\rho(e_1)) = \zeta_{p^n}^{m_i}$, where $p \mid m_i$. We will show that $\rho(e_1^{p^{n-1}}) = I$, which is a contradiction since ρ is a faithful representation and the order of e_1 is p^n. By Proposition 7, we have the decomposition $\mathbb{C}^d = V(r_1) \oplus \cdots \oplus V(r_t)$. For $v \in \mathbb{C}^d$, write $v = v_1 + \cdots + v_t$, where $v_i \in V(r_i)$. Then, for any $m \in \mathbb{Z}$

$$(\rho(e_1))^m v = \zeta_{p^n}^{m_1 m} v_1 + \cdots + \zeta_{p^n}^{m_t m} v_t.$$

In particular, for $m = p^{n-1}$ we have $\rho(e_1^{p^{n-1}})v = v_1 + \cdots + v_t = v$, hence $\rho(e_1^{p^{n-1}}) = I$. □

Proof of Theorem 1 for $m_f(SL_k(\mathbb{Z}/(p^n\mathbb{Z})))$ when $k \ge 3$. Let $\rho : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \to \mathrm{GL}_d(\mathbb{C})$, be a faithful representational. First note that L as an abstract group is isomorphic to the direct sum of $k-1$ copies of the cyclic group $\mathbb{Z}/(p^n\mathbb{Z})$ and is generated by $e_1, \ldots, e_{k-1}$. We will occasionally deviate from our standard notation for the group operation and use additive notation for group operation on L, when this isomorphism is used. For instance, we will write $e_1 + e_2$ instead of $e_1 \cdot e_2$.

By Lemma 3 there is a root r for $\mathcal{S}$ such that $r(\rho(e_1)) = \zeta_{p^n}^{m_1}$, where $\gcd(m_1, p) = 1$. We also assume that for $2 \le i \le k-1$, we have $r(\rho(e_i)) = \zeta_{p^n}^{m_i}$ where $0 \le m_i \le p^n - 1$. For $t \in (\mathbb{Z}/(p^n\mathbb{Z}))^*$ and $a_2, \ldots, a_{k-1} \in \mathbb{Z}/(p^n\mathbb{Z})$ whose values will be assigned later,

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

define

$$\alpha := \alpha(t, a_2, \ldots, a_{k-1}) = \left(\begin{array}{cccc|c} t & a_2 & \cdots & a_{k-1} & 0 \\ 0 & t^{-1} & & & \vdots \\ 0 & 0 & I_{k-3} & & 0 \\ \vdots & \vdots & & & 0 \\ \hline 0 & \cdots & 0 & 0 & 1 \end{array}\right) \in H$$

Using (11), a simple computation shows that

$$\alpha e_1 \alpha^{-1} = te_1, \quad \alpha e_2 \alpha^{-1} = t^{-1}e_2 + a_2 e_1, \quad \alpha e_i \alpha^{-1} = e_i + a_i e_1 \quad (3 \le i \le k-1).$$

By Proposition 8, we have $r_{t,a_2,\ldots,a_{k-1}} := r_\alpha$ is a root and

$$\begin{aligned} r_\alpha(\rho(e_1)) &= r(\rho(\alpha e_1 \alpha^{-1})) = r(\rho(te_1)) = \zeta_{p^n}^{tm_1}, \\ r_\alpha(\rho(e_2)) &= r(\rho(\alpha e_2 \alpha^{-1})) = r(\rho(t^{-1}e_2 + a_2 e_1)) = \zeta_{p^n}^{t^{-1}m_2 + a_2 m_1}, \\ r_\alpha(\rho(e_i)) &= r(\rho(\alpha e_i \alpha^{-1})) = r(\rho(e_i + a_i e_1)) = \zeta_{p^n}^{m_i + a_i m_1} \quad (3 \le i \le k-1). \end{aligned} \tag{12}$$

Now, since $\gcd(m_1, p) = 1$, by varying the values of $t, a_2, \ldots, a_{k-1}$ we can get at least

$$\varphi(p^n)p^{(k-2)n} = (p^n - p^{n-1})p^{(k-2)n},$$

different roots. This shows that the dimension of the representation space has to be at least

$$(p^n - p^{n-1})p^{(k-2)n}.$$

□

Similarly, we have

LEMMA 4. *Let ρ be a non-trivial representation. Then, there exists a root r for $\mathcal{S}$ such that $r(\rho(e_1)) = \zeta_{p^n}^{m_1}$, where m_1 is non-zero in $\mathbb{Z}/(p^n\mathbb{Z})$.*

Proof. If for all roots we have $r_i(\rho(e_1)) = 1$, then similar to the proof of Lemma 3 we can deduce that $\rho(e_1) = I$. But by Lemma 2, we saw that if $\rho(e_1) = I$ then ρ is a trivial representation. That is a contradiction. □

Proof of Theorem 1 for $m(SL_k(\mathbb{Z}/(p^n\mathbb{Z})))$ when $k \ge 3$. Let ρ be a non-trivial representation of $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ in $\mathrm{GL}_d(\mathbb{C})$. By Lemma 2, $\rho(e_1) \ne I$ when ρ is not a trivial representation. With the same notation used in the previous proof, we obtain the following identities similar to (12).

$$\begin{aligned} r_\alpha(\rho(e_1)) &= r(\rho(\alpha e_1 \alpha^{-1})) = r(\rho(te_1)) = \zeta_{p^n}^{tm_1}, \\ r_\alpha(\rho(e_2)) &= r(\rho(\alpha e_2 \alpha^{-1})) = r(\rho(t^{-1}e_2 + a_2 e_1)) = \zeta_{p^n}^{t^{-1}m_2 + a_2 m_1}, \\ r_\alpha(\rho(e_i)) &= r(\rho(\alpha e_i \alpha^{-1})) = r(\rho(e_i + a_i e_1)) = \zeta_{p^n}^{m_i + a_i m_1} \quad (3 \le i \le k-1). \end{aligned} \tag{13}$$

The only difference is that m_1 is here only non-zero in $\mathbb{Z}/(p^n\mathbb{Z})$. So by varying the values of $t, a_2, \ldots, a_{k-1}$ we can get at least $p^{k-1} - p^{k-2}$ different roots. □

For $\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))$ this method does not works. Instead we present a different proof.

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

Proof of Theorem 1 for m_f ($SL_2(\mathbb{Z}/(p^n\mathbb{Z}))$). Let $\rho : \mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z})) \to \mathrm{GL}_d(\mathbb{C})$, be a faithful representation of the group $\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))$. Set $a := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, and let $A := \rho(a) \neq I$. Since the order of a is p^n and ρ is a faithful representation, therefore A has a non-trivial eigenvalue, say ζ, which is a primitive p^nth root of unity, since otherwise $A^{p^{n-1}} = I$, which is a contradiction. Notice that a is conjugate to a^m, where m is a square in $(\mathbb{Z}/(p^n\mathbb{Z}))^*$. Hereafter m will be an arbitrary quadratic residue in $\mathbb{Z}/(p^n\mathbb{Z})$. This implies that A and A^m would have the same set of eigenvalues. But ζ^m is an eigenvalue of A^m. The number of square elements in $(\mathbb{Z}/(p^n\mathbb{Z}))^*$ is $\varphi(p^n)/2$. Therefore A has at least $\varphi(p^n)/2$ different eigenvalues. So $d \geq \frac{\varphi(p^n)}{2}$. □

For $m\,(\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z})))$, the same method gives the bound $(p-1)/2$.

4.2. Root functions for the symplectic groups. Let J denote the $2k \times 2k$ matrix

$$J := \begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix}.$$

One way of defining the symplectic group is by:

$$\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) := \left\{A \in \mathrm{GL}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) : AJA^T = J\right\}.$$

We will use two types of symplectic matrices: First, for any symmetric $k \times k$ matrix σ and any invertible $k \times k$ matrix α, set

$$U_\sigma := \begin{pmatrix} I_k & \sigma \\ 0 & I_k \end{pmatrix}, \quad D_\alpha := \begin{pmatrix} \alpha & 0 \\ 0 & \tilde{\alpha} \end{pmatrix}.$$

For every invertible $k \times k$ matrix α, set the $2k \times 2k$ matrix where $\tilde{\alpha} = (\alpha^{-1})^T$. It is easy to see that U_σ and D_α defined as above are both symplectic. From here and the fact that the set

$$\left\{U_\sigma : \sigma \in M_k(\mathbb{Z}), \sigma = \sigma^T\right\} \cup \{J\},$$

is a generating set for $\mathrm{Sp}_{2k}(\mathbb{Z})$ (See [**16**] Section 5, Proposition 2) and the surjectivity of the reduction map, $\mathrm{Sp}_{2k}(\mathbb{Z}) \to \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$, (See [**14**] Theorem VII.21), we can deduce that the same set reduced mod p^n generates $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$. Since $U_{I_k} U_{-I_k}^T U_{I_k} = J$, then the set

$$\left\{U_\sigma, U_\sigma^T : \sigma \in M_k(\mathbb{Z}/(p^n\mathbb{Z})), \sigma = \sigma^T\right\},$$

is also a generating set for $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$. (See also [**2**], Chapter III). Notice that for a symmetric matrix $\sigma \in M_k(\mathbb{Z}/(p^n\mathbb{Z}))$, we have $JU_\sigma J^{-1} = U_{-\sigma}^T$. Consider the following subgroups of $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$:

$$L := \left\{U_\sigma : \sigma = \sigma^T\right\}, \quad H := \left\{D_\alpha : \alpha \in \mathrm{GL}_k(\mathbb{Z}/(p^n\mathbb{Z}))\right\}.$$

Notice that L is an abelian group and H acts on L via conjugation. In fact we have,

$$D_\alpha U_\alpha D_\alpha^{-1} = U_{\alpha\sigma\alpha^T}. \tag{14}$$

This shows that the action of H on L is the standard action of the general linear group on symmetric quadratic forms. For $1 \leq i, j \leq k$, E_{ij} denotes the symmetric $k \times k$

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

matrix such that the (i, j) and (j, i) entries are one and other entries are zero. Also set $G_{ij} := U_{E_{ij}}$. Now, it is easy to see that if $i_1 \neq j_1$ and $i_2 \neq j_2$ then the matrices $G_{i_1 j_1}$ and $G_{i_2 j_2}$ are conjugate. Similarly, the matrices G_{ii} and G_{jj} are conjugate for all i, j.

LEMMA 5. *Let ρ be a representation of $Sp_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$, so that $\rho(G_{11}) = \rho(G_{12}) = I$, then ρ is a trivial representation.*

Let $a_i \in \mathbb{Z}/(p^n\mathbb{Z})$ and $t \in (\mathbb{Z}/(p^n\mathbb{Z}))^*$, define

$$\alpha = \alpha_{t,a_1,\ldots,a_{k-1}} := \begin{pmatrix} t & a_1 & a_2 & \cdots & a_{k-1} \\ 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathrm{GL}_k(\mathbb{Z}/(p^n\mathbb{Z})), \tag{15}$$

where the only possibly nonzero entries appear in the first row and on the diagonal.

The proof of the following lemma is quite straightforward:

LEMMA 6. *With α defined as in (15), we have*

$$\begin{aligned} D_\alpha G_{11} D_\alpha^{-1} &= G_{11}^{t^2}, \quad D_\alpha G_{1j} D_\alpha^{-1} = G_{11}^{2ta_{j-1}} G_{1j}^{t} && (2 \le j \le k) \\ D_\alpha G_{22} D_\alpha^{-1} &= G_{11}^{a_1{}^2} G_{12}^{a_1} G_{22}, \quad D_\alpha G_{2j} D_\alpha^{-1} = G_{11}^{2a_1 a_{j-1}} G_{1j}^{a_1} G_{12}^{a_{j-1}} G_{2j} && (3 \le j \le k). \end{aligned} \tag{16}$$

The proof of the following propositions are similar to Proposition 8 and Lemma 3:

PROPOSITION 9. *Let r be one of the roots in the decomposition in Proposition 7 and let $h \in H$. For any $s = \rho(l) \in \mathcal{S}$, define*

$$r_h(s) := r(\rho(hlh^{-1})).$$

Then r_h is also a root for $\mathcal{S}$, and $V(r_h) = \rho(h^{-1})V(r)$.

LEMMA 7. *When ρ is a faithful representation, then there exists a root r for $\mathcal{S}$, such that $r(\rho(G_{11})) = \zeta$, where ζ is a primitive p^nth root of unity.*

We are ready to prove Theorem 1 for $\mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z}))$.

Proof of Theorem 1 for $m_f(Sp_{2k}(\mathbb{Z}/(p^n\mathbb{Z})))$. For this specific matrix α defined in (15), we use the shorthand $\overline{\alpha} := D_\alpha$. Let $\rho : \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) \to \mathrm{GL}_d(\mathbb{C})$, be a faithful representation and set $\mathcal{S} = \rho(L)$. Pick a root r for $\mathcal{S}$ such that $r(\rho(G_{11})) = \zeta_{p^n}^m$, where $\gcd(m, p) = 1$. Such a root exists by Lemma 7. For this root, let $r(\rho(G_{1j})) = \zeta_{p^n}^{m_j}$, for $2 \le j \le k$. With the same notation in Proposition 9 and (16) we have

$$r_{\overline{\alpha}}(\rho(G_{11})) = \zeta_{p^n}^{t^2 m}, \quad r_{\overline{\alpha}}(\rho(G_{1j})) = \zeta_{p^n}^{2a_{j-1}tm + tm_j}, \quad (2 \le j \le k). \tag{17}$$

Notice that the number of different square in $(\mathbb{Z}/(p^n\mathbb{Z}))^*$ is $\varphi(p^n)/2$. So by varying $t, a_1, \ldots, a_{k-1}$, we will obtain at least $(p^n - p^{n-1})p^{(k-1)n}/2$ different roots. □

Proof of Theorem 1 for $m(Sp_{2k}(\mathbb{Z}/(p^n\mathbb{Z})))$. Now let $\rho : \mathrm{Sp}_{2k}(\mathbb{Z}/(p^n\mathbb{Z})) \to \mathrm{GL}_d(\mathbb{C})$, be a non-trivial representation. Since ρ is non-trivial, at least one of $\rho(G_{11})$ and $\rho(G_{12})$ are different from the identity. We split the proof into two cases:

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

Case I: Let $\rho(G_{11}) \neq I$. This implies that there exists a root r for $\mathcal{S}$ such that $r(\rho(G_{11})) = \zeta_{p^n}^m$, where $m \neq 0$ in $\mathbb{Z}/(p^n\mathbb{Z})$. For this root, let $r(\rho(G_{1i})) = \zeta_{p^n}^{m_i}$ for $2 \leq i \leq k$. So (16) implies that

$$r_{\overline{\alpha}}(\rho(G_{11})) = \zeta_{p^n}^{t^2 m}, \quad r_{\overline{\alpha}}(\rho(G_{1j})) = \zeta_{p^n}^{2a_{j-1}tm+tm_j}, \quad (2 \leq j \leq k). \tag{18}$$

So by varying $t, a_1, \ldots, a_{k-1}$, we will obtain at least $\frac{1}{2}(p-1)p^{(k-1)}$ different roots.
Case II: Let $\rho(G_{11}) = I$. This will force $\rho(G_{12}) \neq I$. Now, pick a root r for $\mathcal{S}$ such that $r(\rho(G_{12})) = \zeta_{p^n}^m$, where $m \neq 0$ in $\mathbb{Z}/(p^n\mathbb{Z})$. Let for this root $r(\rho(G_{2j})) = \zeta_{p^n}^{m_i}$ for $2 \leq j \leq k$. Then by (16) we have $r_{\overline{\alpha}}(\rho(G_{12})) = r(\rho(G_{11}^{2ta_1}))r(\rho(G_{12}^t)) = r(\rho(G_{12}^t)) = \zeta_{p^n}^{tm}$. Also

$$r_{\overline{\alpha}}(\rho(G_{22})) = r(\rho(G_{11}^{a_1^2}))r(\rho(G_{12}^{a_1}))r(\rho(G_{22})) = r(\rho(G_{12}^{a_1}))r(\rho(G_{22})) = \zeta_{p^n}^{a_1 m} r(\rho(G_{22})).$$

Moreover for $3 \leq j \leq k$

$$r_{\overline{\alpha}}(\rho(G_{2j})) = r(\rho(G_{11}^{2a_1 a_{j-1}}))r(\rho(G_{12}^{a_{j-1}}))r(\rho(G_{1j}^{a_1}))r(\rho(G_{2j})) = \zeta_{p^n}^{a_{j-1}m} r(\rho(G_{1j}^{a_1}))r(\rho(G_{2j})).$$

Varying $t, a_1, \ldots, a_{k-1}$ will now results in at least $(p-1)p^{k-1}$ different roots and this finishes the proof. □

We remark that, by Theorem 1 and Proposition 6, Theorem 2 also follows.

5. Upper bound estimates for the product-free measure. This section gathers the functional analytic ingredients of the proof needed to cast Gowers' proof in the category of compact topological groups. Complete proof of these facts can be found, for instance, in [**17**]. After reviewing these facts, we will give the proof of Theorem 3 and Corollary 1.

DEFINITION 4. *Let $\mathcal{H}$ be a separable Hilbert space with an orthonormal basis $\{e_n\}$ and let $T \in B(\mathcal{H})$, where $B(\mathcal{H})$ denotes the space of bounded operators on $\mathcal{H}$. If the condition*

$$\sum_{n=1}^{\infty} \|T(e_n)\|^2 < \infty,$$

holds then T is called a Hilbert–Schmidt operator.

This is independent of the choice of the orthonormal basis of $\mathcal{H}$. Moreover, for a Hilbert–Schmidt operator T, the value of the sum is also independent of the choice of the orthonormal basis:

$$\|T\|_{HS}^2 := \sum_{n=1}^{\infty} \|T(e_n)\|^2.$$

LEMMA 8. *Let $\mathcal{H}$ be a separable Hilbert space and let $T \in B(\mathcal{H})$ then*
(a) *T is Hilbert–Schmidt if and only if T^* is Hilbert–Schmidt.*
(b) *If either S or T is Hilbert–Schmidt, then ST is Hilbert–Schmidt.*
(c) *If T is Hilbert–Schmidt then it is compact.*

Another useful fact is the singular value decomposition for the compact operators on a Hilbert space:

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

LEMMA 9 (singular value decomposition). *Let $\mathcal{H}$ denote a separable Hilbert space and $T \in B(\mathcal{H})$ a compact operator. Then there exists two orthonormal sets $\{e_n\}$ and $\{e'_n\}$ in $\mathcal{H}$ such that $T(e_i) = \lambda_i e'_i$, $T^*(e'_i) = \lambda_i e_i$, for $i = 1, 2, \ldots$. where $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$, and for any $x \in \mathcal{H}$*

$$T(x) = \sum_{i \geq 1} \lambda_i \langle x, e_i \rangle e'_i. \tag{19}$$

Moreover, by (19), we have $\|T\|_{op} = \lambda_1$.

Now, let G be a compact, second countable, Hausdorff topological group with a normalized Haar measure μ. As usual, set $L^2(G) = \{h : G \to \mathbb{C} : \|h\|_2^2 < \infty\}$, where $\|h\|_2^2 := \int_G |h|^2 d\mu$.

Moreover, let us define $L_0^2(G)$ to be the set of all functions in $L^2(G)$ which are orthogonal to the constant function 1. For $f_1, f_2 \in L^2(G)$, the convolution $f_1 * f_2 \in L^2(G)$ is defined by

$$(f_1 * f_2)(x) := \int_G f_1(xy^{-1}) f_2(y)\, d\mu(y).$$

Now, take a function $f_1 \in L_0^2(G)$ and consider the following kernel $K(x, y) := f_1(xy^{-1})$. Since $f_1 \in L^2(G)$, we have $K(x, y) \in L^2(G \times G)$. So we can define the following integral operator

$$\Phi_K : L^2(G) \longrightarrow L^2(G), \quad h \longmapsto \Phi_K(h), \tag{20}$$

It is clear that $\Phi_K(h)(x) = (f_1 * h)(x)$. One can also easily see that the adjoint operator Φ_K^* is given by

$$\Phi_K^*(h)(y) = \int_G \overline{K(x, y)} h(x) d\mu(x).$$

LEMMA 10. *The integral operator $\Phi_K : L^2(G) \to L^2(G)$ is a Hilbert–Schmidt operator and hence is compact. The norm of Φ_K is given by $\|\Phi_K\|_{HS} = \|K\|_{L^2(G \times G)}$.*

Proof of Theorem 3. To prove Theorem 3 note that by replacing f_2 with $f_2 - \int_G f_2\, d\mu$ and noticing that $f_1 * c = 0$ for every constant function c, without loss of generality, we can assume that $f_2 \in L_0^2(G)$. Consider the operator $\Phi_K : L^2(G) \to L^2(G)$, defined by (20). Let Φ_0 denote the restriction of Φ_K to $L_0^2(G)$. We need to show that

$$\|\Phi_0\|_{op}^2 \leq \frac{1}{m(G)} \|f_1\|_2^2. \tag{21}$$

Apply the singular value decomposition to obtain orthonormal bases $\{e_n\}$ and $\{e'_n\}$ in $L_0^2(G)$ such that $\Phi_0(e_i) = \lambda_i e'_i$, where $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$. Moreover $\|\Phi_0\|_{op} = \lambda_1$. Let V_1 be the eigenspace of the self-adjoint operator $\Phi_0^* \Phi_0$ corresponding to λ_1^2. Since $\Phi_0^* \Phi_0$

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

is a compact operator, $\dim V_1 < \infty$. We have

$$\|\Phi_0\|_{op}^2 \dim V_1 = \lambda_1^2 \dim(V_1) \leq \sum_{i=1}^{\infty} \lambda_i^2 \leq \|\Phi_K\|_{HS}^2 = \|K\|_{L^2(G\times G)}^2$$
$$= \int_G \int_G |f_1(xy^{-1})|^2 d\mu(y) d\mu(x) = \|f_1\|_2^2.$$

We show that $\dim V_1 \geq m(G)$, and this would finish the proof. We will construct a linear action of G on V_1 by defining for every $h \in V_1$ and $g \in G$ $T_g h(x) := h(xg)$. We need to verify that,

$$T_g(\Phi_K^* \Phi_K(h)) = \Phi_K^* \Phi_K(T_g h). \tag{22}$$

Since G is compact and hence unimodular we have,

$$\Phi_K(T_g h)(x) = \int_G f_1(xy^{-1}) h(yg) d\mu(y) = \int_G f_1(x(zg^{-1})^{-1}) h(z) d\mu(z)$$
$$= \int_G f_1(xgz^{-1}) h(z) d\mu(z) = T_g(\Phi_K(h))(x).$$

By acting Φ_K^* from the left we obtain (22). Since V_1 is a subspace of $L_0^2(G)$, it does not contain the constant function, and hence this linear action is non-trivial. This induces a non-trivial representation of G in the unitary group $U(V_1)$, thus $\dim V_1 \geq m(G)$. □

Proof of Corollary 1. Apply the inequality to $f_1 = 1_A$ and $f_2 = 1_B - \mu(B)$. □

Proof of Theorem 4. Let $S := \{y \in G : (1_A * 1_B)(y) = 0\}$. Thus

$$\mu(S)^{1/2} \mu(A)\mu(B) = \left(\int_S |(1_A * 1_B)(y) - \mu(A)\mu(B)|^2 \, d\mu(y) \right)^{1/2}$$
$$\leq \left(\int_G |(1_A * 1_B)(y) - \mu(A)\mu(B)|^2 \, d\mu(y) \right)^{1/2}$$
$$= \|1_A * 1_B - \mu(A)\mu(B)\|_2.$$

From Corollary 1, we can deduce that

$$\mu(S)^{1/2} \mu(A)\mu(B) \leq \sqrt{\frac{\mu(A)\mu(B)}{m(G)}},$$

therefore $\mu(S) \leq 1/(m(G)\mu(A)\mu(B))$. This implies that $\mu(C \setminus S) > 0$, since otherwise we get $\mu(C)\mu(A)\mu(B) \leq 1/m(G)$, which is a contradiction. Hence, there exists a set of positive measure of $y \in C$ so that $1_A * 1_B(y) \neq 0$, which means that $AB \cap C$ has positive measure.

For the second statement, let us define $\Sigma := \{(a, b, c) \in A \times B \times C : ab = c\}$. Notice that

$$\mu(\Sigma) = \langle 1_A * 1_B, 1_C \rangle = \langle 1_A * (1_B - \mu(B)), 1_C \rangle + \mu(A)\mu(B)\mu(C). \tag{23}$$

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

By Cauchy–Schwartz inequality we have

$$\langle 1_A * (1_B - \mu(B)), 1_C\rangle^2 \le \|1_A * (1_B - \mu(B))\|_2^2 \|1_C\|_2^2$$
$$= \|1_A * 1_B - \mu(A)\mu(B)\|_2^2 \mu(C) \le \frac{\mu(A)\mu(B)\mu(C)}{m(G)}.$$

If

$$\frac{\mu(A)\mu(B)\mu(C)}{m(G)} \le \eta^2 \mu(A)^2 \mu(B)^2 \mu(C)^2,$$

which is fulfilled by our assumption, we can deduce that

$$|\langle 1_A * (1_B - \mu(B)), 1_C\rangle| \le \eta \mu(A)\mu(B)\mu(C),$$

and hence, $\mu(\Sigma) \ge \mu(A)\mu(B)\mu(C) - \eta\mu(A)\mu(B)\mu(C) = (1-\eta)\mu(A)\mu(B)\mu(C)$. □

REMARK 2. One can also establish a lower bound for $\mu(AB)$. For $f_1 = 1_A$ and $f_2 = 1_B - \mu(B)$, one has $\|f_2\|_2^2 = \mu(B)(1-\mu(B))$. Thus by Theorem 3 we have

$$\mu(G - AB)^{1/2} \mu(A)\mu(B) \le \sqrt{1/m(G)}\mu(A)^{1/2} (\mu(B)(1-\mu(B)))^{1/2},$$

therefore

$$1 - \frac{1-\mu(B)}{m(G)\mu(A)\mu(B)} \le \mu(AB).$$

6. Lower bounds for the product-free measure. We will now turn to establishing the lower bounds for the product-free measure. Consider the reduction map $\phi : \mathrm{SL}_k(\mathbb{Z}_p) \to \mathrm{SL}_k(\mathbb{Z}/(p\mathbb{Z}))$, and let Q be the subgroup consisting of all matrices $g \in \mathrm{SL}_k(\mathbb{Z}/(p\mathbb{Z}))$ such that $g_{1k} = \cdots = g_{k-1,k} = 0$. It is clear that Q is the stabilizer of a point in the action of $\mathrm{SL}_k(\mathbb{Z}_p)$ on the projective space and hence $[\mathrm{SL}_k(\mathbb{Z}/(p\mathbb{Z})) : Q] = \frac{p^k-1}{p-1}$. Applying Lemma 1 establishes the lower bound.

Now, let us take the symplectic group. It is clear that the reduction map $\phi : \mathrm{Sp}_{2k}(\mathbb{Z}_p) \to \mathrm{Sp}_{2k}(\mathbb{Z}/(p\mathbb{Z}))$, is surjective. Consider the natural action of $\mathrm{Sp}_{2k}(\mathbb{Z}/(p\mathbb{Z}))$ on $(\mathbb{Z}/(p\mathbb{Z}))^{2k}$. We know that for any field F and $l \ge 1$, the action of the symplectic group $\mathrm{Sp}_{2k}(F)$ on the set of l-dimensional isotropic subspaces is transitive. Since every one-dimensional subspace is isotropic, we obtain a transitive action on this space, which is equivalent to the action on the projective space. By choosing H to be the stabilizer of one of a point in the projective space, and taking the inverse image under the reduction map, we obtain a subgroup Q of index $[\mathrm{Sp}_{2k}(\mathbb{Z}_p) : Q] = \frac{p^{2k}-1}{p-1}$, which again establishes the lower bound for the symplectic group.

7. Tree automorphism groups. The goal of this section is to obtain lower and upper bounds on the product-free measure of the group of automorphisms of a rooted tree. Let $T = T_{k+1}$ be a regular tree of degree $k+1$. An automorphism of T is defined to be a permutation of the vertices of T that preserves incidence. The set of all automorphisms of T together with the topology of point-wise convergence forms a locally compact group G that acts on the set of vertices of T transitively. Fix one of the vertices of T as root and denote it by O. Now, consider the stabilizer A_{k+1} of this vertex

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

in G. It is easy to see that this subgroup is a profinite and hence compact group. To see this, note that since every $x \in A_{k+1}$ fixes O, it must permute the set of all the $k+1$ neighbouring vertices. A simple induction shows that for every $j \geq 1$ all $(k+1)k^{j-1}$ vertices of distance j from O must also be permuted by x. These induce a family of homomorphism $\sigma_j : A_{k+1} \to \Sigma_{(k+1)k^{j-1}}$, where Σ_m denotes the symmetric group on $\{1, 2, \ldots, m\}$. Then the following family of finite index subgroups can be used to provide a system of fundamental open neighbourhood of the identity automorphism $\mathscr{C}_j = \{x \in A_{k+1} : \sigma_j(x) = \mathrm{id}\}$. And A_{k+1} is the inverse limit, $A_{k+1} = \varprojlim A_{k+1}/\mathscr{C}_j$. For more details we reefer the reader to [**3**]. We will now set out to define the subgroup of A_{k+1} that appears in the statement of Theorem 6.

DEFINITION 5. *An automorphism $x \in A_{k+1}$ is called positive if $\sigma_j(x)$ is an even permutation for all $j \geq 1$. We will denote the group of all positive automorphisms by A_{k+1}^+.*

First, notice that A_{k+1}^+ is a closed subgroup of A_{k+1} and hence a profinite group. In fact, the group can also be represented by

$$A_{k+1}^+ = \varprojlim A_{k+1}^+/\mathscr{C}_j^+, \tag{24}$$

where $\mathscr{C}_j^+ := \left\{x \in A_{k+1}^+ : \sigma_j(x) = \mathrm{id}\right\}$. In what follows, let $\mathrm{Alt}_{k+1} \leq \Sigma_{k+1}$ denote the alternating group on $k+1$ symbols. We will need the following fact from the representation theory of finite groups:

THEOREM 8 (See [**5**] Exercise 5.5). *.For $k \geq 6$, the minimum dimension of non-trivial representations of Alt_k is $k-1$.*

Proof of Theorem 6. For the lower bound, note that $\sigma_1 : A_{k+1}^+ \to \mathrm{Alt}_{k+1}$ is surjective. Let H be the subgroup of Alt_{k+1} consisting of those permutations that fix $k+1$. H is clearly isomorphic to Alt_k. Now, apply Lemma 1 to the subgroup $\sigma_1^{-1}(H)$ to obtain an open subgroup of index $k+1$ in A_{k+1}^+. This establishes the lower bound.

For the upper bound, we need to show that A_{k+1}^+ does not have any non-trivial continuous representation of dimension less than $k-1$.

By (24) then we should prove that $F_j := A_{k+1}^+/\mathscr{C}_j^+$ does not have any non-trivial representation of dimension less than $k-1$. Suppose ρ be such a non-trivial representation.

For $j=1$, we will get $F_1 = \mathrm{Alt}_{k+1}$, and then by Theorem 8, for $k \geq 5$, all the non-trivial representation has dimension bigger than k. For the sake of clarity and notational simplicity, we will present the argument for $j=2$. The argument readily extends to an arbitrary $j \geq 2$. It is easy to see that

$$F_2 \simeq \mathrm{Alt}_{k+1} \ltimes \underbrace{(\Sigma_k \times \Sigma_k \times \cdots \times \Sigma_k)^+}_{k+1},$$

where

$$\underbrace{(\Sigma_k \times \Sigma_k \times \cdots \times \Sigma_k)^+}_{k+1} := \left\{(\sigma_1, \ldots, \sigma_{k+1}) \in \underbrace{(\Sigma_k \times \Sigma_k \times \cdots \times \Sigma_k)}_{k+1} : \prod_{i=1}^{k+1} \mathrm{sgn}(\sigma_i) = 1\right\}.$$

and Alt_{k+1} acts by permuting the factors.

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

If the restriction of ρ to Alt_{k+1} is non-trivial then we are done by Theorem 8. Suppose that the restriction of ρ to Alt_{k+1} is trivial. Clearly

$$\underbrace{\mathrm{Alt}_k \times \cdots \times \mathrm{Alt}_k}_{k+1} \trianglelefteq \underbrace{(\Sigma_k \times \cdots \times \Sigma_k)^+}_{k+1},$$

Again, we can assume that the restriction of ρ to each one of the factors is trivial, since otherwise we can apply Theorem 8 to obtain the bound $k-1$. So ρ factors through the quotient

$$(\Sigma_k \times \cdots \times \Sigma_k)^+ / (\mathrm{Alt}_k \times \cdots \times \mathrm{Alt}_k).$$

Note that since the restriction of ρ to Alt_{k+1} is trivial we have

$$\rho(\sigma_1, \sigma_2, \ldots, \sigma_k, \sigma_{k+1}) = \rho(\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}, \sigma_{i_{k+1}}),$$

for any even permutation $(i_1, i_2, \ldots, i_k, i_{k+1})$ of the set $\{1, \ldots, k, k+1\}$. Notice that

$$\frac{\overbrace{(\Sigma_k \times \Sigma_k \times \cdots \times \Sigma_k)^+}^{k+1}}{\underbrace{\mathrm{Alt}_k \times \mathrm{Alt}_k \times \cdots \times \mathrm{Alt}_k}_{k+1}} \cong \mathscr{L} := \left\{(v_1, \ldots, v_{k+1}) \in \mathbb{F}_2^{k+1} : v_1 + \cdots + v_{k+1} = 0\right\}. \tag{25}$$

So, ρ will be trivial if we can show:

LEMMA 11. *Let $k \geq 6$ be an integers and $\mathscr{L}$ be the group defined in (25). Let $\rho : \mathscr{L} \to GL_d(\mathbb{C})$, be a non-trivial representation of $\mathscr{L}$ such that $\rho(v_1, \ldots, v_{k+1}) = \rho(v_{i_1}, \ldots, v_{i_{k+1}})$ for any even permutation $(i_1, \ldots, i_{k+1})$ of the set $\{1, \ldots, k+1\}$. Then $d \geq k-1$.*

Proof. We will show that ρ is faithful when $k+1$ is odd and $|\ker(\rho)| \leq 2$ when $k+1$ is even. For $0 \neq v \in \mathscr{L}$, define $I(v) := \{1 \leq i \leq k+1 : v_i = 1\}$. Let assume that ρ is not a faithful representation. If for some $0 \neq v \in \ker(\rho)$, we have $|I(v)| = 2$, then $\ker(\rho)$ will contain every w with $|I(w)| = 2$, since for any $w \in \mathscr{L}$, with $|I(w)| = 2$, we have $\sigma(v) = w$, for some $\sigma \in \mathrm{Alt}_{k+1}$. This implies that $\ker(\rho) = \mathscr{L}$, hence ρ is trivial representation. Suppose $0 \neq v \in \ker(\rho)$ is chosen such that $|I(v)|$ is minimal. Since ρ is non-trivial then $|I(v)| = 2j > 2$. Without loss of generality assume that $v = (1, 1, \ldots, 1, 0, \ldots, 0)$ where the first $2j$ entries are equal to one and the rest are zero.

If $k+1$ is odd, then we can consider the 3-cycle $\sigma = (1, 2, 2j+1) \in \mathrm{Alt}_{k+1}$. Now, it is easy to see that $\sigma \cdot v - v$ has 1 in only two positions, hence $\sigma(v) - v \in \ker(\rho)$, with $|I(\sigma(v) - v)| = 2$. This shows that ρ is a faithful representation when $k+1$ is odd.

A similar argument can be made when $k+1$ is even and $|\ker(\rho)| > 2$. This show that ρ is faithful when $k+1$ is odd and $|\ker(\rho)| \leq 2$ when $k+1$ is even. In either case $\rho(\mathscr{L})$ has a subgroup isomorphic to $\mathbb{F}_2^{k-1}$. The set $\rho(\mathscr{L})$ can be simultaneously diagonalized with diagonal entries being ± 1. Now it is clear that $d \geq k-1$ in both cases. □

For $j \geq 3$, the group F_j is isomorphic to an iterated semi-direct product of alternating groups as above and a similar argument establishes the lower bound on the degree of nontrivial representation. Applying Theorem 4 completes the proof. □

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

8. Product-free measure of abelian groups. We will compute the exact value $\mathrm{pf}(G)$ for connected abelian Lie groups G. Let $\mathbb{T}^k$ denote the k-dimensional torus. Then,

THEOREM 9. *For any $k \geq 1$ we have* $\mathrm{pf}(\mathbb{T}^k) = 1/3$.

Proof. The proof is similar to the proof given in [**12**] where only open sets A are considered. We will show that in fact there is no need to restrict to consider just the open sets. We will write this part of the proof, which is valid for any compact group, using the multiplicative notation. Suppose that A is a product-free subset with $\mu(A) = 1/3 + \beta$ for some $\beta > 0$. First choose a compact set $K \subseteq A$ with $\mu(K) \geq 1/3 + \beta/2$. Clearly K is product-free and since K is compact $d(K, K^2) = \epsilon > 0$ where we use d as as shorthand for $d_{\mathbb{T}^k}$. Let U be the δ-neighbourhood of K, i.e., the set of points $u \in \mathbb{T}^k$ such that $d(u, k) < \delta$ for some $k \in K$. We will show that for δ small enough U will be product-free as well. Let $u_1, u_2, u_3 \in U$. So there exist $k_1, k_2, k_3 \in K$ such that $d(u_i, k_i) < \delta$ for $i = 1, 2, 3$. Using the invariance of d we have

$$\begin{aligned} d(u_2u_3, k_2k_3) &\leq d(u_2u_3, k_2u_3) + d(k_2u_3, k_2k_3) \\ &= d(u_2, k_2) + d(u_3, k_3) < 2\delta. \end{aligned}$$

From here we have $d(u_1, u_2u_3) \geq d(k_1, k_2k_3) - d(k_1, u_1) - d(k_2k_3, u_2u_3) \geq \epsilon - 3\delta$. So, if we choose $\delta = \epsilon/4$ we will have $d(u_1, u_2u_3) > \epsilon/4$ which shows that $U \cap U^2 = \emptyset$.

Now let us assume that A is an open product-free subset of $\mathbb{T}^k = \mathbb{T}^1 \times \cdots \times \mathbb{T}^1$ with $\mu(A) = 1/3 + \beta$. Again, by possibly exchanging β with $\beta/2$ we can assume that A is a disjoint union of finitely many boxes of the form: $I_1 \times I_2 \cdots \times I_k$ where I_j is an interval in the jth copy of $\mathbb{T}^1$. Choose a large prime number p. Set $\zeta = \exp(2\pi i/p)$ and let G_p be the elementary abelian p-group in $\mathbb{T}^k$ consisting of all elements of order p. Note that G_p contains p^k elements. Consider a box $I_1 \times I_2 \cdots \times I_k$ and let h_j be the length of I_j. It is easy to see that

$$|G_p \cap I| \geq (ph_1 - 1) \cdots (ph_k - 1) = p^k \mu(I) + O(p^{k-1}).$$

By adding up over all boxes we will get $|G_p \cap A| \geq p^k \mu(A) + O(p^{k-1})$. Since G_p is a finite p-group, by Green–Ruzsa theorem (see Theorem 10) we have $\mathrm{pf}(G_p) \leq 1/3 + 1/(3p)$. Since A is product-free we must have $(1/3 + \beta/2) + O(1/p) \leq 1/3 + 1/(3p)$, which as $p \to \infty$ gives a contradiction. □

For finite abelian groups, the exact value of $\mathrm{pf}(G)$ is explicitly given by:

THEOREM 10 (Green–Ruzsa, cf. [**7**]). *Suppose G is a finite abelian group of size n.*

1. *If n is divisible by a prime $p \equiv 2 \pmod 3$, then* $\mathrm{pf}(G) = 1/3 + 1/(3p)$ *where p is the smallest such p.*
2. *Otherwise, if $3|n$, then* $\mathrm{pf}(G) = 1/3$.
3. *Otherwise,* $\mathrm{pf}(G) = 1/3 - 1/(3m)$ *where m is the largest order of any element of G.*

Using Theorem 10 we will prove our first theorem.

Proof of Theorem 7. First, we will give the proof for $\mathbb{Z}_p$. Let $\phi_n : \mathbb{Z}_p \to \mathbb{Z}/(p^n\mathbb{Z})$ be reduction modulo p^n for $n \geq 1$. For $p \equiv 2 \pmod 3$, it is easy to verify that if $S \subseteq \mathbb{Z}/(p\mathbb{Z})$ is a product-free set of density $1/3 + 1/(3p)$, provided by Green–Ruzsa theorem, then $\phi_1^{-1}(S) \subseteq \mathbb{Z}_p$ will be a set of the same density. For $p \equiv 1 \pmod 3$, consider the subset

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

of $\mathbb{Z}/(p^n\mathbb{Z})$:

$$S_n = \left\{ \left\lfloor \frac{p^n+1}{3} \right\rfloor, \ldots, 2\left\lfloor \frac{p^n+1}{3} \right\rfloor - 1 \right\}.$$

By Lemma 1 we have

$$\mathrm{pf}(\mathbb{Z}_p) \geq \sup_{n\geq 1} \frac{|S_n|}{p^n} = \sup_{n\geq 1} \frac{\left\lfloor \frac{p^n+1}{3} \right\rfloor - 1}{p^n} = \frac{1}{3}.$$

On the other hand, suppose A is a measurable product-free subset of $\mathbb{Z}_p$ with $\mu(A)$ larger than the function given on the right side of (8), that we denote it by $f(p)$. Choose a compact subset $A_1 \subseteq A$ such that $\mu(A_1) = f(p)(1+\epsilon)$ for some $\epsilon > 0$. By (9), this can be seen in a sufficiently finite quotient of $\mathbb{Z}_p$, i.e., for sufficiently large n, the set $\phi_n(A_1) \subseteq \mathbb{Z}/(p^n\mathbb{Z})$ has a density larger that $f(p)(1+\epsilon/2)$. By the theorem of Green and Ruzsa, this implies that there exist $x_n, y_n, z_n \in A_1$ such that $\phi_n(x_n + y_n - z_n) = 0$. Since A_1 is compact, after passing to a subsequence, there exist $x, y, z \in A_1$ such that $x_n \to x$, $y_n \to y$, $z_n \to z$. Now, since $x_n + y_n - z_n \to 0$, we have $x + y = z$, which is a contradiction.

The proof for $\mathbb{F}_p[[t]]$ is similar. The only difference is that all of the finite quotients of $\mathbb{F}_p[[t]]$ are elementary p-groups. Hence when $p \equiv 1 \pmod 3$, it is the third condition in Green–Ruza theorem that applies. □

ACKNOWLEDGEMENTS. We have benefited from some notes on Terence Tao's weblog as well as Emmanuel Breuillard's lecture notes on "Théorie des groupes approximatifs". We wish to thank them for providing these notes online. For many fruitful discussions, we wish to thank Andrew Granville. The first author was supported in part by Faculté des Études Supérieures et Postdoctorales de l'Université de Montréal. The second author would like to thank CRM in Montreal for the visit during which part of this joint work was done. We would also like to thank the referee for some useful suggestions.

REFERENCES

1. L. Babai and V. T. Sós, Sidon sets in groups and induced subgraphs of Cayley graphs, *Eur. J. Combin.* **6**(2) (1985), 101–114.

2. H. Bass, J. Milnor and J.-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), *Inst. Hautes Études Sci. Publ. Math.* **33**(1) (1967), 59–137.

3. H. Bass and A. Lubotzky, *Tree lattices*, Progress in Mathematics, vol. 176 (Birkhäuser Boston Inc., Boston, MA, USA, 2001). With appendices by Bass, L. Carbone, Lubotzky, G. Rosenberg and J. Tits.

4. J. Bourgain and A. Gamburd, Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. I, *J. Eur. Math. Soc. (JEMS)* **10**(4) (2008), 987–1011.

5. W. Fulton and J. Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129 (Springer-Verlag, New York, USA, 1991). A first course, Readings in Mathematics.

6. W. T. Gowers, Quasirandom groups, *Comb. Probab. Comput.* **17**(3) (2008), 363–387.

7. B. Green and I. Z. Ruzsa, Sum-free sets in abelian groups, *Isr. J. Math.* **147**(1) (2005), 157–188.

8. H. A. Helfgott, Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, *J. Eur. Math. Soc. (JEMS)* **13**(3) (2011), 761–851.

9. K. Hoffman and R. Kunze, *Linear algebra*, 2nd ed. (Prentice-Hall Inc., Englewood Cliffs, N.J., USA, 1971).

https://doi.org/10.1017/S0017089514000251 Published online by Cambridge University Press

10. S. Helgason, *Differential geometry, Lie groups, and symmetric spaces*, Graduate Studies in Mathematics, vol. 34 (American Mathematical Society, Providence, RI, USA, 2001)

11. K. H. Hofmann and S. A. Morris, *The structure of compact groups*, de Gruyter Studies in Mathematics, vol. 25 (Walter de Gruyter & Co., Berlin, augmented ed., 2006).

12. K. S. Kedlaya, Product-free subsets of groups, *Am. Math. Mon.* **105**(10) (1998), 900–906.

13. V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32**(2) (1974), 418–443.

14. M. Newman, *Integral matrices*, Pure and Applied Mathematics, vol. 45 (Academic Press, New York, USA, 1972).

15. N. Nikolov and L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem, *J. Eur. Math. Soc. (JEMS)* **13**(4) (2011), 1063–1077.

16. N. S. Rege, On certain classical groups over Hasse domains, *Math. Z.* **102**(2) (1967), 120–1257.

17. B. P. Rynne and M. A. Youngson, *Linear functional analysis*, Springer Undergraduate Mathematics Series (Springer-Verlag London Ltd., London, UK, 2000).

18. G. Schul and A. Shalev, Words and mixing times in finite simple groups, *Groups Geom. Dyn.* **5**(2) (2011), 509–527.

19. A. Shalev, Mixing and generation in simple groups, *J. Algebra* **319**(7) (2008), 3075–3086.

20. A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, *Ann. Math.* **170**(3) (2009), 1383–1416.

21. J. S. Wilson, *Profinite groups*, London Mathematical Society Monographs. New Series, vol. 19 (The Clarendon Press Oxford University Press, New York, USA, 1998).