PRODUCTS OF NORMAL SUBSETS

MICHAEL LARSEN, ANER SHALEV, AND PHAM HUU TIEP

Abstract. In this paper we consider which families of finite simple groups G have the property that for each $\epsilon > 0$ there exists $N > 0$ such that, if $|G| \geq N$ and S, T are normal subsets of G with at least $\epsilon|G|$ elements each, then every non-trivial element of G is the product of an element of S and an element of T.

We show that this holds in a strong and effective sense for finite simple groups of Lie type of bounded rank, while it does not hold for alternating groups or groups of the form $\mathrm{PSL}_n(q)$ where q is fixed and $n \to \infty$. However, in the case $S = T$ and G alternating this holds with an explicit bound on N in terms of ϵ.

Related problems and applications are also discussed. In particular we show that, if w_1, w_2 are non-trivial words, G is a finite simple group of Lie type of bounded rank, and for $g \in G$, $P_{w_1(G),w_2(G)}(g)$ denotes the probability that $g_1 g_2 = g$ where $g_i \in w_i(G)$ are chosen uniformly and independently, then, as $|G| \to \infty$, the distribution $P_{w_1(G),w_2(G)}$ tends to the uniform distribution on G with respect to the L^∞ norm.

Contents

2010 *Mathematics Subject Classification.* Primary 20D06; Secondary 20F69, 20G40, 20P05.

ML was partially supported by the NSF (grants DMS-1702152 and DMS-2001349), and the Simons Foundation. AS was partially supported by ISF grant 686/17 and the Vinik Chair of mathematics which he holds. PT was partially supported by the NSF (grants DMS-1840702 and DMS-2200850), the Simons Foundation, the Joshua Barlaz Chair in Mathematics, and the Charles Simonyi Endowment at the Institute for Advanced Study (Princeton). All three authors were partially supported by BSF grants 2016072 and 2020037.

The authors are grateful to the referee for careful reading and thoughtful comments which significantly improved the paper.

1. Introduction

In the past two decades there has been considerable interest in the products of subsets of finite groups, especially (nonabelian) finite simple groups. The so-called Gowers trick (see [Go] and [NP]), which is part of the theory of quasi-random groups, shows that the product of three large subsets of a finite group G is the whole of G (where large is defined in terms of $|G|$ and the minimal degree of a non-trivial irreducible representation of G). See Section 7 below for details and consequences.

The celebrated Product Theorem of [BGT] and [PS], which is part of the deep theory of approximate subgroups originating in [He] and [Hr], shows that for finite simple groups G of Lie type and bounded rank there exists $\epsilon > 0$ (depending only on the rank of G) such that for every subset $A \subseteq G$ which generates G, either $|A^3| \geq |A|^{1+\epsilon}$ or $A^3 = G$.

Note that both the Gowers trick and the Product Theorem deal with products of three (or more) subsets. Much less is known about products of two subsets, which is the main topic of this paper.

There has been substantial interest in products of two *normal* subsets. A long-standing conjecture of Thompson asserts that every finite simple group G has a conjugacy class C such that $C^2 = G$. In spite of considerable efforts (see [EG] and the references therein) and the proof of the related Ore Conjecture (see [LBST]), Thompson's Conjecture is still open for groups of Lie type over fields with $q \leq 8$ elements. A weaker result, that all sufficiently large finite simple groups G have conjugacy classes C_1, C_2 such that $C_1C_2 \supseteq G \smallsetminus \{e\}$ is obtained in [LST1]; this was improved in [GM], where the same conclusion is proved for all finite simple groups. See also [Sh1], where it is shown that, for finite simple groups G and random elements $x, y \in G$, the sizes of $x^G y^G$ and of $(x^G)^2$ are $(1-o(1))|G|$. This may be viewed as a probabilistic approximation to Thompson's Conjecture.

For normal subsets S (not equal to $\varnothing, \{e\}$) of arbitrary finite simple groups G, the minimal $k > 0$ such that $S^k = G$ is determined in [LiSh2] up to an absolute multiplicative constant. In [LSSh] it is shown that the product of two small normal subsets of finite simple groups has size which is close to the product of their sizes. However, this says nothing about products of two large normal subsets.

An interesting context in which the products of normal subsets of finite simple groups play a role is the Waring problem for finite simple groups; see for instance [Sh2, LS1, LS2, LBST, LST1, GT, GLBST, LST2], the references therein, and the monograph [Se] on word width.

By a *word* we mean an element w of some free group F_d. A word w and a group G give rise to a word map $w : G^d \to G$ induced by substitution; its image, denoted by $w(G)$, is a normal subset of G (hence a union of conjugacy classes). The main result of [LST1] is that, for non-trivial words $w_1, w_2 \in F_d$, and all sufficiently large finite simple groups G we have

$$w_1(G)w_2(G) = G. \tag{1.1}$$

There are various results showing that word maps $w \neq 1$ on finite simple groups G have large image, see [La, LS1, LS2, NP]. In particular, it is shown in [La] that $|w(G)| \geq |G|^{1-\epsilon}$ for any $\epsilon > 0$ provided $|G| \geq N(\epsilon)$, and that for G of Lie type and bounded rank, there exists $\epsilon > 0$ (depending only on the rank of G) such that for all words $w \neq 1$ we have $|w(G)| \geq \epsilon|G|$. We would like to understand to what extent (1.1) can be extended to products of arbitrary large normal subsets of finite simple groups.

Let $\epsilon > 0$ be a constant. Let G be a finite simple group and S and T normal subsets of G such that $|S|, |T| > \epsilon|G|$. We are particularly interested in the following questions:

Question 1. *Does every element in $G \setminus \{e\}$ lie in ST if $|G|$ is sufficiently large?*

Question 2. *Does the ratio between the number of representations $g = st$ with $(s,t) \in S \times T$ for each $g \in G \setminus \{e\}$ and $\frac{|S||T|}{|G|}$ tend uniformly to 1 as $|G| \to \infty$?*

Question 3. *What happens in the special case $S = T$?*

We exclude the identity in Questions 1 and 2 because every conjugacy class C in a non-trivial finite group G satisfies $|C| = \frac{|G|}{n}$ for some $n \geq 2$, and therefore each such group has a normal subset S with $\frac{|G|}{3} \leq |S| \leq \frac{2|G|}{3}$. Setting $T = G \setminus S^{-1}$, we have $|T| \geq \frac{|G|}{3}$, and $e \notin ST$.

If G is non-trivial and we do not assume that $S, T \subseteq G$ are normal subsets, then we may choose $S, T \subseteq G$ of size at least $\lfloor \frac{|G|}{2} \rfloor$ such that $ST \not\supseteq G \setminus \{e\}$; indeed, fix $g \in G \setminus \{e\}$, choose S of the specified size, and let $T = G \setminus S^{-1}g$.

Our results about these questions are summarized below. An affirmative answer to Question 2 implies an affirmative answer to Question 1 (and, of course, the same holds in the special case $S = T$).

Theorem A. (i) *The answers to Questions 1 and 2 are negative if G is allowed to range over all finite simple groups, or even just over the alternating groups, or just over all projective special linear groups.*
(ii) *In the $S = T$ case, the answer to Question 2 is still negative for alternating groups.*
(iii) *In the $S = T$ case, the answer to Question 1 is positive for alternating groups.*
(iv) *If G is a group of Lie type of bounded rank, then the answers to Questions 1 and 2 are both positive.*

Our proof of part (iv) depends on a result which may be of independent interest, concerning the number of points in a finite product set inside a product variety which lie on a subvariety of the product variety. See Theorem 3.3 below.

We give an application of Theorem A to word maps. A more substantial application, to the question of whether every element in a finite simple transitive permutation group is a product of two derangements, is given in a companion paper [LST3].

Our paper is organized as follows. Sections 2 and 3 are devoted to algebro-geometric results that are needed in the proof of part (iv) of Theorem A, which

is carried out in Section 4. In Section 5 we prove part (i) of Theorem A for special linear groups. Section 6 is devoted to alternating groups and contains proofs of parts (i), (ii) and (iii) of Theorem A. In Section 7 we discuss products of three normal subsets. An application to word maps is presented in Section 8.

2. The Lang-Weil estimate

By a *variety* $\underline{X}$ over a field k, we mean a separated geometrically irreducible scheme of finite type over k. By the Lang-Weil theorem, if $k = \mathbb{F}_q$, then

$$\left| \, |\underline{X}(\mathbb{F}_{q^m})| - q^{m \dim \underline{X}} \, \right| \leq B q^{m(\dim \underline{X} - 1/2)} \tag{2.1}$$

for some constant B depending on $\underline{X}$ but not on m. We will need a number of variants of this statement; the reader who is willing to accept them can skip the remainder of this section.

For any separated scheme of finite type, the left hand side can be computed using the Lefschetz trace formula [SGA $4\frac{1}{2}$, Rapport, Théorème 3.2]:

$$|\underline{X}(\mathbb{F}_{q^m})| = \sum_{i=0}^{2 \dim \underline{X}} (-1)^i \mathrm{Tr}(\mathrm{Frob}_{q^m} | H^i_c(\bar{\underline{X}}, \mathbb{Q}_\ell)). \tag{2.2}$$

Let $d := \dim \underline{X}$. We fix an embedding $\iota \colon \mathbb{Q}_\ell \to \mathbb{C}$. A well-known theorem of Deligne [De, Théorème 3.3.4] asserts that each eigenvalue of Frob_q acting on $H^i_c(\bar{\underline{X}}, \mathbb{Q}_\ell)$ has absolute value $q^{w/2}$ for some non-negative integer $w \leq i$. In particular, the only i for which $H^i(\bar{\underline{X}}, \mathbb{Q}_\ell)$ has an eigenvalue of absolute value $\geq q^d$ is $i = 2d$. If these eigenvalues are $\alpha_1 q^d, \ldots, \alpha_k q^d$ (with repetitions allowed), then each α_i has absolute value 1, and (2.1) implies

$$\lim_{m \to \infty} \left(\alpha_1^m + \cdots + \alpha_k^m \right) = 1,$$

which implies $k = 1$ and $\alpha_1 = 1$. (In fact, geometric irreducibility implies that $H^{\dim \underline{X}}(\bar{\underline{X}}, \mathbb{Q}_\ell)$ is 1-dimensional and the trace map is an isomorphism.) Thus, in (2.1), the $q^{m \dim \underline{X}}$ term cancels the contribution of $i = 2 \dim \underline{X}$ in (2.2), and B can be taken to be the sum of the compactly supported Betti numbers of $\bar{\underline{X}}$. Note that B depends only on $\bar{\underline{X}}$, so this estimate holds uniformly for all Galois twists of $\underline{X}$.

If $\underline{X}$ ranges over the (geometrically irreducible) fibers of a morphism $\pi \colon \mathcal{X} \to \mathcal{S}$ between schemes of finite type over $\mathbb{Z}$, then B is bounded uniformly among all such fibers. This is a consequence of the proper base change theorem [SGA $4\frac{1}{2}$, Arcata, IV, Théorème 5.4] (which identifies the ith étale cohomology group with compact support of a geometric fiber with the corresponding fiber of $R^i \pi_! \mathbb{Q}_\ell$), Nagata's compactification theorem ([SGA $4\frac{1}{2}$, Arcata, IV, (5.3)]), and the constructibility [SGA $4\frac{1}{2}$, Finitude, Théorème 1.1] of the sheaves $R^i \pi'_* j_! \mathbb{Q}_\ell = R^i \pi_! \mathbb{Q}_\ell$ for a compactification

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{\ j\ } & \mathcal{X}' \\ & {\scriptstyle \pi} \searrow \quad \swarrow {\scriptstyle \pi'} & \\ & \mathcal{S} & \end{array}$$

As a consequence, there exists B such that for all q, all points $s \in \mathcal{S}$ with finite residue field $k(s) = \mathbb{F}_q$, all varieties $\underline{X}$ of the form $\underline{X} = \mathcal{X} \times_{\mathcal{S}} k(s)$, and all positive integers m,

$$\left| \, |\underline{X}(\mathbb{F}_{q^m})| - q^{m \dim \underline{X}} \, \right| \leq B q^{m(\dim \underline{X} - 1/2)}. \tag{2.3}$$

Given any integer r, there are only finitely many root systems of rank r, and for each root system Φ, there exists a Chevalley group scheme $\mathcal{G}$ over $\mathbb{Z}$, that is, a smooth group scheme over $\operatorname{Spec} \mathbb{Z}$, whose fiber over each field F is the connected, simply connected, split semisimple algebraic group over F with root system Φ. Thus, we can uniformly bound the sum of compactly supported Betti numbers for all semisimple groups of rank r over all algebraically closed fields.

Suppose $\underline{X}$ is a variety over $\mathbb{F}_q$ and $F \colon \underline{X} \to \underline{X}$ is an endomorphism of varieties over $\mathbb{F}_q$ such that $F^2 = \operatorname{Frob}_q$. Then for $f \in \mathbb{N}$ sufficiently large,

$$\left| \, |\underline{X}(\bar{\mathbb{F}}_q)^{F^{2f+1}}| - q^{(f+1/2)\dim \underline{X}} \, \right| < B q^{(f+1/2)(\dim \underline{X} - 1/2)}. \tag{2.4}$$

This follows from Fujiwara's extension of the Lefschetz trace formula [Va]. This allows us to treat Suzuki and Ree groups on the same footing as the other finite simple groups of Lie type.

If $\underline{Z}$ is a variety and $\underline{W}$ is a proper closed subvariety, then $\dim \underline{W} \leq \dim \underline{Z} - 1$, so

$$|\underline{W}(\mathbb{F}_q)| \leq B q^{\dim \underline{Z} - 1},$$

where B is the sum of Betti numbers of $\underline{W}$. As $\underline{Z}$ and $\underline{W}$ range over the fibers of a morphism of finite type over $\mathbb{Z}$, the constant B can be bounded uniformly as before.

If $\pi \colon \underline{Z} \to \underline{S}$ is a dominant morphism of $\mathbb{F}_q$-varieties whose generic fiber is geometrically irreducible, then there exists a proper closed subscheme $\underline{W}$ of $\underline{Z}$ such that the restriction of π to the complement of $\underline{W}$ is geometrically irreducible [EGA IV_3, Corollaire 9.7.9]. If B denotes the maximum sum of Betti numbers of any fiber of $\pi|_{\underline{Z} \smallsetminus \underline{W}}$, B' denotes the sum of Betti numbers of $\underline{W}$, and B'' denotes the sum of Betti numbers of $\underline{S}$, then for all $S \subset \underline{S}(\mathbb{F}_{q^m})$,

$$\begin{aligned} \left| \, |\pi^{-1}(S)| - |S| q^{m(\dim \underline{Z} - \dim \underline{S})} \, \right| &\leq B |S| q^{m(\dim \underline{Z} - \dim \underline{S}) - 1/2} + B' q^{m(\dim \underline{Z} - 1)} \\ &\leq (B + BB'' + B') q^{m(\dim \underline{Z}) - 1/2}. \end{aligned}$$

3. Morphisms which respect products

If $\pi \colon \underline{Z} \to \underline{S}$ is a morphism of varieties over $\mathbb{F}_q$, we denote by π_m the function $\underline{Z}(\mathbb{F}_{q^m}) \to \underline{S}(\mathbb{F}_{q^m})$ that it determines. Let $S_m \subset \underline{S}(\mathbb{F}_{q^m})$. We have seen that if π has geometrically irreducible generic fiber, then

$$|\pi_m^{-1}(S_m)| = q^{m(\dim \underline{Z} - \dim \underline{S})} |S_m| + O(q^{m((\dim \underline{Z}) - 1/2)}).$$

Applying Lang-Weil for $\underline{S}$ and $\underline{Z}$, this estimate can be expressed equivalently as

$$\frac{|\pi_m^{-1}(S_m)|}{|\underline{Z}(\mathbb{F}_{q^m})|} = \frac{|S_m|}{|\underline{S}(\mathbb{F}_{q^m})|} + O(q^{-m/2}). \tag{3.1}$$

All we actually need from the estimate (3.1) is the weaker version

$$\frac{|\pi_m^{-1}(S_m)|}{|\underline{Z}(\mathbb{F}_{q^m})|} = \frac{|S_m|}{|\underline{S}(\mathbb{F}_{q^m})|} + o(1), \tag{3.2}$$

or, equivalently,

$$\frac{|\pi_m^{-1}(S_m)|}{q^{m\dim \underline{Z}}} = \frac{|S_m|}{q^{m\dim \underline{S}}} + o(1). \tag{3.3}$$

We remark that in principle we have effective bounds for all the relevant Betti numbers if π is an explicit morphism of quasi-projective varieties, so we could replace $o(1)$ here and in what follows by an explicit multiple of an explicit negative power of q^m.

Conversely, if (3.2) holds for all S_m, then π is generically geometrically irreducible [LST2, Proposition 2.1].

Now, let $\underline{X}$, $\underline{Y}$, and $\underline{Z}$ denote varieties over $\mathbb{F}_q$ and $\pi\colon \underline{Z} \to \underline{X} \times \underline{Y}$ a morphism of $\mathbb{F}_q$-varieties. By Lang-Weil for $\underline{X}$, $\underline{Y}$, or $\underline{Z}$, we mean the $o(1)$ form of the error term rather than the $O(q^{-m/2})$ form.

Definition 3.1. *We say* π respects products *if, as* $m \to \infty$*, for all* $X_m \subset \underline{X}(\mathbb{F}_{q^m})$ *and* $Y_m \subset \underline{Y}(\mathbb{F}_{q^m})$*, we have*

$$\frac{|\pi_m^{-1}(X_m \times Y_m)|}{q^{m\dim \underline{Z}}} = \frac{|X_m \times Y_m|}{q^{m\dim \underline{X}\times\underline{Y}}} + o(1). \tag{3.4}$$

Alexis Chevalier pointed out to us that this definition and Theorem 3.3 below are very much in the spirit of Tao's algebraic regularity lemma [Ta].

It is clear that π respects products if it has geometrically irreducible generic fiber. The converse is not true, but we have the following weaker statement. Let $\pi_{\underline{X}}$ and $\pi_{\underline{Y}}$ denote the compositions of π with the projection morphisms from $\underline{X} \times \underline{Y}$ to $\underline{X}$ and $\underline{Y}$ respectively.

Lemma 3.2. *If* π *respects products, then* $\pi_{\underline{X}}$ *and* $\pi_{\underline{Y}}$ *are generically geometrically irreducible.*

Proof. By specializing to the case $X_m = \underline{X}(\mathbb{F}_{q^m})$, (3.4) becomes (3.3), which implies that $\pi_{\underline{Y}}$ is generically geometrically irreducible. By symmetry, the same is true for $\pi_{\underline{X}}$ as well. □

Note that just because $\pi_{\underline{X}}$ and $\pi_{\underline{Y}}$ are generically geometrically irreducible, it is not necessarily the case that π respects products. For example, if $\underline{X} = \operatorname{Spec} \mathbb{F}_q[x]$, $\underline{Y} = \operatorname{Spec} \mathbb{F}_q[y]$, and

$$\underline{Z} = \operatorname{Spec} \mathbb{F}_q[x, y, z]/(z^2 - xy),$$

π corresponds to the obvious homomorphism

$$\mathbb{F}_q[x] \otimes \mathbb{F}_q[y] \to \mathbb{F}_q[x, y, z]/(z^2 - xy),$$

and $X_m = Y_m$ is the set of squares of elements of $\mathbb{F}_{q^m}^\times$, then the left hand side of (3.4) approaches $1/2$, while the right hand side is $1/4 + o(1)$.

However, in many cases, the converse of Lemma 3.2 does hold. Suppose that $\pi_{\underline{Y}}$ is flat with geometrically irreducible generic fiber. As flatness is preserved by base change and the composition of flat morphisms is flat, $\underline{Z} \times_{\underline{Y}} \underline{Z}$ is flat over $\underline{Y}$, and this remains true after base change from $\mathbb{F}_q$ to $\bar{\mathbb{F}}_q$. By [EGA IV_2, 2.4.6], therefore, every geometric component of $\underline{Z} \times_{\underline{Y}} \underline{Z}$ dominates $\underline{Y} \times_{\operatorname{Spec} \mathbb{F}_q} \operatorname{Spec} \bar{\mathbb{F}}_q$. However, the generic fiber of $\underline{Z} \times_{\underline{Y}} \underline{Z}$ is geometrically irreducible [EGA IV_2, Corollaire 4.5.8], so there is only one geometric component, and $\underline{Z} \times_{\underline{Y}} \underline{Z}$ is therefore a variety.

Theorem 3.3. *Assume $\underline{Z}$ is flat over $\underline{Y}$. Let $\psi\colon \underline{Z} \times_{\underline{Y}} \underline{Z} \to \underline{X} \times \underline{X}$ denote the morphism of varieties given by $\psi(z_1, z_2) = (\pi_{\underline{X}}(z_1), \pi_{\underline{X}}(z_2))$. If ψ respects products and $\pi_{\underline{X}}$ and $\pi_{\underline{Y}}$ have geometrically irreducible generic fiber, then π respects products.*

Proof. Let $X_m \subset \underline{X}(\mathbb{F}_{q^m})$ and $Y_m \subset \underline{Y}(\mathbb{F}_{q^m})$ be subsets, Y_m^c the complement of Y_m in $\underline{Y}(\mathbb{F}_{q^m})$, and

$$Z_m := \pi_{\underline{X}}^{-1}(X_m) = \pi_m^{-1}(X_m \times \underline{Y}(\mathbb{F}_{q^m})).$$

As $\pi_{\underline{X}}$ has geometrically irreducible generic fiber,

$$\frac{|Z_m|}{q^{m \dim \underline{Z}}} = \frac{|X_m|}{q^{m \dim \underline{X}}} + o(1). \tag{3.5}$$

Since $X_m \subset \underline{X}(\mathbb{F}_{q^m})$,

$$\frac{|Z_m|^2}{q^{2m \dim \underline{Z}}} = \frac{|X_m|^2}{q^{2m \dim \underline{X}}} + o(1). \tag{3.6}$$

Let

$$\begin{aligned}
\Delta_m &:= |\pi_m^{-1}(X_m \times Y_m)|\,|Y_m^c| - |\pi_m^{-1}(X_m \times Y_m^c)|\,|Y_m| \\
&= |\pi_m^{-1}(X_m \times Y_m)|\,|\underline{Y}(\mathbb{F}_{q^m})| - |\pi_m^{-1}(X_m \times \underline{Y}(\mathbb{F}_{q^m}))|\,|Y_m| \\
&= |\pi_m^{-1}(X_m \times Y_m)|\,|\underline{Y}(\mathbb{F}_{q^m})| - |Z_m|\,|Y_m|.
\end{aligned}$$

We aim to prove an $o(1)$ bound for

$$\begin{aligned}
&\frac{|\pi_m^{-1}(X_m \times Y_m)|}{|\underline{Z}(\mathbb{F}_{q^m})|} - \frac{|X_m \times Y_m|}{|(\underline{X} \times \underline{Y})(\mathbb{F}_{q^m})|} \\
&\qquad = \frac{|\pi_m^{-1}(X_m \times Y_m)|\,|(\underline{X} \times \underline{Y})(\mathbb{F}_{q^m})| - |X_m \times Y_m|\,|\underline{Z}(\mathbb{F}_{q^m})|}{|(\underline{X} \times \underline{Y} \times \underline{Z})(\mathbb{F}_{q^m})|} \\
&\qquad = \frac{\Delta_m |\underline{X}(\mathbb{F}_{q^m})| + |Y_m|(|\underline{X}(\mathbb{F}_{q^m})|\,|Z_m| - |X_m|\,|\underline{Z}(\mathbb{F}_{q^m})|)}{|(\underline{X} \times \underline{Y} \times \underline{Z})(\mathbb{F}_{q^m})|} \\
&\qquad = \frac{\Delta_m}{|(\underline{Y} \times \underline{Z})(\mathbb{F}_{q^m})|} + \frac{|Y_m|}{|\underline{Y}(\mathbb{F}_{q^m})|}\Big(\frac{|Z_m|}{\underline{Z}(\mathbb{F}_{q^m})|} - \frac{|X_m|}{|\underline{X}(\mathbb{F}_{q^m})|}\Big).
\end{aligned} \tag{3.7}$$

By (3.5) and Lang-Weil for $\underline{Y}$ and $\underline{Z}$, this expression can be written

$$\frac{\Delta_m}{q^{m(\dim \underline{Y} + \dim \underline{Z})}} + o(1).$$

It suffices, therefore, to prove that

$$\Delta_m = o\big(q^{m(\dim \underline{Y}+\dim \underline{Z})}\big). \tag{3.8}$$

We have

$$\psi_m^{-1}(X_m \times X_m) = \{(z_1, z_2, y) \in Z_m \times Z_m \times \underline{Y}(\mathbb{F}_{q^m}) \mid \pi_{\underline{Y}}(z_1) = \pi_{\underline{Y}}(z_2) = y\},$$

so the cardinality of the left hand side is

$$\begin{aligned}
&\sum_{y \in \underline{Y}(\mathbb{F}_{q^m})} |\pi_m^{-1}(X_m \times \{y\})|^2 \\
&\quad = \sum_{y \in Y_m} |\pi_m^{-1}(X_m \times \{y\})|^2 + \sum_{y \in Y_m^c} |\pi_m^{-1}(X_m \times \{y\})|^2 \\
&\quad \geq \frac{\left(\sum_{y \in Y_m} |\pi_m^{-1}(X_m \times \{y\})|\right)^2}{|Y_m|} + \frac{\left(\sum_{y \in Y_m^c} |\pi_m^{-1}(X_m \times \{y\})|\right)^2}{|Y_m^c|} \\
&\quad = \frac{|\pi_m^{-1}(X_m \times Y_m)|^2}{|Y_m|} + \frac{|\pi_m^{-1}(X_m \times Y_m^c)|^2}{|Y_m^c|} \\
&\quad = \frac{(|\pi_m^{-1}(X_m \times Y_m)| + |\pi_m^{-1}(X_m \times Y_m^c)|)^2 + \frac{\Delta_m^2}{|Y_m|\,|Y_m^c|}}{|Y_m| + |Y_m^c|} \\
&\quad = \frac{|Z_m|^2 + \frac{\Delta_m^2}{|Y_m|\,|Y_m^c|}}{|\underline{Y}(\mathbb{F}_{q^m})|} \\
&\quad = \frac{q^{2m(\dim \underline{Z} - \dim \underline{X})}|X_m|^2 + \frac{\Delta_m^2}{|Y_m|\,|Y_m^c|}}{q^{m \dim \underline{Y}}} + o(q^{m(2\dim \underline{Z} - \dim \underline{Y})}),
\end{aligned} \tag{3.9}$$

by Cauchy-Schwarz, (3.6), and Lang-Weil for $\underline{Y}$. As ψ respects products,

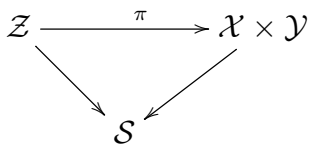
$$\frac{|\psi_m^{-1}(X_m \times X_m)|}{q^{m(2\dim \underline{Z} - \dim \underline{Y})}} = \frac{|X_m|^2}{q^{2m \dim \underline{X}}} + o(1). \tag{3.10}$$

Thus (3.9) implies

$$\frac{\Delta_m^2}{|Y_m|\,|Y_m^c|} = o(q^{2m \dim \underline{Z}}),$$

which, by Lang-Weil for $\underline{Y}$, gives (3.8). □

Note that the implicit bound of (3.7) can be expressed in terms of the implicit bounds in the Lang-Weil estimates of $\underline{X}$, $\underline{Y}$, and $\underline{Z}$ and those in (3.5) and (3.10). The uniformity (2.3) in Lang-Weil estimates for families over a scheme of finite type over $\mathbb{Z}$ implies the following. Let



be a morphism of schemes of finite type over $\mathbb{Z}$ for which the corresponding morphism $\pi_{\mathcal{Y}}\colon \mathcal{Z} \to \mathcal{Y}$ is flat. For each point s with finite residue field $k(s) = \mathbb{F}_q$, we consider the specialization $\underline{Z} \to \underline{X}\times\underline{Y}$ of π. Assuming that for some family of such morphisms we have a uniform $o(1)$ error bound for (3.10), then we have a uniform $o(1)$ error bound in (3.4) for all members of the family of morphisms. As Betti numbers depend only on cohomology after base change to $\bar{\mathbb{F}}_q$, we also have a uniform $o(1)$ error bound in (3.4) for morphisms obtained from members of the family by Galois twisting.

The estimate (2.4) gives a uniform $o(1)$ bound of type (3.4) in the setting of Suzuki and Ree groups. Explicitly, let $\pi\colon \underline{Z} \to \underline{X}\times\underline{Y}$ be a morphism of $\mathbb{F}_q$-varieties, and let $\psi\colon \underline{Z} \times_{\underline{Y}} \underline{Z} \to \underline{X} \times \underline{X}$ be defined as before. Suppose F_X, F_Y and F_Z are endomorphisms of $\underline{X}$, $\underline{Y}$, and $\underline{Z}$ as $\mathbb{F}_q$-varieties such that F_X^2, F_Y^2, and F_Z^2 are the q-Frobenius morphisms on $\underline{X}$, $\underline{Y}$, and $\underline{Z}$ respectively. Suppose further that the diagram

$$\begin{array}{ccc} \underline{Z} & \longrightarrow & \underline{X}\times\underline{Y} \\ {\scriptstyle F_Z}\downarrow & & \downarrow{\scriptstyle F_X\times F_Y} \\ \underline{Z} & \longrightarrow & \underline{X}\times\underline{Y} \end{array}$$

commutes. For f a non-negative integer, let

$$\pi_f\colon \underline{Z}(\bar{\mathbb{F}}_q)^{F^{2f+1}} \to \underline{X}(\bar{\mathbb{F}}_q)^{F^{2f+1}} \times \underline{Y}(\bar{\mathbb{F}}_q)^{F^{2f+1}},$$

denote the obvious restriction of π, and likewise for

$$\psi_f\colon (\underline{Z} \times_{\underline{Y}} \underline{Z})(\bar{\mathbb{F}}_q)^{F^{2f+1}} \to \underline{X}(\bar{\mathbb{F}}_q)^{F^{2f+1}} \times \underline{X}(\bar{\mathbb{F}}_q)^{F^{2f+1}}.$$

Let X and Y denote subsets of $\underline{X}(\bar{\mathbb{F}}_q)^{F^{2f+1}}$ and $\underline{Y}(\bar{\mathbb{F}}_q)^{F^{2f+1}}$. Then

$$\frac{|\psi_f^{-1}(X\times X)|}{q^{(f+1/2)\dim \underline{Z}\times_{\underline{Y}}\underline{Z}}} = \frac{|X\times X|}{q^{(f+1/2)\dim \underline{X}\times\underline{X}}} + o(1)$$

implies

$$\frac{|\pi_f^{-1}(X\times Y)|}{q^{(f+1/2)\dim \underline{Z}}} = \frac{|X\times Y|}{q^{(f+1/2)\dim \underline{X}\times\underline{Y}}} + o(1). \tag{3.11}$$

In applying Theorem 3.3 and its variants, we are always in the situation that $\pi_{\underline{Y}}$ is a projection map from a product variety to one of its factors. It is therefore flat (since every morphism to the spectrum of a field is flat, and flatness respects base change.)

4. Equidistribution for bounded rank groups of Lie type

In this section, we show that Questions 1 and 2 have an affirmative answer if one restricts to finite simple groups of bounded rank. Throughout the section, $\underline{G}$ denotes a simply connected simple algebraic group over $\mathbb{F}_q$.

Theorem 4.1. *If $c \in \underline{G}(\mathbb{F}_{q^m})$ is not central then for every integer $n \geq 2 \dim \underline{G}$, the morphism*

$$\phi \colon \underline{G}^{2n} \to \underline{G}$$

given by

$$\phi(x_1, y_1, \ldots, x_n, y_n) = x_1 c x_1^{-1} y_1 c^{-1} y_1^{-1} \cdots x_n c x_n^{-1} y_n c^{-1} y_n^{-1}$$

has geometrically irreducible generic fiber.

Proof. It suffices to prove that, fixing n,

$$|\phi_m^{-1}(g)| = (1 + o(1)) q^{m(2n-1)\dim \underline{G}} \tag{4.1}$$

for all $g \in \underline{G}(\mathbb{F}_{q^m})$ as $m \to \infty$. A well-known theorem of Frobenius asserts that if $C_1, \ldots, C_k$ are conjugacy classes in a finite group G and $g \in G$, then the number of elements in the set

$$\{(g_1, \ldots, g_k) \in C_1 \times \cdots \times C_k \mid g_1 \cdots g_k = g\}$$

is

$$\frac{|C_1| \cdots |C_k|}{|G|} \sum_{\chi} \frac{\chi(C_1) \cdots \chi(C_k) \bar{\chi}(g)}{\chi(1)^{k-1}}, \tag{4.2}$$

where the sum is taken over irreducible characters χ of G. Thus, if C is a conjugacy class in $\underline{G}(\mathbb{F}_{q^m})$, the number of representations

$$|\{(x_1, y_1, \ldots, x_n, y_n) \in C^{2n} \mid x_1 y_1^{-1} \cdots x_n y_n^{-1} = g\}|$$

is given by

$$\frac{|C|^{2n}}{|\underline{G}(\mathbb{F}_{q^m})|} \sum_{\chi} \frac{|\chi(C)|^{2n} \bar{\chi}(g)}{\chi(1)^{2n-1}},$$

Therefore,

$$|\phi_m^{-1}(g)| = |\underline{G}(\mathbb{F}_{q^m})|^{2n-1} \left(1 + \sum_{\chi \neq 1} \frac{|\chi(C)|^{2n} \bar{\chi}(g)}{\chi(1)^{2n-1}}\right).$$

By a theorem of Gluck [Gl], for every non-central element $x \in \underline{G}(\mathbb{F}_{q^m})$ and every non-trivial irreducible character χ, we have

$$\frac{|\chi(x)|}{\chi(1)} \leq a q^{-m/2},$$

where a is an absolute constant. As

$$|\chi(1)\bar{\chi}(g)| \leq \chi(1)^2 \leq |\underline{G}(\mathbb{F}_{q^m})| = (1 + o(1)) q^{m \dim \underline{G}},$$

we have

$$\frac{|\chi(C)^{2n} \bar{\chi}(g)|}{\chi(1)^{2n-1}} \leq (1 + o(1)) a^{2n} q^{m \dim \underline{G} - mn}.$$

The total number of irreducible characters is

$$o(|\underline{G}(\mathbb{F}_{q^m})|) = o(q^{m \dim \underline{G}}),$$

so $n \geq 2 \dim \underline{G}$ implies (4.1). □

Corollary 4.2. *With notations as above, If* $\theta^{(n)}\colon \underline{G}^{2n} \times \underline{G} \to \underline{G} \times \underline{G}$ *is defined by*

$$\theta^{(n)}(x_1, y_1, \dots, x_n, y_n, g) = (\phi(x_1, y_1, \dots, x_n, y_n)g, g),$$

then $\theta^{(n)}$ *has geometrically irreducible generic fiber.*

Proof. We have

$$|(\theta_m^{(n)})^{-1}(g_1, g_2)| = |\phi_m^{-1}(g_1 g_2^{-1})|.$$

By (4.1), the right hand side is always

$$(1 + o(1))q^{m(2n-1)\dim \underline{G}} = (1 + o(1))q^{m(\dim \underline{Z} - \dim \underline{X}\times\underline{Y})}.$$

The corollary follows from (3.1). □

Theorem 4.3. *Let* $\underline{X} = \underline{Y} = \underline{G}$ *and* $\underline{Z} = \underline{G} \times \underline{G}$. *Let* $\pi\colon \underline{Z} \to \underline{X} \times \underline{Y}$ *be defined by* $\pi(x, g) = (xcx^{-1}g, g)$. *Then* π *respects products.*

Proof. The isomorphism $\omega\colon \underline{Z} \times_{\underline{G}} \underline{Z} \to \underline{G}^2 \times \underline{G}$ defined by

$$\omega((x_1, g), (x_2, g)) = (x_1, x_2, x_2 c x_2^{-1} g)$$

makes the diagram

$$\begin{array}{ccc} \underline{Z} \times_{\underline{G}} \underline{Z} & \xrightarrow{\quad\omega\quad} & \underline{G}^2 \times \underline{G} \\ & {\scriptstyle\psi} \searrow \quad \swarrow {\scriptstyle\theta^{(1)}} & \\ & \underline{G} \times \underline{G} & \end{array}$$

commute. By Theorem 3.3, if π does not respect products, then $\theta^{(1)}$ does not respect them either.

For $n \geq 1$, we define

$$\xi^{(n)}\colon (\underline{G}^{2n} \times \underline{G}) \times_{\underline{G}} (\underline{G}^{2n} \times \underline{G}) \to (\underline{G}^{4n} \times \underline{G})$$

by

$$\begin{aligned} \xi^{(n)}((x_1, y_1, \dots, x_n, y_n, g), (x_{n+1}, y_{n+1} \dots, x_{2n}, y_{2n}, g)) \\ = (x_1, y_1, \dots, x_{2n}, y_{2n}, \phi(x_{n+1}, y_{n+1}, \dots, y_{2n})g) \end{aligned}$$

and

$$\eta^{(n)}\colon (\underline{G}^{2n} \times \underline{G}) \times_{\underline{G}} (\underline{G}^{2n} \times \underline{G}) \to \underline{G} \times \underline{G}$$

by

$$\begin{aligned} \eta^{(n)}((x_1, y_1, \dots, x_n, y_n, g),&(x_{n+1}, y_{n+1} \dots, x_{2n}, y_{2n}, g)) \\ &= (\phi(x_1, y_1, \dots, y_n)g, \phi(x_{n+1}, y_{n+1}, \dots, y_{2n})g), \end{aligned}$$

the diagram

$$\begin{array}{ccc} (\underline{G}^{2n} \times \underline{G}) \times_{\underline{G}} (\underline{G}^{2n} \times \underline{G}) & \xrightarrow{\quad\xi^{(n)}\quad} & \underline{G}^{4n} \times \underline{G} \\ & {\scriptstyle\eta^{(n)}} \searrow \quad \swarrow {\scriptstyle\theta^{(2n)}} & \\ & \underline{G} \times \underline{G} & \end{array}$$

commutes. Applying Theorem 3.3 in the case $\underline{X} = \underline{Y} = \underline{G}$, $\underline{Z} := \underline{G}^{2n} \times \underline{G}$, and $\pi = \theta^{(n)}$, so $\pi_{\underline{X}}$ and $\pi_{\underline{Y}}$ are both given by composing $\theta^{(n)}$ with projection to the first coordinate, and therefore ψ is $\eta^{(n)}$, we deduce that if $\theta^{(n)}$ does not respect products, $\theta^{(2n)}$ does not respect them either. Thus if $\theta^{(1)}$ does not respect products, by induction $\theta^{(2^i)}$ does not respect them either.

By Corollary 4.2, for i sufficiently large, $\theta^{(2^i)}$ is generically geometrically irreducible and therefore does respect products. The theorem follows. □

Theorem 4.4. *Given a simply connected simple algebraic group $\underline{G}$ over $\mathbb{F}_q$ and $\epsilon > 0$, there exists M such that if $m > M$, S and T are subsets of $\underline{G}(\mathbb{F}_{q^m})$ with at least $\epsilon q^{m \dim \underline{G}}$ elements, and C is a non-central conjugacy class of $\underline{G}(\mathbb{F}_{q^m})$, then the number of pairs $(s,t) \in S \times T$ with $st^{-1} \in C$ satisfies*

$$1 - \epsilon < \frac{|\{(s,t) \in S \times T \mid st^{-1} \in C\}|\,|\underline{G}(\mathbb{F}_{q^m})|}{|S|\,|T|\,|C|} < 1 + \epsilon. \tag{4.3}$$

Proof. If $c \in C$, the number of such pairs is $|\underline{G}(\mathbb{F}_{q^m})|^{-1}|C|$ times the number of solutions of $st^{-1} = xcx^{-1}$, $s \in S$, $t \in T$, $x \in \underline{G}(\mathbb{F}_{q^m})$. Theorem 4.3 implies the the number of such solutions is asymptotic to $|S|\,|T|$ as $m \to \infty$, which gives the theorem. □

Note that T^{-1} is normal, and $|T| = |T^{-1}|$, so the theorem gives equivalently

$$1 - \epsilon < \frac{|\{(s,t) \in S \times T \mid st \in C\}|\,|\underline{G}(\mathbb{F}_{q^m})|}{|S|\,|T|\,|C|} < 1 + \epsilon.$$

Note also that as the error $o(1)$ in Theorem 3.3 is uniform over all finite simple groups of bounded rank and all choices of c, the same is true for Theorem 4.4.

By the comments following the proof of Theorem 4.3, we have the following "Suzuki-Ree" version of Theorem 4.4:

Theorem 4.5. *Given a simply connected simple algebraic group $\underline{G}$ over $\mathbb{F}_q$ and an endomorphism F of $\underline{G}$ such that $F^2 = \mathrm{Frob}_q$, for all $\epsilon > 0$, there exists M such that if $f > M$, S and T are subsets of $G := \underline{G}(\bar{\mathbb{F}}_q)^{F^{2f+1}}$ with at least $\epsilon q^{(f+1/2)\dim \underline{G}}$ elements, and C is a non-central conjugacy class of G, then the number of pairs $(s,t) \in S \times T$ with $st^{-1} \in C$ satisfies*

$$1 - \epsilon < \frac{|\{(s,t) \in S \times T \mid st^{-1} \in C\}|\,|G|}{|S|\,|T|\,|C|} < 1 + \epsilon. \tag{4.4}$$

Theorem 4.6. *Let r and $\epsilon > 0$ be fixed. If G is the universal central extension of a finite simple group of Lie type of rank r and S and T are normal subsets with at least $\epsilon|G|$ elements each, the number of representations of any non-central element c as st, $s \in S$ and $t \in T$, is*

$$(1 + o(1))\frac{|S|\,|T|}{|G|}.$$

Proof. With finitely many exceptions, the universal central extension G of a finite simple group of Lie type is either of the form $\underline{G}(\mathbb{F}_{q^m})$, where $\underline{G}$ is a simply connected

simple algebraic group over $\mathbb{F}_q$, or is a Ree or Suzuki group. In the former case, the theorem is just Theorem 4.4; in the latter case, it is Theorem 4.5. □

Theorem 4.7. *Questions 1 and 2 have an affirmative answer for finite simple groups G of Lie type of bounded rank.*

Proof. Let $\tilde{G}$ denote the universal central extension of G, so we may assume either $\tilde{G} = \underline{G}(\mathbb{F}_q)$ for some simply connected simple algebraic group of bounded rank, or $\tilde{G} = \underline{G}(\bar{\mathbb{F}}_q)^{F^{2f+1}}$. Let $\pi\colon \tilde{G} \to G$ be the quotient map by the center of $\tilde{G}$. Let z denote the order of $\ker\pi$. If S and T are normal subsets of G, $\tilde{S} = \pi^{-1}(S)$ and $\tilde{T} = \pi^{-1}(T)$ are normal subsets of $\tilde{G}$ of cardinality $z|S|$ and $z|T|$ respectively. For any $c \in G$, the total number of representations of c as st, $s \in S$ and $t \in T$ is z^{-2} times the sum over the elements $\tilde{c} \in \pi^{-1}(c)$ of the number of representations of $\tilde{c}$ as $\tilde{s}\tilde{t}$ with $\tilde{s} \in \tilde{S}$, $\tilde{t} \in \tilde{T}$. For each of these z elements, the number of such representations is

$$(1+o(1))\frac{|\tilde{S}|\,|\tilde{T}|}{|\tilde{G}|} = (1+o(1))z\frac{|S|\,|T|}{|G|},$$

which gives the theorem. □

In principle, these $o(1)$ bounds are effective.

5. Behavior of $\mathrm{PSL}_n(q)$ for fixed q

In this section we prove that for q fixed and $n \to \infty$, the answer to Question 1 (and therefore also Question 2) is negative for the set of groups $\{\mathrm{PSL}_n(q) \mid n \geq 2\}$.

For $0 \leq m \leq n$, let $\mathrm{SL}_n(\mathbb{F}_q)_{[\geq m]}$ denote the set of elements $g \in \mathrm{SL}_n(\mathbb{F}_q)$ such that the dimension of the subspace $(\mathbb{F}_q^n)^{\langle g\rangle}$ of g-fixed points is at least m, and let $\mathrm{SL}_n(\mathbb{F}_q)_{[m]}$ denote the set of elements g for which the dimension of the g-fixed-point subspace is exactly m. Let $G_{k,m}$ denote the Grassmannian of m-dimensional $\mathbb{F}_q$-subspaces of a k-dimensional $\mathbb{F}_q$-vector space W. Its cardinality is the number of ordered linearly independent m-tuples in W divided by the number of ordered bases for a given m-dimensional subspace V, i.e.,

$$\frac{(q^k-1)(q^k-q)\cdots(q^k-q^{m-1})}{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})} < \frac{q^{m(k-m)}}{(1-q^{-1})\cdots(1-q^{-n})} < 4q^{m(k-m)} \tag{5.1}$$

since

$$\prod_{i=1}^{\infty}\frac{1}{1-q^{-i}} \leq \prod_{i=1}^{\infty}\frac{1}{1-2^{-i}} < 4.$$

On the other hand, there is an obvious lower bound, $|G_{k,m}| \geq q^{m(k-m)}$.

Lemma 5.1. *For $1 \leq m \leq n-1$, the cardinality of $\mathrm{SL}_n(\mathbb{F}_q)_{[\geq m]}$ is less than*

$$16q^{-m^2}|\mathrm{SL}_n(\mathbb{F}_q)|.$$

Proof. As $\mathrm{SL}_n(\mathbb{F}_q)$ acts transitively on linearly independent m-tuples in $\mathbb{F}_q^n$, the index of the stabilizer of an ordered linearly independent m-tuple is

$$(q^n-1)(q^n-q)\cdots(q^n-q^{m-1}) > \frac{q^{nm}}{4},$$

so the number of elements of $\mathrm{SL}_n(\mathbb{F}_q)$ in the pointwise stabilizer $\mathrm{Stab}(V)$ of a given m-dimensional subspace V satisfies

$$\frac{|\mathrm{SL}_n(\mathbb{F}_q)|}{q^{mn}} \leq |\mathrm{Stab}(V)| < \frac{4|\mathrm{SL}_n(\mathbb{F}_q)|}{q^{mn}}. \tag{5.2}$$

The lemma follows by combining the upper bound with (5.1). □

Note that this lemma does not cover the case $m = n$, but the bound $16q^{1-m^2}|\mathrm{SL}_n(\mathbb{F}_q)|$ works also for $m = n$ since it is greater than $4 > 1$ in this case.

Lemma 5.2. *The number of elements in* $\mathrm{SL}_n(\mathbb{F}_q)_{[m]}$ *is at least*

$$(1-128q^{-m})q^{-m^2}|\mathrm{SL}_n(\mathbb{F}_q))|. \tag{5.3}$$

Proof. Let $\mathrm{Stab}(V)$ denotes the pointwise stabilizer in $\mathrm{SL}_n(\mathbb{F}_q)$ of $V \in G_{n,m}$. Then,

$$\begin{aligned}
\sum_{V\in G_{n,m}} |\mathrm{Stab}(V)| &= \sum_{k=m}^{n} |\mathrm{SL}_n(\mathbb{F}_q)_{[k]}|\,|G_{k,m}| \\
&= |\mathrm{SL}_n(\mathbb{F}_q)_{[m]}| + \sum_{k=m+1}^{n} |\mathrm{SL}_n(\mathbb{F}_q)_{[k]}|\,|G_{k,m}| \\
&\leq |\mathrm{SL}_n(\mathbb{F}_q)_{[m]}| + 4\sum_{k=m+1}^{n} |\mathrm{SL}_n(\mathbb{F}_q)_{[k]}|q^{m(k-m)} \\
&\leq |\mathrm{SL}_n(\mathbb{F}_q)_{[m]}| + 64|\mathrm{SL}_n(\mathbb{F}_q)|\sum_{k=m+1}^{n} q^{1-k^2}q^{m(k-m)} \\
&= |\mathrm{SL}_n(\mathbb{F}_q)_{[m]}| + 64q^{1-m^2}|\mathrm{SL}_n(\mathbb{F}_q)|\sum_{k=m+1}^{n} q^{k(m-k)} \\
&\leq |\mathrm{SL}_n(\mathbb{F}_q)_{[m]}| + 128q^{-m^2}q^{-m}|\mathrm{SL}_n(\mathbb{F}_q)|.
\end{aligned}$$

By the lower bound in (5.2) and the trivial lower bound for the cardinality of a Grassmannian,

$$q^{-m^2}|\mathrm{SL}_n(\mathbb{F}_q)| \leq \sum_{V\in G_{n,m}} |\mathrm{Stab}(V)|.$$

Combining these inequalities, we get (5.3). □

We can now answer Question 1 for fixed q.

Theorem 5.3. *If q is fixed, there exist normal subsets $S_n, T_n \subset \mathrm{SL}_n(\mathbb{F}_q)$ such that S_nT_n does not contain any transvection, and*

$$\liminf_n \frac{|S_n|}{|\mathrm{SL}_n(\mathbb{F}_q)|}, \liminf_n \frac{|T_n|}{|\mathrm{SL}_n(\mathbb{F}_q)|} > 0. \tag{5.4}$$

Proof. For small n, we can take $S_n = T_n = \{e\}$, so without loss of generality, we may assume $n \geq 10$. Let $S_n = \mathrm{SL}_n(\mathbb{F}_q)_{[8]}$ and $T_n = \mathrm{SL}_n(\mathbb{F}_q)_{[10]}$. By (5.3),

$$\liminf_n \frac{|S_n|}{|\mathrm{SL}_n(\mathbb{F}_q)|}, \liminf_n \frac{|T_n|}{|\mathrm{SL}_n(\mathbb{F}_q)|} > 0.$$

Let $\sigma \in S_n$ and $\tau \in T_n$. If $\rho := \sigma\tau$ were a transvection, then it would fix a codimension 1 subspace $V' \subset \mathbb{F}_q^n$ pointwise, while τ fixes a 10-dimensional subspace $V \subset \mathbb{F}_q^n$ pointwise. This implies that σ fixes $V \cap V'$, which is of dimension ≥ 9 pointwise, contrary to the definition of S_n. □

Corollary 5.4. *For each fixed prime power q, Question 1 has a negative answer for the set of groups $\{\mathrm{PSL}_n(q) \mid n \geq 2,\ \gcd(n, q-1) = 1\}$.*

Proof. For n relatively prime to $q-1$, we have an isomorphism $\mathrm{SL}_n(\mathbb{F}_q) \to \mathrm{PSL}_n(q)$, so the corollary follows. □

6. Alternating groups

For alternating groups, we can prove an even stronger negative result.

Theorem 6.1. *If $0 \leq s, t \leq 1$ then there exists an infinite sequence of pairs of normal subsets $S_n, T_n \subset \mathsf{A}_n$, $n \geq 3$, such that*

$$\lim_{n\to\infty} \frac{|S_n|}{|\mathsf{A}_n|} = s,\ \lim_{n\to\infty} \frac{|T_n|}{|\mathsf{A}_n|} = t, \tag{6.1}$$

and S_nT_n contains no 3-cycle if and only if $s + t \leq 1$. In particular, Question 1 has a negative answer for alternating groups.

We begin with two lemmas. For $\sigma \in \mathsf{S}_n$, let $\mathsf{cyc}(\sigma)$ denote the total number of cycles of σ, i.e., the number of orbits of $\langle\sigma\rangle$ on $\{1, 2, \ldots, n\}$.

Lemma 6.2. *If $\sigma, \tau \in \mathsf{A}_n$ and $\sigma\tau$ is a 3-cycle, then*

$$\mathsf{cyc}(\tau) - \mathsf{cyc}(\sigma) \in \{-2, 0, 2\}. \tag{6.2}$$

Proof. For all elements $\sigma \in \mathsf{A}_n$, $n - \mathsf{cyc}(\sigma)$ is even. Thus, it suffices to prove that

$$|\mathsf{cyc}(\tau) - \mathsf{cyc}(\sigma)| \leq 3.$$

Every cycle of σ which is disjoint from the support of $\sigma\tau$ is also a cycle of τ. There are at most three cycles of σ which meet the support of $\sigma\tau$, so

$$\mathsf{cyc}(\tau) \geq \mathsf{cyc}(\sigma) - 3.$$

By the same argument,

$$\mathsf{cyc}(\sigma) = \mathsf{cyc}(\sigma^{-1}) \geq \mathsf{cyc}(\tau^{-1}) - 3 = \mathsf{cyc}(\tau) - 3.$$

□

Lemma 6.3. *Let m be a fixed positive integer. For any integer a, the number of elements $\sigma \in \mathsf{S}_n$ such that $\mathsf{cyc}(\sigma) \equiv a \pmod m$ is $(m^{-1} + o(1))n!$.*

Proof. Let $P_{n,m,a}$ denote the number of such elements, and let $\omega \in \mathbb{C}$ satisfy $\omega^m = 1$. Then,

$$Q_{n,m,\omega} := \sum_{a=0}^{m-1} \omega^a P_{n,m,a} = \sum_{k=0}^{n} \omega^k s(n,k),$$

where $s(n,k)$ is the Stirling number of the first kind, which by [St, Proposition 1.3.7] is the x^k coefficient of $x(x+1)\cdots(x+n-1)$. Thus,

$$Q_{n,m,\omega} = \omega(\omega+1)\cdots(\omega+n-1) = \frac{\Gamma(\omega+n)}{\Gamma(\omega)},$$

where $\Gamma(\cdot)$ is the gamma-function. Stirling's approximation [WW, 12.33] gives

$$\log\Gamma(z) = (z - \frac{1}{2})\log z - z + \frac{\log 2\pi}{2} + O(|z|^{-1})$$

for $\arg(z) \in [\epsilon - \pi/2, \pi/2 - \epsilon]$ for each fixed $\epsilon > 0$. In particular, taking $\epsilon < \pi/3$, this estimate holds for $\omega + n$ for all ω on the unit circle and all $n \geq 2$. As

$$\log(\omega+n) = \log n + O(n^{-1}),$$

$$\log\Gamma(\omega+n) = (n + \Re(\omega) - \frac{1}{2})\log n - \log n + O(1),$$

so

$$|\Gamma(\omega+n)| = O(n^{\Re(\omega)-1}\Gamma(n+1)).$$

Together with the functional equation $\Gamma(z+1) = z\Gamma(z)$, Stirling's approximation implies that Γ has no zeroes, so

$$Q_{n,m,\omega} = O(\Gamma(\omega+n)) = O(n^{\Re(\omega)-1}\Gamma(n+1)).$$

In particular, for $\omega \neq 1$, we have

$$Q_{n,m,\omega} = o(Q_{n,m,1}),$$

so

$$P_{n,m,a} = \frac{1}{m} \sum_{\{\omega | \omega^m = 1\}} \omega^{-a} Q_{n,m,\omega} = (m^{-1} + o(1))Q_{n,m,1} = (m^{-1} + o(1))n!. \tag{6.3}$$

□

We can now prove Theorem 6.1.

Proof. A permutation $\sigma \in \mathsf{S}_n$ is even if and only if $\mathsf{cyc}(\sigma) \equiv n \pmod 2$. Therefore, if m is odd,

$$|\{\sigma \in \mathsf{A}_n \mid \mathsf{cyc}(\sigma) \equiv a \pmod m\}| = (m^{-1} + o(1))|\mathsf{A}_n|.$$

If $s + t \leq 1$, by (6.3), we can choose for each n, an odd integer m_n in such a way that $m_n \to \infty$ as $n \to \infty$ and

$$\sup_a \frac{|m_n P_{n,m_n,a} - n!|}{n!} \to 0. \tag{6.4}$$

Now we can choose $k_n < l_n \leq m_n$ such that $k_n/m_n \to s$ and $(l_n - k_n)/m_n \to t$, and let $S_n \subset \mathsf{A}_n$ consist of all even permutations σ with $\mathsf{cyc}(\sigma)$ congruent to any element of $\{2, 4, \ldots, 2k_n - 2\} \pmod{m_n}$, and T_n consist of all even permutations τ with $\mathsf{cyc}(\tau)$ congruent to any element of $\{2k_n + 2, 2k_n + 4, \ldots, 2l_n - 2\} \pmod{m_n}$. Then by (6.2), $S_n T_n$ does not contain any 3-cycle. By construction, (6.4) implies (6.1).

If $s + t > 1$ then $|S_n| + |T_n| > \frac{n!}{2}$ for all $n \gg 0$, so $S_n T_n = \mathsf{A}_n$ follows immediately. □

In the case $S = T$, Question 1 has a positive answer for alternating groups.

Theorem 6.4. *If $0 < \epsilon < 1$, $n > e^{1000/\epsilon}$, and S is a normal subset of A_n containing at least $\epsilon|\mathsf{A}_n|$ elements, then $S^2 = \mathsf{A}_n$.*

To prove this we need two preliminary lemmas. The first is an explicit special case of a theorem of Müller and Schlage-Puchta [MSP1, Corollary 2], which is concerned with the Witten zeta-function of finite groups, studied in [LiSh1, LiSh2, LiSh3]. Recall that for a finite group G, the zeta-function $\zeta^G : \mathbb{R} \to \mathbb{R}$ is defined as

$$\zeta^G(s) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-s}. \tag{6.5}$$

Lemma 6.5. *If $n > e^{1000/\epsilon}$, then*

$$\zeta^{\mathsf{S}_n}(0.01) - 2 < \frac{\epsilon}{4}. \tag{6.6}$$

Proof. We follow the argument in [LiSh1]. Let $\lambda \vdash n$ be a partition and χ_λ the corresponding character of S_n. If λ' denotes the transpose, then χ_λ and $\chi_{\lambda'}$ have the same degree, so writing Λ_n for the set of $\lambda \vdash n$ such that $\lambda'_1 \leq \lambda_1 < n$, it suffices to prove

$$\sum_{\lambda \in \Lambda_n} \chi_\lambda(1)^{-1/100} < \frac{\epsilon}{8}.$$

By [LiSh1, Proposition 2.5], if $\lambda_1' \le \lambda_1 < (1-\frac{1}{8e})n$, then $\chi_\lambda(1) \ge 2^{n/8e-1} > 2^{n/16e}$ as $n > 16e$. By the same proposition, if $\lambda_1 > 2n/3$, then $\chi_\lambda(1) \ge \left(\frac{2n}{3}\right)^{n-\lambda_1}$. Thus,

$$\begin{aligned}\sum_{\lambda\in\Lambda_n} \chi_\lambda(1)^{-1/100} &= \sum_{\{\lambda\in\Lambda_n|\lambda_1\le 2n/3\}} \chi_\lambda(1)^{-1/100} + \sum_{\{\lambda\in\Lambda_n|\lambda_1>2n/3\}} \chi_\lambda(1)^{-1/100} \\ &< p(n)2^{-n/1600e} + \sum_{1\le l<n/3} p(l)\Big(\frac{2n}{3}\Big)^{-l/100},\end{aligned} \tag{6.7}$$

where $p(\cdot)$ denotes the partition function.

By a well known bound [Ap, Theorem 14.5], $p(x) \le e^{\pi\sqrt{2/3}\sqrt{x}} < 16^{\sqrt{x}} \le 16^x$. As

$$\frac{2n}{3} > 10^{899}(e^{1/\epsilon})^{100} > 10^{300}\epsilon^{-100},$$

we have $16^l(2n/3)^{-l/100} < (\epsilon/50)^l$, so the second summand on the right hand side of (6.7) is less than $\epsilon/10$. On the other hand, $n > (4\cdot 3200e)^2$, so $4\sqrt{n} < n/3200e$, and the first summand on the right hand side of (6.7) is less than

$$2^{-n/3200e} = e^{-n\log 2/3200e} < e^{-e^{900/\epsilon}} < e^{-900/\epsilon} < \frac{\epsilon}{900},$$

proving (6.6). □

Next we need an explicit version of a result of Erdős-Turán.

Lemma 6.6. *If $n > e^{1000/\epsilon}$, then the number of elements $\sigma \in \mathsf{S}_n$ with more than $2\log n$ cycles is less than $n^{-0.3}|\mathsf{S}_n|$.*

Proof. Setting $x = 2$ in $x(x+1)\cdots(x+n-1)$, we obtain

$$2^{2\log n}\sum_{k\ge 2\log n} s(n,k) < \sum_{k\ge 0} 2^k s(n,k) = (n+1)!.$$

Thus,

$$\sum_{k\ge 2\log n} s(n,k) < \frac{n+1}{n^{2\log 2}}n! = \frac{1+n^{-1}}{n^{2\log 2-1}}n!.$$

As $n > e^{1000}$ and $2\log 2 > 1.38$, the lemma holds. □

We can now prove Theorem 6.4.

Proof. The number of elements $\sigma \in \mathsf{A}_n$ such that $\sigma^{\mathsf{A}_n} \ne \sigma^{\mathsf{S}_n}$ is less than

$$\frac{2|\mathsf{A}_n|}{\log n/e} < \frac{2|\mathsf{A}_n|}{1000/\epsilon - 1} < \frac{\epsilon}{400}|\mathsf{A}_n|,$$

so, in particular, this is true for the number of elements $\sigma \in S$ for which $\sigma^{\mathsf{A}_n} \ne \sigma^{\mathsf{S}_n}$.

For any irreducible character χ, the number of elements $\sigma \in \mathsf{S}_n$ such that

$$|\chi(\sigma)| > \chi(1)^{.01}$$

is less than $|\mathsf{S}_n|\chi(1)^{-.02}$. By (6.6), the number of elements $\sigma \in \mathsf{S}_n$ for which this holds for any irreducible character χ of degree > 1 is less than

$$|\mathsf{S}_n| \sum_{\chi(1)>1} \chi(1)^{-.02} < |\mathsf{S}_n| \sum_{\chi(1)>1} \chi(1)^{-.01} < \frac{\epsilon|\mathsf{A}_n|}{2},$$

so the same holds for the number of elements $\sigma \in S$ satisfying $|\chi(\sigma)| > \chi(1)^{.01}$ for some irreducible character of degree > 1.

By Lemma 6.6, the number of elements of A_n consisting of more than $2\log n$ cycles is less than

$$e^{-300/\epsilon}|\mathsf{S}_n| < \frac{\epsilon}{300}|\mathsf{S}_n| = \frac{\epsilon}{150}|\mathsf{A}_n|.$$

Therefore, there exists $\sigma \in S$ with less than $2\log n$ cycles, such that

$$|\chi(\sigma)| \leq \chi(1)^{.01} \tag{6.8}$$

for all irreducible characters of S_n, and such that $\sigma^{\mathsf{A}_n} = \sigma^{\mathsf{S}_n}$. We claim that every element of A_n is the product of two elements of σ^{A_n} or, equivalently, that every even element of S_n is a product of two elements of σ^{S_n}.

Let τ be any even permutation. Suppose that τ has less than $14\log n < n^{1/13}$ fixed points. By a theorem of Müller and Schlage-Puchta [MSP2, Theorem B],

$$|\chi(\tau)| \leq \chi(1)^{31/32} \leq \chi(1)^{.97}. \tag{6.9}$$

for every irreducible character χ of S_n, since $n > e^{14}$.

Applying the Frobenius formula (4.2) with $C_1 = C_2 = \sigma^{\mathsf{S}_n}$ and $g = \tau$, to conclude that $\tau \in \sigma^{\mathsf{S}_n}\sigma^{\mathsf{S}_n}$, it suffices to know that

$$\sum_{\chi\in\mathrm{Irr}(\mathsf{S}_n),\ \chi(1)>1} \frac{|\chi(\sigma)|^2|\chi(\tau)|}{\chi(1)} < 2.$$

By (6.8) and (6.9), it suffices to show

$$\sum_{\chi\in\mathrm{Irr}(\mathsf{S}_n),\ \chi(1)>1} \chi(1)^{-0.01} < 2,$$

and that follows immediately from (6.6).

Finally, we consider the case that τ has at least $14\log n$ fixed points. Then it has at least 7 times as many fixed points as σ has cycles, and the fact that τ is a product of two conjugates of σ follows from [LS1, Proposition 6.1]. □

On the other hand, we have the following theorem.

Theorem 6.7. *Even in the case $S = T$, Question 2 has a negative answer for alternating groups.*

Proof. We prove that if, for each n, $S_n = T_n$ denotes the set of derangements in A_n, then $|S_n| = |T_n| \sim \frac{n!}{2e}$ and the number of representations of any 3-cycle as st, $s \in S_n$ and $t \in T_n$, is also asymptotic to $\frac{n!}{2e}$.

The first claim is an analogue of a well-known fact about derangements in S_n, and the argument is the same. As A_n acts $(n-2)$-transitively on $X_n = \{1, 2, \ldots, n\}$, for

each subset Σ of X_n with $\leq n-2$ elements, the number of elements in A_n which fix Σ pointwise is

$$\frac{n!}{2(n-|\Sigma|)!}.$$

Therefore,

$$\sum_{|\Sigma|=r\leq n-2} |\mathrm{Stab}_{\mathsf{A}_n}\Sigma| = \frac{n!}{2r!}.$$

By the Bonferroni inequalities, the number of derangements in A_n lies between any two consecutive values of the sequence

$$\sum_{r=0}^{n-3} \frac{(-1)^r n!}{2\,r!},$$

where $r = 1, 2, \ldots, n-2$, implying the first claim.

For the second claim, it suffices to prove that in the limit $n \to \infty$, the probability approaches 1 that the product of a given 3-cycle in A_n and a uniformly distributed random element should again be a derangement approaches 1. Without loss of generality, we take our fixed 3-cycle to be $\sigma = (123)$ and let τ denote a random derangement in A_n. Then $\tau\sigma$ can fix only 1, 2, or 3. It fixes 1 if and only if $\tau(2) = 1$, and likewise for 2 and 3. By symmetry, the probability that $\tau(2) = 1$ is the same as the probability that $\tau(2)$ takes any other value in $X_n \smallsetminus \{2\}$, i.e., $\dfrac{1}{n-1}$. Thus, the probability that $\tau\sigma$ is a derangement is at least $1 - \dfrac{3}{n-1}$. □

7. Products of three normal subsets

While Questions 1 and 2 have negative answers for general finite simple groups, the analogous questions for products of three normal subsets of arbitrary finite simple groups G have a positive answer. This follows easily and effectively from existing results, even without assuming the normality of the subsets.

By the so-called Gowers trick (see Gowers [Go] and Nikolov-Pyber [NP]), if G is a finite group, $m(G)$ is the minimal degree of a non-trivial character of G, and $A, B, C \subseteq G$ satisfy

$$|A|\,|B|\,|C| \geq \frac{|G|^3}{m(G)},$$

then $ABC = G$. Thus Question 1 for three arbitrary subsets has a positive answer, with $\epsilon = m(G)^{-1/3}$; this holds also for general *quasi-random* families of non-simple groups, that is, provided $m(G) \to \infty$ as $|G| \to \infty$.

Question 2 for $t \geq 3$ subsets is solved in[BNP, 2.8], which we quote below.

Theorem 7.1. *Let G be a finite group, $t \geq 3$ an integer, and $\alpha > 0$. Let $C_1, \dots, C_t$ be subsets of G which satisfy*

$$\prod_{i=1}^{t} |C_i| \geq \alpha \frac{|G|^t}{m(G)^{t-2}}.$$

For $g \in G$ let N_g denote the number of solutions to the equation $x_1 \cdots x_t = g$ with $x_i \in C_i$ $(i = 1, \dots, t)$. Set

$$E = \frac{\prod_{i=1}^{t} |C_i|}{|G|}.$$

Then, for every $g \in G$ we have

$$|N_g - E| \leq \alpha^{-1/2} E.$$

For a group G and subsets $C_1, \dots, C_t$ of G, denote by $\mathbf{P}_{C_1,\dots,C_t}$ the probability distribution on G such that, for $g \in G$, $\mathbf{P}_{C_1,\dots,C_t}(g)$ is the probability that $x_1 \cdots x_t = g$ where $x_i \in C_i$ $(i = 1, \dots, t)$ are randomly chosen, uniformly and independently.

We also denote by $\mathbf{U}_G$ the uniform distribution on G.

Theorem 7.1 for $t = 3$ yields the following.

Corollary 7.2. *For finite groups G, and subsets $A, B, C \subseteq G$ satisfying*

$$m(G)|A|\,|B|\,|C|/|G|^3 \to \infty$$

as $|G| \to \infty$, we have

$$\|\mathbf{P}_{A,B,C} - \mathbf{U}_G\|_{L^\infty} \to 0 \text{ as } |G| \to \infty.$$

In particular we have $ABC = G$ for $|G| \gg 0$.

These two conclusions hold when G is a finite simple group and $A, B, C \subseteq G$ are subsets of sizes $\geq \epsilon|G| > 0$ for any fixed $\epsilon > 0$.

For finite simple classical groups G and normal subsets $R, S, T \subseteq G$ we can obtain $RST = G$ under asymptotically weaker assumptions. The proof uses character methods.

Suppose C_i above are conjugacy classes of G. Then (4.2) implies that

$$\mathbf{P}_{C_1,C_2,C_3}(g) = |G|^{-1} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C_1)\chi(C_2)\chi(C_3)\chi(g^{-1})}{\chi(1)^2},$$

where $\chi(C_i)$ is the common value of χ on elements of C_i.

Since $|\chi(g^{-1})|/\chi(1) \leq 1$, this yields

$$|\mathbf{P}_{C_1,C_2,C_3}(g) - |G|^{-1}| \leq \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(C_1)|\,|\chi(C_2)|\,|\chi(C_3)|}{\chi(1)}. \tag{7.1}$$

Denote by $\mathrm{Cl}_n(q)$ the set of finite simple classical groups over $\mathbb{F}_q$ with an n-dimensional natural module. We need the following slight extension of [GLT, 7.5] and its proof.

Proposition 7.3. *There exists an absolute constant $0 < \gamma < 1$ such that the following holds. Suppose $n \geq 9$, $G \in \mathrm{Cl}_n(q)$, and for $i = 1, 2, 3$ let $g_i \in G$ satisfy $|\mathbf{C}_G(g_i)| \leq |G|^\gamma$. Set $C_i = g_i^G$ $(i = 1, 2, 3)$. Then we have*

(i) $\lim_{|G|\to\infty} \|\mathbf{P}_{C_1,C_2,C_3} - \mathbf{U}_G\|_\infty = 0$.
(ii) *There exists an absolute constant N such that, if $|G| \geq N$, then $C_1C_2C_3 = G$.*

Proof. By Theorem 1.3 of [GLT] we may choose $0 < \gamma < 1$ such that, if $g \in G$ satisfies $|\mathbf{C}_G(g)| \leq |G|^\gamma$, then $|\chi(g)| \leq \chi(1)^{1/4}$ for all $\chi \in \mathrm{Irr}(G)$.

Let g_i, C_i be as in the statement of the proposition. Then $|\chi(g_i)| \leq \chi(1)^{1/4}$, and therefore inequality (7.1) above shows that

$$|\mathbf{P}_{C_1,C_2,C_3}(g) - |G|^{-1}| \leq |G|^{-1} \sum_{1\neq\chi\in\mathrm{Irr}(G)} \chi(1)^{-1/4} = |G|^{-1}(\zeta^G(1/4) - 1);$$

recall (6.5) for the definition of ζ^G. By [LiSh3, 1.1] and our assumptions on G, it follows that $\zeta^G(1/4) - 1 \to 0$ as $|G| \to \infty$. This completes the proof of part (i).

Part (ii) follows from part (i) and the effective nature of the proof of [LiSh3, 1.1]. □

We note that the results [Sh2, 2.4, 2.5] provide a weaker version of Proposition 7.3. More specifically, these results show that the conclusions of Proposition 7.3 hold if we assume

$$|\mathbf{C}_G(g_i)| \leq q^{(4/3-\delta)r},\ i = 1, 2, 3$$

for any fixed $\delta > 0$ and $N = N(\delta)$.

Proposition 7.3 easily implies the following.

Theorem 7.4. *There exist an absolute constant $\delta > 0$ and an integer N such that the following holds. Suppose $n \geq N$, $G \in \mathrm{Cl}_n(q)$, and $R, S, T \subseteq G$ are normal subsets satisfying $|R|, |S|, |T| \geq |G|^{1-\delta}$. Then $RST = G$.*

Proof. Let γ be as in Proposition 7.3, and define, say, $\delta = \gamma/2$.

Suppose G above has rank r. Then, by [FG], we have $k(G) \leq cq^r$, for a small absolute constant $c > 0$. Clearly, R, S, T contain conjugacy classes C_1, C_2, C_3 respectively satisfying

$$|C_i| \geq \frac{|G|^{1-\delta}}{k(G)} \geq c^{-1}q^{-r}|G|^{1-\delta} \geq |G|^{1-\gamma/2-o_r(1)} \geq |G|^{1-\gamma},$$

provided N is large enough and $r \geq N$.

It follows from Proposition 7.3 that (enlarging N if needed) $C_1C_2C_3 = G$ and hence $RST = G$. □

8. An application to word maps

Probabilistic Waring problems for finite simple groups are studied [LST2]. For a word $w \in F_d$ and a finite group G, let $\mathbf{P}_{w,G}$ denote the probability induced by the corresponding word map $w : G^d \to G$, namely

$$\mathbf{P}_{w,G}(g) = |w^{-1}(g)|/|G|^d$$

for $g \in G$.

It is shown in [LST2, Theorem 4] that for every $\ell \in \mathbb{N}$ there exists $N = N(\ell)$ such that, if $w_1, \ldots, w_N \in F_d$ are non-trivial words in pairwise disjoint sets of variables, all of length at most ℓ, then

$$\|\mathbf{P}_{w_1 \cdots w_N, G} - \mathbf{U}_G\|_\infty \to 0 \text{ as } |G| \to \infty,$$

where G ranges over the finite simple groups. The dependence of N on ℓ in that result is genuine and explicit: $N(\ell) = 2 \cdot 10^{18} \cdot \ell^4$.

It turns out that, if we change the probabilistic model, let G be a finite simple group of Lie type, choose random elements $g_i \in w_i(G)$ $(i = 1, \ldots, N)$ and study the distribution of $g_1 \cdots g_N$, we obtain an almost uniform distribution in L^∞ much faster, namely in three steps.

We would like to thank Saveliy Skresanov for pointing out an error in the statement of the following theorem in the published version of this paper.

Theorem 8.1. *Let $w_1, w_2, w_3 \in F_d$ be non-trivial words and let G be a finite simple group of classical type. Then*

$$\|\mathbf{P}_{w_1(G), w_2(G), w_3(G)} - \mathbf{U}_G\|_{L^\infty} \to 0 \text{ as } |G| \to \infty.$$

Proof. Suppose G is of Lie type and its rank r is bounded. By [La], there exist N and $\epsilon > 0$ such that if $|G| \geq N$ then $|w_i(G)| \geq \epsilon |G|$ for $i = 1, 2$. Therefore,

$$\mathbf{P}_{w_1(G), w_2(G)}(e) = O(|G|^{-1}),$$

and by part (iv) of Theorem A,

$$\mathbf{P}_{w_1(G), w_2(G)}(g) = (1 + o(1))|G|^{-1}$$

for $g \neq e$. This implies the theorem for bounded r.

We may therefore assume that r tends to infinity. Theorem 1.12 of [LS1] shows that, if G is symplectic or orthogonal, then $|w_i(G)| \geq cr^{-1}|G|$ $(i = 1, 2, 3)$, where $c > 0$ is an absolute constant. Since $m(G) \geq bq^r$ for fixed $b > 0$ (see [FG]) we have

$$\frac{m(G)|w_1(G)|\,|w_2(G)|\,|w_3(G)|}{|G|^3} \to \infty \text{ as } |G| \to \infty. \tag{8.1}$$

In the case where G is $\mathrm{PSL}_n(q)$ or $\mathrm{PSU}_n(q)$, Propositions 1.7 and 1.8 of [NP] show that $|w_i(G)| \geq q^{-n/4 + o_n(1)}|G|$ $(i = 1, 2, 3)$, which implies (8.1) for $n \gg 0$.

The desired conclusion now follows from Theorem 7.2. □

References

[Ap] T.M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[BNP] L. Babai, N. Nikolov and L. Pyber, Product growth and mixing in finite groups, (Extended abstract.) In: '*Proc. 19th Ann. Symp. Discrete Algorithms (SODA'08), ACM–SIAM 2008*', pp. 248–257.

[BGT] E. Breuillard, B. Green and T. Tao, Approximate subgroups of linear groups, *Geom. Funct. Anal.* **21** (2011), 774–819.

[SGA $4\frac{1}{2}$] P. Deligne, '*Cohomologie Étale. Séminaire de Géométrie Algébrique du Bois-Marie SGA* $4\frac{1}{2}$', Lecture Notes in Mathematics **569**, Springer-Verlag, Berlin, 1977.

[De] P. Deligne, La conjecture de Weil. II, *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252.

[EG] E.W. Ellers and N. Gordeev, On conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671.

[FG] J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364** (2012), 3023–3070.

[Gl] D. Gluck, Character value estimates for nonsemisimple elements, *J. Algebra* **155** (1993), 221–237.

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

[EGA IV_2] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II, *Inst. Hautes Études Sci. Publ. Math.* **24**, 1965.

[EGA IV_3] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III, *Inst. Hautes Études Sci. Publ. Math.* **28**, 1966.

[GLT] R.M. Guralnick, M. Larsen and P.H. Tiep, Character levels and character bounds for finite classical groups, arXiv:1904.08070v1.

[GLBST] R.M. Guralnick, M.W. Liebeck, E.A. O'Brien, A. Shalev and P.H. Tiep, Surjective word maps and Burnside's p^aq^b theorem, *Invent. Math.* **213** (2018), 589–695.

[GM] R.M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (2012), 77–121.

[GT] R.M. Guralnick and P.H. Tiep, Effective results on the Waring problem for finite simple groups, *Amer. J. Math.* **137** (2015), 1401–1430.

[He] H.A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math.* **167** (2008), 601–623.

[Hr] E. Hrushovski, Stable group theory and approximate subgroups, *J. Amer. Math. Soc.* **25** (2012), 189–243.

[La] M. Larsen, Word maps have large image, *Israel J. Math.* **139** (2004), 149–156.

[LS1] M. Larsen and A. Shalev, Word maps and Waring type problems, *J. Amer. Math. Soc.* **22** (2009), 437–466.

[LS2] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, *Invent. Math.* **174** (2008), 645–687.

[LST1] M. Larsen, A. Shalev and P.H. Tiep, The Waring problem for finite simple groups, *Ann. of Math.* **174** (2011), 1885–1950.

[LST2] M. Larsen, A. Shalev and P.H. Tiep, Probabilistic Waring problems for finite simple groups, *Ann. of Math.* **190** (2019), 561–608.

[LST3] M. Larsen, A. Shalev and P.H. Tiep, Products of derangements in simple permutation groups, *Forum of Math. Sigma* **10** (2022), e83, `https://doi.org/10.1017/fms.2022.69`

[LBST] M.W. Liebeck, E.A. O'Brien, A. Shalev and P.H. Tiep, The Ore conjecture, *J. Europ. Math. Soc.* **12** (2010), 939–1008.

[LiSh1] M.W. Liebeck and A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks. *J. Algebra* **276** (2004), no. 2, 552–601.

[LiSh2] M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups, and representation varieties, *Invent. Math.* **159** (2005), 317–367.

[LiSh3] M.W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type, *Proc. London Math. Soc.* **90** (2005), 61–86.

[LSSh] M.W. Liebeck, G. Schul and A. Shalev, Rapid growth in finite simple groups, *Trans. Amer. Math. Soc.* **369** (2017), 8765–8779.

[MSP1] T.W. Müller and J-C. Puchta, Character theory of symmetric groups and subgroup growth of surface groups. *J. London Math. Soc. (2)* **66** (2002), no. 3, 623–640.

[MSP2] T.W. Müller and J-C. Puchta, Character theory of symmetric groups, subgroup growth of Fuchsian groups, and random walks. *Adv. Math.* **213** (2007), no. 2, 919–982.

[NP] N. Nikolov and L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem, *J. Europ. Math. Soc.* **13** (2011), 1063–1077.

[PS] L. Pyber and E. Szabó, Growth in finite simple groups of Lie type, *J. Amer. Math. Soc.* **29** (2016), 95–146.

[Se] D. Segal, '*Words: Notes on Verbal Width in Groups*', London Math. Soc. Lecture Note Series **361**, Cambridge University Press, Cambridge, 2009.

[Sh1] A. Shalev, Mixing and generation in simple groups, *J. Algebra* **319** (2008), 3075–3086.

[Sh2] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, *Ann. of Math.* **170** (2009), 1383–1416.

[St] R.P. Stanley, '*Enumerative Combinatorics*', vol. **1**, Cambridge Studies in Advanced Mathematics, **49**, Cambridge University Press, Cambridge, 2011.

[Ta] T. Tao, What's new, `https://terrytao.wordpress.com/tag/algebraic-regularity-lemma/`.

[Va] Y. Varshavsky, Lefschetz-Verdier trace formula and a generalization of a theorem of Fujiwara, *Geom. Funct. Anal.* **17** (2007), 271–319.

[WW] E.T. Whittaker and G.N. Watson, '*A Course of Modern Analysis. An Introduction to the General Theory of Infinite Processes and of Analytic Functions; with an Account of the Principal Transcendental Functions*', 4th edition, Cambridge University Press, Cambridge, 1927.

Department of Mathematics, Indiana University, Bloomington, IN 47405, U.S.A.
Email address: `mjlarsen@indiana.edu`

Einstein Institute of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel
Email address: `shalev@math.huji.ac.il`

Department of Mathematics, Rutgers University, Piscataway, NJ 08854, U.S.A.
Email address: `tiep@math.rutgers.edu`