DOI 10.4171/8ECM/21

Covering and growth for group subsets and representations

Aner Shalev

Abstract. Deep results on products of subsets of finite groups, and of finite simple groups in particular, were obtained this century. Gowers' theory of quasi-random groups, further developed and applied by Nikolov and Pyber, focuses on covering results, while the theory of approximate subgroups and the product theorem, developed by Helfgott, Hrushovski, Breuillard, Green and Tao, and Pyber and Szabó, focus on growth results.

In recent joint works with Larsen and Tiep, following works with Liebeck and Tiep, we explore analogous problems in representation theory. We replace subsets of a group by its characters, and subset products by products of characters. We also study covering and growth for normal subsets of finite simple groups and derive various applications. In particular, we prove that every element of a sufficiently large finite simple transitive permutation group is a product of two derangements.

The product theorem establishes 3-step growth of the form $|A^3| \geq |A|^{1+\varepsilon}$ for (certain) subsets A of finite simple groups of Lie type of bounded rank. Surprisingly, stronger results hold for characters. We obtain 2-step growth for characters of finite simple groups of Lie type, including those of unbounded rank. For a character χ of G, we set $|\chi| = \sum_i \chi_i(1)^2$, where χ_i are the (distinct) irreducible constituents of χ. For a finite simple group G of Lie type, we show that for every $\delta > 0$ there exists $\varepsilon > 0$ such that if χ is an irreducible character of G satisfying $|\chi| \leq |G|^{1-\delta}$, then $|\chi^2| \geq |\chi|^{1+\varepsilon}$. In addition, we obtain results for reducible characters and establish faster growth of the form $|\chi^2| \geq |\chi|^{2-\varepsilon}$ if $|\chi| \leq |G|^{\delta}$.

Following a recent work of Sellke, we also study covering phenomena in representation theory, proving that if $|\chi_1| \cdots |\chi_m|$ is a sufficiently large power of $|G|$, then every irreducible character of G is a constituent of $\chi_1 \cdots \chi_m$. Finally, we obtain related results for characters of compact semisimple Lie groups.

1. Subset products and covering

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, which is part of the theory of quasi-random groups (see [1, 17, 57]), establishes

2020 Mathematics Subject Classification. Primary 20C33; Secondary 20D06.
Keywords. Finite simple groups, growth, covering, characters, approximate subgroups.

a useful 3-step covering result. Let $m(G)$ denote the minimal degree of a non-trivial irreducible character of a finite group G. The *density* of a subset $A \subseteq G$ is defined as $|A|/|G|$. Let A, B, and C be subsets of G satisfying $|A||B||C| \geq |G|^3/m(G)$. Then, Gowers' trick shows that $ABC = G$. In particular, if the density of A is at least $m(G)^{-1/3}$, then $A^3 = G$.

A family F of finite groups is said to be *quasi-random* if $m(G) \to \infty$ as G ranges over the groups in F. It follows that if F is a quasi-random family of finite groups, $\varepsilon > 0$, $G \in F$, and the density of $A, B, C \subseteq G$ is at least ε, then $ABC = G$ provided that $|G|$ is sufficiently large.

Much less is known about the products of two subsets, which is the main topic of this section. It is easy to see that the above assertion fails to hold for length 2 products AB. Moreover, for every positive integer k, there exist infinitely many finite groups G and subsets $A, B \subset G$ such that $|A|, |B| \geq |G|/(k+1)$ and $|AB| \leq |G| - k$. To see this, fix $k \geq 1$, and let G be any finite group of order divisible by $k+1$. Let $A, S \subset G$ be subsets satisfying $|A| = |G|/(k+1)$ and $|S| = k$. Define $B := G \setminus A^{-1}S$ (where $A^{-1} := \{a^{-1} : a \in A\}$). Note that $|B| = |G| - |A^{-1}S| \geq |G| - |S||A| = |G| - k|G|/(k+1) = |G|/(k+1)$. Clearly, $AB \cap S = \emptyset$ (if $ab = s$ for some $a \in A$, $b \in B$, and $s \in S$, then $b = a^{-1}s$, so $B \cap A^{-1}S \neq \emptyset$, a contradiction). Thus, $AB \subseteq G \setminus S$ and $|AB| \leq |G| - k$, proving the claim.

Can we still obtain 2-step covering results under suitable stronger assumptions?

A trivial observation (which is still useful) is that if subsets $A, B \subseteq G$ have densities α and β, respectively, and $\alpha + \beta > 1$, then $AB = G$. In particular, if $A, B \subseteq G$ have size greater than $|G|/2$, then $AB = G$. This observation will play a role in the complicated proof of the main result of Section 2 (see Theorems 2.4 and 2.8).

Next, let us assume that F is the family of all finite simple groups G. It is well known that F is quasi-random (see [29] for detailed information on $m(G)$). Let $S, T \subseteq G$ be *normal* subsets of G; this means that S, T are closed under conjugation by elements of G, and so they are unions of conjugacy classes of G. What can we say about the product ST and about related distributions?

Products of two (or more) normal subsets of finite simple groups have been extensively studied. This includes the challenging case of products of two conjugacy classes. A major motivation is a longstanding conjecture of Thompson, which asserts that every finite simple group G has a conjugacy class C such that $C^2 = G$. In spite of considerable progress (see Ellers and Gordeev [8] and the references therein) and the proof of the related Ore conjecture (see [42]), Thompson's conjecture is still open for various infinite families of groups of Lie type over fields with $q \leq 8$ elements. A weaker result, that all finite simple groups G of order exceeding 2^{630} have conjugacy classes C_1, C_2 such that $C_1C_2 \supseteq G \setminus \{e\}$, is obtained in [36]; this was improved, using computational group theory and other tools, by Guralnick and Malle in [18], where the same conclusion is established for *all* finite simple groups.

See also [65], where a probabilistic approximation to Thompson's conjecture is obtained. It is shown there that, for finite simple groups G and random (not necessarily independent) elements $x, y \in G$, the sizes of $x^G y^G$ and of $(x^G)^2$ are $(1-o(1))|G|$. Thus, the square of the conjugacy class x^G of a random element $x \in G$ almost covers G as $|G| \to \infty$. Very recently, Larsen and Tiep [39] have proved Thompson's conjecture for additional infinite families of finite simple groups.

For normal subsets S (not equal to $\emptyset$, $\{e\}$) of arbitrary finite simple groups G, the minimal $k > 0$ such that $S^k = G$ is determined by Liebeck and me in [45] up to an absolute multiplicative constant. Indeed, we show there that $\log|G|/\log|S| \le k \le c \log|G|/\log|S|$ and derive various applications. Note that the lower bound on k is trivial and that the upper bound on k is also an upper bound on the diameter of the Cayley graph $\Gamma(G, S)$.

A beautiful improvement of this result in the case $G = \mathrm{PSL}_n(q)$ was obtained by Rodgers and Saxl [59]. They show that if $C_1, \dots, C_k$ are conjugacy classes of G satisfying $|C_1| \cdots |C_k| > |G|^{12}$, then $C_1 \cdots C_k = G$.

Very recently, Maróti and Pyber [54] have obtained an impressive common extension of [45, 59], proving the following covering result.

Theorem 1.1 (Maróti and Pyber, 2021). *There exists an absolute constant c such that if G is any finite simple group, $k \in \mathbb{N}$, and $T_1, \dots, T_k \subseteq G$ are normal subsets of G satisfying $|T_1| \cdots |T_k| \ge |G|^c$, then $T_1 \cdots T_k = G$.*

In [41], Liebeck, Nikolov, and I conjectured that there is an absolute constant c such that if G is any finite simple group and $A \subseteq G$ is any subset of size at least two, then there is $k \le c \log|G|/\log|A|$ and elements $g_1, \dots, g_k \in G$ such that $A^{g_1} \cdots A^{g_k} = G$ (where $A^g = g^{-1}Ag$). This conjecture is still open in general, but Gill, Pyber, Short, and Szabó [15] confirmed it for finite simple groups of Lie type of bounded rank.

The following stronger covering conjecture, which implies Theorem 1.1, was stated by Gill, Pyber, and Szabó in [16] and proved there for finite simple groups of Lie type of bounded rank.

Conjecture 1.2. *There is an absolute constant c such that if G is any finite simple group, $k \in \mathbb{N}$, and $A_1, \dots, A_k \subseteq G$ are subsets of G satisfying $|A_1| \cdots |A_k| \ge |G|^c$, then there exist elements $g_1, \dots, g_k \in G$ such that $A_1^{g_1} \cdots A_k^{g_k} = G$.*

Some covering results have deep applications, also to the theory of expander graphs. It is now known that all finite simple groups can be made expanders uniformly with respect to bounded generating sets. Remarkable pioneering work by Kassabov established this for alternating groups [28] and then for special linear groups of unbounded rank. A key step in proving expansion for the remaining finite simple groups was to present the simple groups of Lie type of bounded rank (except the

Suzuki groups, shown to be expanders in [6]) as a bounded product of subgroups of the types $\mathrm{SL}_2(q)$ and $\mathrm{PSL}_2(q)$. This is done effectively in [40] with explicit bounds and ineffectively (using a model-theoretic approach based on work by Hrushovski and Pillay) by Lubotzky in [51].

In the work [43], Liebeck, Schul, and I show that the product of two small normal subsets of finite simple groups has size close to the product of their sizes (see Section 3 for more details).

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, [21,22,32,33,36,37,42,55,60,66], the references therein, and Segal's monograph [61] on word width and the affirmative solution by Nikolov and Segal of Serre's problem, whether every finite index subgroup of a (topologically) finitely generated profinite group is open.

By a *word*, we mean an element $w = w(x_1, \ldots, x_d)$ of the free group F_d freely generated by $x_1, \ldots, x_d$. A word w and a group G give rise to a word map $w : G^d \to G$ induced by substituting group elements $g_1, \ldots, g_d$ in $x_1, \ldots, x_d$, respectively; its image, denoted by $w(G)$, is a normal subset of G.

The classical Waring problem in number theory, solved by Hilbert and subsequently by Hardy and Littlewood using the circle method, deals with sums of nth powers of natural numbers (see [56]). In [55, 60], the analogous problem for finite simple groups G is studied; it is shown there that for every integer $n > 1$ there is a number $f(n)$ such that if G is a finite simple group not satisfying the identity $x^n = 1$, then every element of G is a product of $f(n)$ nth powers. In other words, if $w = w_n := x^n$, then $w(G)^{f(n)} = G$ for such groups G.

This result is improved in [66] for sufficiently large finite simple groups in several ways: the inexplicit function f (depending on w) is replaced by the fixed small number 3; the equality $w(G)^3 = G$ holds for all non-trivial words w provided that $|G| \geq N_w$; moreover, it is shown in [66] that, for all non-trivial words $w_1, w_2, w_3 \in F_d$ and all sufficiently large finite simple groups G, we have $w_1(G)w_2(G)w_3(G) = G$. This is improved by Larsen, Tiep, and me in [36] for length 2 products; i.e., for non-trivial words $w_1, w_2 \in F_d$ and all sufficiently large finite simple groups G, we have

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

The tools we apply in proving this and other results on word maps include representation theory and the Deligne–Lustig theory of characters, as well as algebraic geometry and some model theory; see Hrushovski's work on the elementary theory of Frobenius automorphism [27] and Varshavsky's strengthening of Fujiwara's proof of Deligne's conjecture [68].

There are various asymptotic results showing that word maps associated with words $w \neq 1$ on finite simple groups G have large image; see [31–33, 57]. In partic-

ular, it is shown by Larsen in [31] that $|w(G)| \geq |G|^{1-\varepsilon}$ for any $\varepsilon > 0$ provided that $|G| \gg 0$, and that for G of Lie type and bounded rank there exists $\varepsilon > 0$ (depending only on the rank of G) such that for all words $w \neq 1$ we have $|w(G)| \geq \varepsilon|G|$. In the recent preprint [35], we attempt to understand to what extent (1.1) can be extended to products of arbitrary large normal subsets of finite simple groups.

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

Question 1.3. Does every element in $G \smallsetminus \{e\}$ lie in ST if $|G|$ is sufficiently large?

Question 1.4. Does the ratio between the number of representations of each $g \in G \smallsetminus \{e\}$ and $\frac{|S||T|}{|G|}$ tend uniformly to 1 as $|G| \to \infty$?

Question 1.5. What happens in the special case $S = T$?

An affirmative answer to Question 1.4 implies an affirmative answer to Question 1.3 (and the same holds in the special case $S = T$).

We exclude the identity element e of G in Questions 1.3 and 1.4 because every conjugacy class C in a non-trivial finite group G satisfies $|C| = \frac{|G|}{n}$ for some $n \geq 2$, so each such group has a normal subset S with $\frac{|G|}{3} \leq |S| \leq \frac{2|G|}{3}$. Setting $T = G \smallsetminus S^{-1}$, 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 $ST \not\supseteq G \smallsetminus \{e\}$; indeed, fix $g \in G \smallsetminus \{e\}$, choose S of the specified size, and let $T = G \smallsetminus S^{-1}g$.

Our answers to these questions are listed below.

Theorem 1.6. (1) *The answers to Questions 1.3 and 1.4 are negative if G ranges over all finite simple groups, or even just over the alternating groups, or just over all projective special linear groups.*

(2) *In the $S = T$ case, the answer to Question 1.4 is still negative for alternating groups.*

(3) *In the $S = T$ case, the answer to Question 1.3 is positive for alternating groups.*

(4) *If G is a group of Lie type of bounded rank, then the answers to Questions 1.3 and 1.4 are both positive.*

In view of this, we may say that the simple groups of Lie type of bounded rank are the most well behaved in this context, and that the alternating groups are mildly well behaved.

Let us now outline the proof of Theorem 1.6, starting with the case of alternating groups A_n. Part (3) in this case follows from the more detailed result below.

Proposition 1.7. *For every $s, t \geq 0$ with $s + t \leq 1$, there are normal subsets $S_n, T_n \subset A_n$ such that $|S_n|/|A_n| \to s$, $|T_n|/|A_n| \to t$, and $S_n T_n$ contains no 3-cycle.*

It follows that, for normal subsets $S, T \subset A_n$, even the inequalities $|S|, |T| \geq (1/2 - o(1))|A_n|$ do not imply $ST \supseteq A_n \setminus \{e\}$.

As for part (3) of Theorem 1.6, namely, the positive result for A_n in the case $S = T$, the following more detailed proposition shows that we obtain a covering result even when $\varepsilon \to 0$ rather fast.

Proposition 1.8. *For every $0 < \alpha < 1/4$, there exists $N > 0$ such that if $n \geq N$ and $T \subseteq A_n$ is a normal subset satisfying $|T| \geq \exp(-n^\alpha) \cdot |A_n|$, then $T^2 = A_n$.*

The main tool in the proof of Proposition 1.8 are strong character bounds for symmetric groups obtained in [32]. Roughly speaking, we show that for each $\sigma \in S_n$ there is a well-defined $E(\sigma) \in [0, 1]$ such that

$$\big|\chi(\sigma)\big| \leq \chi(1)^{E(\sigma)+o(1)} \quad \text{for all } \chi \in \mathrm{Irr}(S_n).$$

Applying these character bounds and other tools, we deduce that $E(\sigma) < 1/4$ implies $(\sigma^{S_n})^2 = A_n$ for all $n \gg 0$. It is also shown in [32] that, for every subset $T \subseteq A_n$ satisfying $|T| \geq \exp(-n^\alpha) \cdot |A_n|$ with $\alpha < 1/4$, a random $\sigma \in T$ satisfies $E(\sigma) < 1/4$ almost surely. We therefore deduce that there is $\sigma \in T$ such that $(\sigma^{S_n})^2 = A_n$ if $n \gg 0$. Finally, replacing σ^{S_n} with σ^{A_n} and using Erdős–Turán's statistical group theory (see, for instance, [9]), we show that $T^2 = A_n$ for $n \gg 0$.

We now turn to projective special linear groups $\mathrm{PSL}_n(q)$. We show the following.

Proposition 1.9. *Let q be a fixed prime power. Then, there exists $\varepsilon > 0$ such that, for every $n \geq 2$ which is relatively prime to $q - 1$, there are normal subsets $S_n, T_n \subset \mathrm{SL}_n(q) \cong \mathrm{PSL}_n(q)$ of density at least ε such that $S_n T_n$ does not contain any transvection.*

This result completes the proof of part (1) of Theorem 1.6.

Our proof of part (4) of Theorem 1.6, dealing with Lie-type groups of bounded rank, depends on a new result in algebraic geometry, which may be of independent interest; it may be regarded as a refinement of the classical Lang–Weil estimate [30] (see also Varshavsky [68]), which concerns the number of points in a finite product set inside a product variety which lies on a subvariety of the product variety. Another major ingredient of the proof is character theory. To explain the connection, we need some notation. For normal subsets $R_1, \ldots, R_k$ of a finite group G and $g \in G$, let $P_{R_1,\ldots,R_k}(g)$ denote the probability that $x_1 \cdots x_k = g$, where $x_i \in R_i$ are randomly chosen. Using this notation, we formulate and establish the following result, which is equivalent to part (4) of Theorem 1.6.

Theorem 1.10. *Let $G = X_r(q)$, a finite simple group of Lie type of rank r over F_q. Suppose that r is bounded and $q \to \infty$. Fix $\varepsilon > 0$ and let $S, T \subseteq G$ be normal subsets of size $\geq \varepsilon|G|$. Then, for every $g \in G \setminus \{e\}$ we have*

$$P_{S,T}(g) = \big(1 + o(1)\big)|G|^{-1}.$$

The relevance of character theory and character bounds to the proof of Theorem 1.10 stems from a classical result of Frobenius: let $C_1, \ldots, C_k \subset G$ be conjugacy classes, and $g \in G$. Then,

$$P_{C_1,\ldots,C_k}(g) = |G|^{-1} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C_1)\cdots\chi(C_k)\overline{\chi(g)}}{\chi(1)^{k-1}}.$$

Frobenius' formula above is also useful for classical groups of unbounded rank. In this case, part (1) of Theorem 1.6 and the more detailed Proposition 1.8 provide counterexamples to 2-step covering by large normal subsets. It turns out that 3-step covering is achieved. More specifically, Question 1.3 for products of three normal subsets has a positive answer with a tiny $\varepsilon = |G|^{-\delta}$, which tends to zero as $|G| \to \infty$.

Theorem 1.11. *There exists a fixed $\delta > 0$ such that if G is a finite simple classical group and $R, S, T \subseteq G$ are normal subsets of size $\geq |G|^{1-\delta}$, then $RST = G$.*

Note that this result does not follow from Gowers' trick. Indeed, for G of rank $r \to \infty$, $|G|^{-\delta} \sim q^{-ar^2}$ is much smaller than $m(G)^{-1/3} \sim q^{-br}$.

The proof of Theorem 1.11 relies heavily on recent developments in representation theory and, more specifically, on the theory of *exponential character bounds* for finite simple groups G; these are bounds of the form

$$\big|\chi(g)\big| \leq \chi(1)^{\alpha(g)},$$

for various $g \in G$, where $\alpha(g) \in [0, 1]$ is an explicit function of g.

For symmetric and alternating groups, such bounds were first obtained by Fomin and Lulov [10] in 1997 for the so-called homogeneous permutations. Bounds for almost homogeneous permutations were subsequently obtained in [46] (see also [48]) with various applications to Fuchsian groups, Higman's conjecture, subgroup growth, and representation varieties. In [32], Larsen and I obtain essentially best-possible exponential character bounds for most permutations in S_n, with applications to word maps and other topics.

Exponential character bounds for finite simple groups of Lie type were recently obtained by Bezrukavnikov, Liebeck, Tiep, and me in [2], by Guralnick, Larsen, and Tiep in [19, 20], and by Taylor and Tiep in [67].

The proof of Theorem 1.11 relies mainly on the level theory of characters developed by Guralnick, Larsen, and Tiep in [19, 20], combined with earlier results on the Witten zeta function

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

and its abscissa of convergence obtained by Liebeck and me in [47].

More specifically, we apply a theorem from [20] according to which there exists an absolute constant $\gamma > 0$ such that if G is a finite simple classical group and $g \in G$ satisfies $|C_G(g)| \leq |G|^\gamma$, then $|\chi(g)| \leq \chi(1)^{1/4}$ for all $\chi \in \mathrm{Irr}(G)$.

We then apply Frobenius' formula and [47, Theorem 1.2], stating that, for any fixed $s > 0$ and r sufficiently large (in terms of s), $\zeta^G(s)$ converges and tends to 1 as $r \to \infty$. In fact, the case $s = 1/4$ suffices.

We now turn to applications of Theorem 1.6. We start with a direct (yet highly non-trivial) application to word maps. A major application, the proof of which is considerably harder, will be discussed in the next section (see Theorem 2.8).

For a non-trivial word $w \in F_d$ and a finite group G, consider the word map $w : G^d \to G$, and define $P_{w,G}(g) := |w^{-1}(g)|/|G|^d$. Thus, $P_{w,G}(g)$ is the probability that $w(g_1, \ldots, g_d) = g$ as $g_1, \ldots, g_d \in G$ are chosen uniformly and independently.

In [37, Theorem 4], we show that for every $\ell \geq 1$ there exists $N = N(\ell) := 2 \cdot 10^{18} \cdot \ell^4$ such that if $1 \neq w_1, \ldots, w_N \in F_d$ are pairwise disjoint words of length $\leq \ell$, G is a finite simple group, and U_G is the uniform distribution on G, then

$$\| P_{w_1 \cdots w_N, G} - U_G \|_\infty \to 0 \quad \text{as } |G| \to \infty;$$

namely, $P_{w_1 \cdots w_N, G}$ is almost uniform with respect to the L^∞ norm.

Surprisingly, changing the probabilistic model and using Theorem 1.10, we obtain an almost uniform distribution in L^∞ much more rapidly.

Corollary 1.12. *Let $1 \neq w_1, w_2 \in F_d$ and let G be a finite simple group of Lie type of bounded rank. Then,*

$$\| P_{w_1(G), w_2(G)} - U_G \|_\infty \to 0 \quad \textit{as } |G| \to \infty.$$

A version for classical groups of unbounded rank was previously implicitly obtained by Nikolov and Pyber in [57] using Gowers' theory of quasi-random groups; it shows that

$$\| P_{w_1(G), w_2(G), w_3(G)} - U_G \|_\infty \to 0 \quad \text{as } |G| \to \infty.$$

Note that Theorem 1.11 extends this result, since $w_i(G)$ are normal subsets of size at least $|G|^{1-\delta}$ by [31].

2. Permutation groups and derangements

A major application of our results from Section 1 on products of normal subsets concerns permutation groups and fixed-point-free permutations, also called *derangements*.

The study of derangements goes back three centuries.

In 1708, Monmort proved that the proportion of derangements in the symmetric group S_n (in its natural action) tends to $1/e$ as $n \to \infty$. Passing to general permutation groups $G \leq S_n$, it is easy to see that if G is intransitive it need not contain derangements (e.g., all permutations in G may have a common fixed point).

In the 1870s, Jordan showed that if $G \leq S_n$ is transitive and $2 \leq n < \infty$, then there exists a derangement $g \in G$ (this result fails to hold for infinite transitive permutation groups).

What can be said about the proportion of derangements in finite transitive permutation groups?

In 1990, Cameron and Cohen [7] proved that the proportion of derangements in transitive permutation groups of degree n is at least $1/n$ and that this lower bound is sharp (as shown by the example of Frobenius groups). Subsequently, it was conjectured that a much better lower bound holds for finite *simple* transitive permutation groups.

Conjecture 2.1 (Boston–Shalev, 1990s). *The proportion of derangements in any finite simple transitive permutation group is at least ε for some fixed $\varepsilon > 0$.*

Let $G \leq S_n$ be a transitive permutation group. Let $D(G)$ denote the set of derangements in G. Clearly, $D(G) = D(G)^{-1}$ and $D(G)$ is a normal subset of G. Let H be a point stabilizer in G. The set of derangements in G in this case is also denoted by $D(G, H)$. Clearly,

$$D(G, H) = G \setminus \bigcup_{g \in G} H^g.$$

Conjecture 2.1 states that if G is simple, then

$$\big|D(G)\big| \geq \varepsilon |G|,$$

for some absolute positive constant ε.

Impressive work on Conjecture 2.1 was carried out in 2002–2018 by Fulman and Guralnick (see, e.g., [11–13]), culminating in the following result.

Theorem 2.2 (Fulman–Guralnick, 2018). *The Boston–Shalev conjecture holds. Moreover, if G is sufficiently large we may take $\varepsilon = 0.016$.*

It would be nice to find an explicit number N such that if the finite simple transitive permutation group G has order at least N, then $|D(G)| \geq 0.016|G|$ or to find an explicit (possibly smaller) $\varepsilon > 0$ such that $|D(G)| \geq \varepsilon |G|$ without exceptions.

Since finite simple groups are quasi-random, Theorem 2.2, combined with Gowers' trick, yields the following.

Corollary 2.3. *For all sufficiently large finite simple transitive permutation groups G, every permutation in G is a product of three derangements, namely, $D(G)^3 = G$.*

Can we replace three by two? Note that the proof of Corollary 2.3 does not use the fact that $D(G)$ is a normal subset of G. Using the normality of $D(G)$, Theorem 1.6 becomes highly relevant. Applying parts (3) and (4) of it, noting that $e \in D(G)^2$, we immediately obtain the following.

Theorem 2.4. *Let G be a finite simple transitive permutation group which is alternating or of Lie type of bounded rank. If $|G| \gg 0$, then $D(G)^2 = G$; namely, every element of G is a product of two derangements.*

Indeed, we proved for the groups above that $T^2 = G$ for every normal subset $T \subseteq G$ of size $\geq \varepsilon|G|$, so take $T := D(G)$.

In order to extend Theorem 2.4 to all types of finite simple groups, it remains to deal with classical groups G of unbounded rank (since the sporadic groups have bounded order). We may assume that G is primitive; i.e., a point stabilizer $H < G$ is a maximal subgroup. Indeed, if H is not maximal, it is contained in a maximal subgroup M of G, and

$$D(G,H) = G \setminus \bigcup_{g\in G} H^g \supseteq G \setminus \bigcup_{g\in G} M^g = D(G,M),$$

so $D(G,M)^2 = G$ implies that $D(G,H)^2 = G$.

We need some additional tools in order to deal with the remaining case of classical groups of unbounded rank.

In 1993, Łuczak and Pyber [52] proved a conjecture of Cameron that as $n \to \infty$, almost all permutations in S_n do not lie in a proper transitive subgroup (not containing A_n). In the same paper, they pose a similar problem for $\mathrm{GL}_n(p)$, where p is a fixed prime and $n \to \infty$. In 1998, this problem was solved in [64].

Theorem 2.5. *Let q be a fixed prime power. Then, as $n \to \infty$, almost all matrices in $\mathrm{GL}_n(q)$ do not lie in a proper irreducible subgroup (not containing $\mathrm{SL}_n(q)$).*

In 2018, Fulman and Guralnick [13] proved a stronger result for all classical groups in dimension $n \to \infty$, where the size of the underlying field need not be fixed. In the case $G = \mathrm{Sp}_n(2^k)$, they exclude (apart from irreducible subgroups) the subgroups $O_n^{\pm}(2^k)$. We apply this to obtain the following.

Corollary 2.6. *Let G be a finite simple classical group in dimension $n \gg 0$. Let $H < G$ be a maximal subgroup. Suppose that H is irreducible and not $O_n^{\pm}(2^k)$ when $G = \mathrm{Sp}_n(2^k)$. Then, $D(G,H)^2 = G$.*

To prove this, let $X(G)$ denote the union of the above maximal subgroups $H < G$. Then, $|X(G)|/|G| \to 0$ as $n \to \infty$. Therefore, $|X(G)| < |G|/2$ for $n \gg 0$. Fixing one such subgroup H (noting that $X(G)$ is closed under conjugation), we see that $\bigcup_{g \in G} H^g \subseteq X(G)$ implies that $|D(G, H)| \geq |G| - |X(G)| > |G|/2$. Applying an observation from Section 1, it follows that $D(G, H)^2 = G$.

Hence we may assume that H is reducible (namely, a parabolic subgroup) or $G = \mathrm{Sp}_n(2^k)$ and $H = O_n^{\pm}(2^k)$.

Our next result settles the problem in additional cases.

Proposition 2.7. *There are absolute constants c_1, c_2 such that the following holds. Let $G \in \mathrm{Cl}_n(q)$ be a finite simple classical primitive permutation group with point stabilizer H. If q is even, assume $(G, H) \neq (\mathrm{Sp}_n(\mathbb{F}_q), O_n^{\pm}(\mathbb{F}_q))$. Suppose that $n \geq c_1$ and the action is not a subspace action on subspaces of dimension $k \leq c_2$. Then, $D(G)^2 = G$.*

To show this, we may assume that H is reducible; namely, G acts in subspace action, say on subspaces (non-degenerate or totally singular for $G \neq \mathrm{PSL}_n(q)$) of dimension k, with $1 \leq k \leq n/2$. Theorems 6.4, 9.4, 9.10, 9.17, and 9.30 of [12] show that, as $k \to \infty$, the proportion of derangements in G is $1 - O(k^{-0.005})$, which tends to 1. The result follows as before.

We are left with very concrete cases, of subspace action on subspaces of bounded dimension and of $\mathrm{Sp}_n(\mathbb{F}_q)$ for q even acting on cosets of $GO_n^{\pm}(\mathbb{F}_q)$. These cases are handled using character methods and the theory of symbols. Roughly speaking, we apply the method of [53] and its extension in [36] and use weakly orthogonal tori T_1, T_2 and regular semisimple elements $t_i \in T_i$ such that only few (unipotent) characters $\chi \in \mathrm{Irr}(G)$ satisfy $\chi(t_1)\chi(t_2) \neq 0$. This helps show that $t_1^G t_2^G \supseteq G \setminus \{e\}$. This rather long case-by-case study completes the proof of the main result of this section (see [34]).

Theorem 2.8. *Let G be a finite simple transitive permutation group. If G is sufficiently large, then every element of G is a product of two derangements.*

We conjecture that the assumption that G is sufficiently large is not needed; namely:

Conjecture 2.9. *Let G be a finite simple transitive permutation group. Then, every element of G is a product of two derangements.*

Computations carried out by Eamonn O'Brien provide strong evidence in favor of this conjecture, but proving it seems to require new methods.

3. Subset growth

The celebrated product theorem of [5,58], which is part of the deep theory of approximate subgroups [4] following the pioneering work of Helfgott on $\mathrm{SL}_2(p)$ [24] (see also [25]) and Hrushovski's model-theoretic approach [26], shows that for finite simple groups G of Lie type and bounded rank there exists $\varepsilon > 0$ such that, for every subset $A \subseteq G$ which generates G, either $|A^3| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.

Can we extend this result to general finite simple groups? The answer is known to be negative, as shown by counterexamples for classical groups of unbounded rank and alternating groups of unbounded degree.

However, the situation changes dramatically if we replace arbitrary subsets by normal subsets. A first result in this direction was obtained in [66] before the product theorem was fully established. Indeed, Theorem 2.7 there states the following.

Theorem 3.1. *For any $\delta > 0$, there exists $\varepsilon > 0$ depending only on δ such that if G is a finite simple group and C is a conjugacy class of G of size at most $|G|^{1-\delta}$, then $|C^3| \geq |C|^{1+\varepsilon}$.*

Note that an upper bound on the size of C of the type above is necessary for the conclusion to hold. The proof of Theorem 3.1 uses tools from character theory, properties of the Witten zeta function obtained by Liebeck and me in [47], as well as [24, Lemma 2.2] of Helfgott and its proof.

Can we extend this 3-step growth result to 2-step growth results, replacing C^3 by C^2? It turns out that the answer is positive if G is a finite simple group of Lie type of bounded rank. Indeed, we have the following (see [66, Proposition 10.4]).

Theorem 3.2. *If C is a conjugacy class of a finite simple group G of Lie type, then $|C^2| \geq |C|^{1+\varepsilon}$, where $\varepsilon > 0$ depends only on the rank of G.*

The above result was extended by Gill, Pyber, Short, and Szabó in [15, Theorem 1.5], where conjugacy classes C are replaced by arbitrary normal subsets T, and G is an arbitrary finite simple group.

Theorem 3.3. *There are absolute constants $b \in \mathbb{N}$ and $\varepsilon > 0$ such that, for any normal subset T of a finite simple group G, either $T^b = G$ or $|T^2| \geq |T|^{1+\varepsilon}$.*

Subsequently, Liebeck, Schul, and I obtained stronger expansion results for normal subsets in [43].

Theorem 3.4. *Given any $\varepsilon > 0$, there exists $b \in \mathbb{N}$ such that, for any normal subset T of any finite simple group G, either $T^b = G$ or $|T^2| \geq |T|^{2-\varepsilon}$.*

Theorem 3.4 is deduced from the following result.

Theorem 3.5. *Given any $\varepsilon > 0$, there exists $\delta = \delta(\varepsilon) > 0$ such that if T is a normal subset of a finite simple group G satisfying $|T| \leq |G|^{\delta}$, then $|T^2| \geq |T|^{2-\varepsilon}$.*

Obviously $|T^2| \leq |T|^2$, so Theorem 3.5 shows that small normal subsets of finite simple groups expand almost as quickly as possible.

Note that some upper bound on the size of T is needed in order for the conclusion to hold.

To deduce Theorem 3.4, fix $\varepsilon > 0$ and choose $\delta = \delta(\varepsilon) > 0$ as above. Recall that, by the main result of [45], there exists an absolute constant c and a positive integer $k \leq c \log |G| / \log |T|$ such that $T^k = G$ for every (non-trivial) normal subset T of a finite simple group G. Hence, if $|T| \geq |G|^{\delta}$, then $T^k = G$ for some $k \leq c\delta$. Thus, Theorem 3.4 holds with $b = \lfloor c\delta \rfloor$.

Theorem 3.5 holds vacuously for simple groups of bounded order or of bounded rank, since for these we may choose δ so small that $|T| > |G|^{\delta}$ for all non-trivial normal subsets T; in particular, it holds for the sporadic groups and the exceptional groups of Lie type. It therefore remains to prove the theorem for classical groups of large rank and alternating groups of large degree.

We deduce Theorem 3.5 from the following more general result.

Theorem 3.6. *Given any $\varepsilon > 0$, there exists $\delta > 0$ such that if T_1, T_2 are normal subsets of a finite simple group G satisfying $|T_1|, |T_2| \leq |G|^{\delta}$, then $|T_1 T_2| \geq (|T_1|\,|T_2|)^{1-\varepsilon}$.*

The proof of Theorem 3.6 in [43] is based on results from [44, 45, 47], together with some new results of independent interest on the size of the conjugacy classes in classical groups and in symmetric groups in terms of the *support* of their elements.

The support of a permutation $x \in S_n$ is the number of points moved by x. Let $C \subset S_n$ be a non-trivial conjugacy class and let s be the support of its elements (obviously all the elements of C have the same support), which may be regarded as the support of C. Then, $2 \leq s \leq n$. For our purpose, it is essential to obtain good estimates on the size of C in terms of its support s. We show that

$$|C| \leq \frac{n!}{(n-s)!s}$$

for all s and that

$$|C| \geq \frac{n!}{(n-s)!2^{s/2}\lfloor s/2 \rfloor !}$$

for all $s \neq 3$.

Note that the above lower bound on $|C|$ is best possible, since it is attained in the case where the permutations in C decompose into $s/2$ 2-cycles (s even). The upper bound on $|C|$ is also sharp; it is attained when C consists of s-cycles. Finally, if $s = 3$,

then the lower bound does not hold, but it does hold for all s if we replace $\lfloor s/2 \rfloor$ by $\lceil s/2 \rceil$.

Next, let G be one of the classical groups $L_n^{\pm}(q)$, $PSp_n(q)$ or $PO_n^{\pm}(q)$, and let $V = V_n(q^u)$ be the natural module for G with n large, where $u = 2$ if G is unitary and $u = 1$ otherwise. Let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}_q$, and let $\overline{V} = V \otimes \overline{\mathbb{F}}$. Let $x \in G$, and let $\hat{x}$ be a preimage of x in $\mathrm{GL}(V)$. Define

$$\nu(x) = \nu_{V,\overline{\mathbb{F}}}(x) = \min\left\{ \dim[\overline{V}, \lambda\hat{x}] : \lambda \in \overline{\mathbb{F}}^* \right\},$$

where $[\overline{V}, \lambda\hat{x}]$ denotes the subspace $\overline{V}(\lambda\hat{x} - Id_{\overline{V}})$. We shall refer to $\nu(x)$ as the *support* of x.

Define

$$a(G) = \begin{cases} 1, & \text{if } G = L_n^{\pm}(q), \\ \frac{1}{2}, & \text{otherwise.} \end{cases}$$

The inequalities we state below, which are an extension of [44, Lemma 3.4], show that $\nu(x)$ is closely related to the size of the conjugacy class $C = x^G$. Suppose that $\nu(x) = s < \frac{n}{2}$, and let $a = a(G)$. We prove that

$$c_1 q^{2as(n-s-1)} \leq |x^G| \leq c_2 q^{as(2n-s+1)}$$

for some absolute constants $c_1, c_2 > 0$.

In fact, under the assumptions of Theorem 3.6, we establish a stronger conclusion: there exists a single conjugacy class $C \subseteq T_1 T_2$ such that $|C| \geq (|T_1|\,|T_2|)^{1-\varepsilon}$. The notion of the support of elements of G plays a key role in our argument.

A similar result for k subsets follows inductively from Theorem 3.6.

Corollary 3.7. *Given $\varepsilon > 0$ and $k \in \mathbb{N}$, there exists $\delta > 0$ such that if $T_1, \ldots, T_k \subseteq G$ are normal subsets of a finite simple group G with $|T_i| \leq |G|^{\delta}$ for $i = 1, \ldots, k$, then $|T_1 \cdots T_k| \geq (|T_1| \cdots |T_k|)^{1-\varepsilon}$. In particular, $|T^k| \geq |T|^{k-\varepsilon}$ for every normal subset T of G satisfying $|T| \leq |G|^{\delta}$, where δ depends on ε and k.*

Finally, we prove a result analogous to Theorem 3.6 for algebraic groups over algebraically closed fields.

Theorem 3.8. *For any $\varepsilon > 0$, there exists $\delta > 0$ such that if C_1, C_2 are conjugacy classes in a simple algebraic group G satisfying $\dim C_i \leq \delta \dim G$ for $i = 1, 2$, then the product $C_1 C_2$ contains a conjugacy class of dimension at least $(1 - \varepsilon)(\dim C_1 + \dim C_2)$.*

4. Character growth and covering

The main goal of this section, based mainly on the recent preprint [38] with Larsen and Tiep, is to study covering and growth phenomena in representation theory, with

emphasis on (complex) representations of the finite simple groups G of Lie type. Here, products of subsets of G are replaced by tensor products of representations (or equivalently, products of characters). Our results on tensor product growth are somewhat stronger than the product theorem in two senses: instead of 3-step growth, we establish 2-step growth, as well as uniform growth when the rank of G tends to infinity.

In some cases, the results of this section are character-theoretic analogues of results from the previous section, dealing with product growth of conjugacy classes (corresponding to irreducible characters) and normal subsets (corresponding to arbitrary characters). An irreducible constituent of an arbitrary character may be regarded as an analogue of a conjugacy class contained in a normal subset.

Covering results by products of characters of finite simple groups were obtained by Liebeck, Tiep, and me in the recent papers [49,50]. These papers study the McKay graphs of finite simple groups, with emphasis on their diameter.

We need some background and notation. For a finite group G and a complex character α of G, the *McKay graph* $MC(G,\alpha)$ is defined to be the directed graph with vertex set $\mathrm{Irr}(G)$, and with an edge from χ_1 to χ_2 if and only if χ_2 is a constituent of $\alpha\chi_1$.

A classical result of Burnside and Brauer [3] shows that $MC(G,\alpha)$ is connected if and only if α is faithful; furthermore, in this case an upper bound for the diameter $\mathsf{diam}\, MC(G,\alpha)$ is given by $N-1$, where N is the number of distinct values of α. This means that $\sum_{j=0}^{N-1}\alpha^j$ contains every irreducible character of G.

An obvious lower bound for $\mathsf{diam}\, MC(G,\alpha)$ (when $\alpha(1)>1$) is given by $\frac{\log \mathsf{b}(G)}{\log \alpha(1)}$, where $\mathsf{b}(G)$ is the largest degree of an irreducible character of G. This lower bound (which can be slightly improved) is in general far from tight. However, finite simple groups often behave better than arbitrary groups, and for them we stated the following conjecture in [50].

Conjecture 4.1. *There is an absolute constant c such that, for any finite non-abelian simple group G and any non-trivial irreducible character α of G, we have*

$$\mathsf{diam}\, MC(G,\alpha) \le c\frac{\log|G|}{\log\alpha(1)}.$$

This conjecture may be regarded as a representation-theoretic analogue of [45, Theorem 1.1] on the diameter of the Cayley graph $\Gamma(G,S)$ of a finite simple group G with respect to a (non-trivial) normal subset S.

Various results supporting this conjecture were obtained in [49, 50], where it is proved for several families of groups of Lie type and for alternating groups following Sellke's paper [62] proving it for symmetric groups. In [49], we also obtain some results showing that, under suitable assumptions, products $\chi_1\cdots\chi_m$ of possibly different characters cover $\mathrm{Irr}(G)$ (namely, every irreducible character is a constituent of

the above product). In [39], Larsen and Tiep have completed the proof of Conjecture 4.1.

A more recent covering result of Sellke [63] is a character-theoretic analogue of Gowers' trick and the theory of quasi-random groups discussed in Section 1, which focuses on 3-step covering. We need some notation.

Let G be a finite group. We say that an arbitrary complex character ψ of G *covers* $\mathrm{Irr}(G)$ if every irreducible character of G is a constituent of ψ. If $X = \{\chi_1, \dots, \chi_k\}$ is a set of (pairwise distinct) irreducible characters of G, we define

$$|X| = \sum_{i=1}^{k} \chi_i(1)^2.$$

This is the Plancherel measure, normalized so that $|\mathrm{Irr}(G)| = |G|$. If χ is any character of G, we define $|\chi| = |X_\chi|$, where X_χ denotes the set of distinct irreducible constituents of χ. We show in [38] that the function sending χ to $|\chi|$ has convenient properties: it is sub-multiplicative and satisfies the triangle inequality in the sense that

$$|\chi_1\chi_2| \le |\chi_1| \cdot |\chi_2| \quad \text{and} \quad |\chi_1 + \chi_2| \le |\chi_1| + |\chi_2|. \tag{4.1}$$

We can now state the covering result mentioned above, which is the main part of [63, Theorem 1.3]. For a finite group G, let $c(G)$ denote the minimal size of a conjugacy class $\neq \{e\}$ in G. Let us say that a collection F of finite groups is *conjugacy-random* if $c(G) \to \infty$ as G ranges over the groups in F.

Theorem 4.2 (Sellke, 2021). *Let F be a conjugacy-random set of finite groups. Fix $\varepsilon > 0$. Let $G \in F$ and let χ_1, χ_2, χ_3 be (not necessarily irreducible) characters of G with the property that $|\chi_1|, |\chi_2|, |\chi_3| \ge \varepsilon|G|$. Then, $\chi_1\chi_2\chi_3$ covers $\mathrm{Irr}(G)$ provided $|G|$ is sufficiently large.*

While most of our results below establish rapid tensor product growth in various situations, some of them, i.e., Theorems 4.8 and 4.9, are covering results, while Theorem 4.7 establishes a growth-or-covering phenomenon.

Recall that G is *quasisimple* if $G = [G, G]$ and $G/\mathbf{Z}(G)$ is simple.

Our first growth results are as follows.

Theorem 4.3. *For all $\delta > 0$, there exists $\varepsilon > 0$ such that if G is a finite quasisimple group of Lie type and χ is an irreducible character of G with $|\chi| \le |G|^{1-\delta}$, then $|\chi^2| \ge |\chi|^{1+\varepsilon}$ and $|\chi\overline{\chi}| \ge |\chi|^{1+\varepsilon}$.*

We also have a version of this result for general characters in groups of high rank.

Theorem 4.4. *For all $\delta > 0$, there exist $\varepsilon > 0$ and $R > 0$ such that if G is a finite quasisimple group of Lie type and rank $\ge R$ and χ is any (not necessarily irreducible) character of G with $|\chi| \le |G|^{1-\delta}$, then $|\chi^2| \ge |\chi|^{1+\varepsilon}$ and $|\chi\overline{\chi}| \ge |\chi|^{1+\varepsilon}$.*

An essential tool in the proofs of most of the results in this section is a new uniform character bound obtained by Larsen and Tiep [39, Theorem A]. The proofs of Theorems 4.3 and 4.4 present ε as an explicit function of δ, e.g., $\varepsilon = \frac{c\delta}{4+2c(1-\delta)}$ in Theorem 4.3, where $c > 0$ is the absolute constant in [39, Theorem A]. Moreover, if G is sufficiently large but of bounded rank r, and χ is irreducible, then $\varepsilon = \frac{\delta}{2-2\delta}$ will do; for example, any irreducible character χ of G with $|\chi| \leq |G|^{1/2}$ satisfies $|\chi^2| \geq |\chi|^{3/2}$. Can we establish faster growth when $|\chi|$ is smaller?

Our next result provides an affirmative answer and may be regarded as a character-theoretic analogue of the main result of Section 3, namely, Theorem 3.6 (which obviously implies Theorem 3.4).

Theorem 4.5. *For any $\varepsilon > 0$, there exists an explicit $\delta > 0$ such that the following statement holds. If G is a finite quasisimple group of Lie type and χ_1, χ_2 are any (not necessarily irreducible) characters of G with $|\chi_1|, |\chi_2| \leq |G|^{\delta}$, then*

$$|\chi_1\chi_2| \geq \big(|\chi_1| \cdot |\chi_2|\big)^{1-\varepsilon}.$$

In particular, if χ is a character of G satisfying $|\chi| \leq |G|^{\delta}$, then $|\chi^2| \geq |\chi|^{2-2\varepsilon}$.

The inequality $|\chi_1\chi_2| \leq |\chi_1| \cdot |\chi_2|$ mentioned in (4.1) shows that the growth established in Theorem 4.5 is almost best possible.

Theorem 4.5 is easily extended to products of arbitrary length, in the spirit of Corollary 3.7 for k normal subsets.

Corollary 4.6. *For any $\varepsilon > 0$ and any integer $k \geq 1$, there exists an explicit $\gamma = \gamma(\varepsilon, k) > 0$ such that the following statement holds. If G is a finite quasisimple group of Lie type and $\chi_1, \chi_2, \ldots, \chi_k$ are any (not necessarily irreducible) characters of G with $|\chi_1|, |\chi_2|, \ldots, |\chi_k| \leq |G|^{\gamma}$, then*

$$|\chi_1\chi_2\cdots\chi_k| \geq \big(|\chi_1| \cdot |\chi_2| \cdots |\chi_k|\big)^{1-\varepsilon}.$$

In particular, if χ is a character of G satisfying $|\chi| \leq |G|^{\gamma}$, then $|\chi^k| \geq |\chi|^{k-k\varepsilon}$.

To show this, we prove by induction on $k \geq 2$ the following equivalent statement.

For any $\varepsilon > 0$ and any $k \geq 2$, there exists an explicit $\gamma > 0$ (depending on both ε and k) such that if G is a finite quasisimple group of Lie type and $\chi_1, \chi_2, \ldots, \chi_k$ are any characters of G with $|\chi_1|, |\chi_2|, \ldots, |\chi_k| \leq |G|^{\gamma}$, then

$$|\chi_1\chi_2\cdots\chi_k| \geq \big(|\chi_1| \cdot |\chi_2| \cdots |\chi_k|\big)^{1-k\varepsilon}.$$

We will show that this statement holds with $\gamma := \delta/(k-1)$, where δ is the constant in Theorem 4.5. The case $k = 2$ is already established in Theorem 4.5. For the

inductive step, note that (4.1) and the induction hypothesis yield

$$\big(|\chi_2|\cdots|\chi_k|\big)^{1-(k-1)\varepsilon} \le |\chi_2\cdots\chi_k| \le \prod_{i=2}^{k}|\chi_i| \le |G|^{\gamma(k-1)} \le |G|^{\delta}.$$

Since $|\chi_1| \le |G|^{\delta}$, by Theorem 4.5 we have

$$\begin{aligned}|\chi_1\chi_2\cdots\chi_k| &\ge \big(|\chi_1|\cdot|\chi_2\cdots\chi_k|\big)^{1-\varepsilon}\\ &\ge \big(|\chi_1|\cdot\big(|\chi_2|\cdots|\chi_k|\big)^{1-(k-1)\varepsilon}\big)^{1-\varepsilon}\\ &\ge \big(|\chi_1|\cdot|\chi_2|\cdots|\chi_k|\big)^{1-k\varepsilon}.\end{aligned}$$

The above result shows that, for any $\varepsilon > 0$ and any integer $k \ge 2$, there exists an explicit $\delta = \delta(\varepsilon, k) > 0$ such that, for G as above and any (not necessarily irreducible) character χ of G satisfying $|\chi| \le |G|^{\delta}$, we have $|\chi^k| \ge |\chi|^{k-\varepsilon}$; indeed, define $\delta(\varepsilon, k) = \gamma(\varepsilon/k, k)$.

Applying Theorem 4.5, we deduce the following result, which is a character-theoretic analogue of Theorem 3.4.

Theorem 4.7. *For all $\varepsilon > 0$, there exists an explicit positive integer b such that if G is a finite simple group of Lie type and χ is any (not necessarily irreducible) character of G, then either χ^b contains every irreducible character of G or $|\chi^2| \ge |\chi|^{2-\varepsilon}$.*

In view of Gowers' theorem, it is natural to ask whether $b = 3$ suffices in Theorem 4.7 when $|\chi|$ is sufficiently large. Sellke's theorem (Theorem 4.2) shows that the answer to this question is affirmative for large G provided that $|\chi| \ge |G|^{\delta}$ for some fixed $\delta > 0$. We therefore ask the following.

Question. If G is a finite simple group of Lie type and χ is an arbitrary character of G such that $|\chi| \ge |G|^{\delta}$ for some fixed $\delta > 0$, is it true that $|\chi^3| = |G|$ provided $|G| \gg 0$?

We remark that the stronger equality $|\chi^2| = |G|$ does not always hold, as shown by the example of $\mathrm{PSU}_{2n+1}(q)$ (see [23, Theorem 1.2]). On the other hand, for certain simple groups of Lie type, we can bring b down to 6 or 7.

Theorem 4.8. *If $G = \mathrm{PSL}_n(q)$ and q is sufficiently large in terms of n, then $|\chi| \ge |G|^{11/12}$ implies that $|\chi^6| = |G|$. If $G = \mathrm{PSU}_n(q)$ and q is sufficiently large in terms of n, then $|\chi| \ge |G|^{11/12}$ implies that $|\chi^7| = |G|$.*

Our next result is an analogue of Theorem 1.1 by Maróti and Pyber (following [45] and Rodgers–Saxl [59]), where the normal subsets are replaced by characters of G. In the case where the characters are irreducible, this analogue was conjectured by Gill in [14] and proved by Larsen and Tiep in [39, Theorem 8.5]. A more general version, for arbitrary characters, is given below.

Theorem 4.9. *There exists an explicit constant $c>0$ such that the following statement holds. If G is a finite simple group of Lie type, $m \geq 1$ any integer, and $\chi_1, \chi_2, \ldots, \chi_m$ are any (not necessarily irreducible) characters of G with $\prod_{i=1}^{m} |\chi_i| \geq |G|^c$, then $|\chi_1 \chi_2 \cdots \chi_m| = |G|$ and thus $\chi_1 \chi_2 \cdots \chi_m$ contains every irreducible character of G.*

Finally, we prove an analogue of Theorem 4.3 for compact semisimple Lie groups.

Theorem 4.10. *Let G be a compact semisimple Lie group. Then, there exists $\varepsilon > 0$ such that, for each irreducible character χ of G, we have $|\chi^2| \geq |\chi|^{1+\varepsilon}$.*

Funding. The author was supported in part by BSF grant 2016072, ISF grant 686/17, and the Vinik Chair of Mathematics which he holds.

References

[1] L. Babai, N. Nikolov, and L. Pyber, Product growth and mixing in finite groups. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 248–257, ACM, New York, 2008 Zbl 1192.60016 MR 2485310

[2] R. Bezrukavnikov, M. W. Liebeck, A. Shalev, and P. H. Tiep, Character bounds for finite groups of Lie type. *Acta Math.* **221** (2018), no. 1, 1–57 Zbl 06983623 MR 3877017

[3] R. Brauer, A note on theorems of Burnside and Blichfeldt. *Proc. Amer. Math. Soc.* **15** (1964), 31–34 Zbl 0122.27503 MR 158004

[4] E. Breuillard, Lectures on approximate groups and Hilbert's 5th problem. In *Recent Trends in Combinatorics*, pp. 369–404, IMA Vol. Math. Appl. 159, Springer, Cham, 2016 Zbl 1407.11019 MR 3526417

[5] E. Breuillard, B. Green, and T. Tao, Approximate subgroups of linear groups. *Geom. Funct. Anal.* **21** (2011), no. 4, 774–819 Zbl 1229.20045 MR 2827010

[6] E. Breuillard, B. Green, and T. Tao, Suzuki groups as expanders. *Groups Geom. Dyn.* **5** (2011), no. 2, 281–299 Zbl 1247.20017 MR 2782174

[7] P. J. Cameron and A. M. Cohen, On the number of fixed point free elements in a permutation group. A collection of contributions in honour of Jack van Lint. *Discrete Math.* **106/107** (1992), 135–138 Zbl 0813.20001 MR 1181907

[8] E. W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore. *Trans. Amer. Math. Soc.* **350** (1998), no. 9, 3657–3671 Zbl 0910.20007 MR 1422600

[9] P. Erdős and P. Turán, On some problems of a statistical group-theory. II. *Acta math. Acad. Sci. Hungar.* **18** (1967), 151–163 Zbl 0189.31302 MR 0207810

[10] S. V. Fomin and N. Lulov, On the number of rim hook tableaux. *J. Math. Sci. (New York)* **87** (1997), 4118–4123 Zbl 0909.05046

[11] 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), no. 6, 3023–3070 Zbl 1256.20048 MR 2888238

[12] J. Fulman and R. Guralnick, Derangements in subspace actions of finite classical groups. *Trans. Amer. Math. Soc.* **369** (2017), no. 4, 2521–2572 Zbl 1431.20033 MR 3592520

[13] J. Fulman and R. Guralnick, Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston–Shalev conjecture. *Trans. Amer. Math. Soc.* **370** (2018), no. 7, 4601–4622 Zbl 06862789 MR 3812089

[14] N. Gill, A Rodgers–Saxl type conjecture for characters. https://nickpgill.github.io/a-rodgers-saxl-conjecture-for-characters

[15] N. Gill, L. Pyber, I. Short, and E. Szabó, On the product decomposition conjecture for finite simple groups. *Groups Geom. Dyn.* **7** (2013), no. 4, 867–882 Zbl 1355.20013 MR 3134028

[16] N. Gill, L. Pyber, and E. Szabó, A generalization of a theorem of Rodgers and Saxl for simple groups of bounded rank. *Bull. Lond. Math. Soc.* **52** (2020), no. 3, 464–471 Zbl 07224936 MR 4171380

[17] W. T. Gowers, Quasirandom groups. *Combin. Probab. Comput.* **17** (2008), no. 3, 363–387 Zbl 1191.20016 MR 2410393

[18] R. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces. *J. Amer. Math. Soc.* **25** (2012), no. 1, 77–121 Zbl 1286.20007 MR 2833479

[19] R. M. Guralnick, M. Larsen, and P. H. Tiep, Character levels and character bounds. II. 2019, arXiv:1904.08070v1

[20] R. M. Guralnick, M. Larsen, and P. H. Tiep, Character levels and character bounds. *Forum Math. Pi* **8** (2020), e2 Zbl 07158138 MR 4061963

[21] R. M. Guralnick, M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep, Surjective word maps and Burnside's $p^a q^b$ theorem. *Invent. Math.* **213** (2018), no. 2, 589–695 Zbl 1397.20037 MR 3827208

[22] R. M. Guralnick and P. H. Tiep, Effective results on the Waring problem for finite simple groups. *Amer. J. Math.* **137** (2015), no. 5, 1401–1430 Zbl 1338.20009 MR 3405871

[23] G. Heide, J. Saxl, P. H. Tiep, and A. E. Zalesski, Conjugacy action, induced representations and the Steinberg square for simple groups of Lie type. *Proc. Lond. Math. Soc. (3)* **106** (2013), no. 4, 908–930 Zbl 1372.20017 MR 3056296

[24] H. A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math. (2)* **167** (2008), no. 2, 601–623 Zbl 1213.20045 MR 2415382

[25] H. A. Helfgott, Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$. *J. Eur. Math. Soc. (JEMS)* **13** (2011), no. 3, 761–851 Zbl 1235.20047 MR 2781932

[26] E. Hrushovski, Stable group theory and approximate subgroups. *J. Amer. Math. Soc.* **25** (2012), no. 1, 189–243 Zbl 1259.03049 MR 2833482

[27] E. Hrushovski, The elementary theory of the Frobenius automorphisms. 2022, arXiv: math/0406514v2

[28] M. Kassabov, Symmetric groups and expander graphs. *Invent. Math.* **170** (2007), no. 2, 327–354 Zbl 1191.20002 MR 2342639

[29] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443 Zbl 0325.20008 MR 360852

[30] S. Lang and A. Weil, Number of points of varieties in finite fields. *Amer. J. Math.* **76** (1954), 819–827 Zbl 0058.27202 MR 65218

[31] M. Larsen, Word maps have large image. *Israel J. Math.* **139** (2004), 149–156 Zbl 1130.20310 MR 2041227

[32] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications. *Invent. Math.* **174** (2008), no. 3, 645–687 Zbl 1166.20009 MR 2453603

[33] M. Larsen and A. Shalev, Word maps and Waring type problems. *J. Amer. Math. Soc.* **22** (2009), no. 2, 437–466 Zbl 1206.20014 MR 2476780

[34] M. Larsen, A. Shalev, and P. H. Tiep, Products of derangements in simple permutation groups. *Int. Math. Res. Not. IMRN*, to appear

[35] M. Larsen, A. Shalev, and P. H. Tiep, Products of normal subsets. Preprint

[36] M. Larsen, A. Shalev, and P. H. Tiep, The Waring problem for finite simple groups. *Ann. of Math. (2)* **174** (2011), no. 3, 1885–1950 Zbl 1283.20008 MR 2846493

[37] M. Larsen, A. Shalev, and P. H. Tiep, Probabilistic Waring problems for finite simple groups. *Ann. of Math. (2)* **190** (2019), no. 2, 561–608 Zbl 1448.20063 MR 3997129

[38] M. Larsen, A. Shalev, and P. H. Tiep, Representations and tensor product growth. 2021, arXiv:2104.11716

[39] M. Larsen and P. H. Tiep, Uniform character bounds for finite classical groups. Preprint

[40] M. W. Liebeck, N. Nikolov, and A. Shalev, Groups of Lie type as products of SL_2 subgroups. *J. Algebra* **326** (2011), 201–207 Zbl 1225.20016 MR 2746060

[41] M. W. Liebeck, N. Nikolov, and A. Shalev, Product decompositions in finite simple groups. *Bull. Lond. Math. Soc.* **44** (2012), no. 3, 469–472 Zbl 1250.20018 MR 2966992

[42] M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep, The Ore conjecture. *J. Eur. Math. Soc. (JEMS)* **12** (2010), no. 4, 939–1008 Zbl 1205.20011 MR 2654085

[43] M. W. Liebeck, G. Schul, and A. Shalev, Rapid growth in finite simple groups. *Trans. Amer. Math. Soc.* **369** (2017), no. 12, 8765–8779 Zbl 06790363 MR 3710643

[44] M. W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.* **12** (1999), no. 2, 497–520 Zbl 0916.20003 MR 1639620

[45] M. W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications. *Ann. of Math. (2)* **154** (2001), no. 2, 383–406 Zbl 1003.20014 MR 1865975

[46] 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 Zbl 1068.20052 MR 2058457

[47] M. W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type. *Proc. London Math. Soc. (3)* **90** (2005), no. 1, 61–86 Zbl 1077.20020 MR 2107038

[48] M. W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties. *Invent. Math.* **159** (2005), no. 2, 317–367 Zbl 1134.20059 MR 2116277

[49] M. W. Liebeck, A. Shalev, and P. H. Tiep, McKay graphs for alternating and classical groups. *Trans. Amer. Math. Soc.* **374** (2021), no. 8, 5651–5676 Zbl 07377376 MR 4293783

[50] M. W. Liebeck, A. Shalev, and P. H. Tiep, On the diameters of McKay graphs for finite simple groups. *Israel J. Math.* **241** (2021), no. 1, 449–464 Zbl 1475.20016 MR 4242157

[51] A. Lubotzky, Finite simple groups of Lie type as expanders. *J. Eur. Math. Soc. (JEMS)* **13** (2011), no. 5, 1331–1341 Zbl 1257.20016 MR 2825166

[52] T. Łuczak and L. Pyber, On random generation of the symmetric group. *Combin. Probab. Comput.* **2** (1993), no. 4, 505–512 Zbl 0817.20002 MR 1264722

[53] G. Malle, J. Saxl, and T. Weigel, Generation of classical groups. *Geom. Dedicata* **49** (1994), no. 1, 85–116 Zbl 0832.20029 MR 1261575

[54] A. Maróti and L. Pyber, A generalization of the diameter bound of Liebeck and Shalev for finite simple groups. *Acta Math. Hungar.* **164** (2021), no. 2, 350–359 Zbl 07377593 MR 4279340

[55] C. Martinez and E. Zelmanov, Products of powers in finite simple groups. *Israel J. Math.* **96** (1996), no. part B, 469–479 Zbl 0890.20013 MR 1433702

[56] M. B. Nathanson, *Additive Number Theory. The Classical Bases*. Grad. Texts in Math. 164, Springer, New York, 1996 Zbl 0859.11002 MR 1395371

[57] N. Nikolov and L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem. *J. Eur. Math. Soc. (JEMS)* **13** (2011), no. 4, 1063–1077 Zbl 1228.20020 MR 2800484

[58] L. Pyber and E. Szabó, Growth in finite simple groups of Lie type. *J. Amer. Math. Soc.* **29** (2016), no. 1, 95–146 Zbl 1371.20010 MR 3402696

[59] D. M. Rodgers and J. Saxl, Products of conjugacy classes in the special linear groups. *Comm. Algebra* **31** (2003), no. 9, 4623–4638 Zbl 1032.20031 MR 1995555

[60] J. Saxl and J. S. Wilson, A note on powers in simple groups. *Math. Proc. Cambridge Philos. Soc.* **122** (1997), no. 1, 91–94 Zbl 0890.20014 MR 1443588

[61] D. Segal, *Words: Notes on Verbal Width in Groups*. London Math. Soc. Lecture Note Ser. 361, Cambridge University Press, Cambridge, 2009 Zbl 1198.20001 MR 2547644

[62] M. Sellke, Covering $\mathrm{Irrep}(S_n)$ with tensor products and powers. 2020, arXiv: 2004.05283v3

[63] M. Sellke, Tensor quasi-random groups. *Proc. Amer. Math. Soc. Ser. B* **9** (2022), 12–21 MR 4377265

[64] A. Shalev, A theorem on random matrices and some applications. *J. Algebra* **199** (1998), no. 1, 124–141 Zbl 0910.20031 MR 1489358

[65] A. Shalev, Mixing and generation in simple groups. *J. Algebra* **319** (2008), no. 7, 3075–3086 Zbl 1146.20057 MR 2397424

[66] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem. *Ann. of Math. (2)* **170** (2009), no. 3, 1383–1416 Zbl 1203.20013 MR 2600876

[67] J. Taylor and P. H. Tiep, Lusztig induction, unipotent supports, and character bounds. *Trans. Amer. Math. Soc.* **373** (2020), no. 12, 8637–8676 Zbl 07301836 MR 4177271

[68] Y. Varshavsky, Lefschetz–Verdier trace formula and a generalization of a theorem of Fujiwara. *Geom. Funct. Anal.* **17** (2007), no. 1, 271–319 Zbl 1131.14019 MR 2306659

Aner Shalev
Einstein Institute of Mathematics, Hebrew University, Jerusalem 9190401, Israel;
aner.shalev@mail.huji.ac.il