Received: 22 January 2024 | Accepted: 18 April 2024

DOI: 10.1112/blms.13093

RESEARCH ARTICLE

Bulletin of the London Mathematical Society

# Growth of products of subsets in finite simple groups

**Daniele Dona** | **Attila Maróti** | **László Pyber**

Hun-Ren Alfréd Rényi Institute of Mathematics, Budapest, Hungary

**Correspondence**
Attila Maróti, Hun-Ren Alfréd Rényi Institute of Mathematics, Reáltanoda Utca 13-15, H-1053 Budapest, Hungary.
Email: maroti.attila@renyi.hu

**Funding information**
European Research Council; European Union's Horizon 2020 Research and Innovation Programme, Grant/Award Number: 741420; National Research, Development and Innovation Office, Grant/Award Numbers: K138596, K132951, K138828

**Abstract**

We prove that the product of a subset and a normal subset inside any finite simple non-abelian group $G$ grows rapidly. More precisely, if $A$ and $B$ are two subsets with $B$ normal and neither of them is too large inside $G$, then $|AB| \geqslant |A||B|^{1-\epsilon}$ where $\epsilon > 0$ can be taken arbitrarily small. This is a somewhat surprising strengthening of a theorem of Liebeck, Schul, and Shalev.

**MSC 2020**
20D06, 20F69 (primary)

## 1 | INTRODUCTION

The study of growth of products of subsets in finite simple groups has been the subject of significant work in the recent decades. Part of the interest revolves around a conjecture of Liebeck, Nikolov, and Shalev [5], which claims that for any finite simple non-abelian group $G$ and any set $A \subseteq G$ of size at least 2 we can write $G$ as the product of $N$ conjugates of $A$ with $N = O(\log|G|/\log|A|)$. This conjecture generalizes an already deep theorem of Liebeck and Shalev [7], which proves it for $A$ a *normal* subset, that is, a union of conjugacy classes of $G$.

In attempting to prove the conjecture, or partial cases thereof, a natural way is to show that the product of two subsets has size comparable to the product of the sizes of the two original sets. A result in this vein is the following, due to Gill, Pyber, Short, and Szabó [4, Proposition 5.2]. For any $\epsilon > 0$, there exists $\delta > 0$ such that if $G$ is a finite simple non-abelian group, $A$ is a subset with $|A| \leqslant |G|^{1-\delta}$, and $B$ is a normal subset, then $|AB| \geqslant |A||B|^{\epsilon}$. This theorem strengthens the expansion result given in [8, Proposition 10.4] for conjugacy classes that are not too large with respect to the size of $G$. Liebeck, Schul, and Shalev later used another result of this kind to prove that for small classes, and indeed for small normal subsets, the expansion is particularly rapid.

They proved [6, Theorem 1.3] that for any $\epsilon > 0$ there exists $\delta > 0$ such that if $G$ is a finite simple non-abelian group and $A, B$ are two normal subsets with $|A|, |B| \leqslant |G|^{\delta}$, then $|AB| \geqslant (|A||B|)^{1-\epsilon}$.

In the present paper, we prove the following.

**Theorem 1.1.** *For any $\epsilon > 0$ there exists $\delta > 0$ such that if $G$ is a finite simple non-abelian group, $A$ is a subset and $B$ is a normal subset with $|A|, |B| \leqslant |G|^{\delta}$, then $|AB| \geqslant |A||B|^{1-\epsilon}$.*

Theorem 1.1 is a direct generalization of [6, Theorem 1.3], and it improves [4, Proposition 5.2] for sets of size at most $|G|^{\delta}$.

## 2 | BOUNDING CONJUGACY CLASS SIZES IN ALTERNATING GROUPS

In this section, let $G$ be the alternating group of degree $r$ and let $x \in G$. We define $\Delta(x)$ to be $(r - t)/r$ where $t$ denotes the number of cycles in the disjoint cycle decomposition of $x$. The purpose of this section is to show that, unlike the support of $x$, the invariant $\Delta(x)$ controls the size of the conjugacy class $x^G$, provided that it is small.

We will need a variant of [2, Lemma 2.3].

**Lemma 2.1.** *For every $\gamma$ and $\epsilon$ with $0 < \gamma < 1$ and $0 < \epsilon < 1$ there exists $N$ such that for every $r \geqslant N$, whenever $x \in G$ satisfies $|x^G| \geqslant |G|^{\gamma}$, then $\Delta(x) > (1-\epsilon)\gamma$.*

*Proof.* Fix $\gamma$ and $\epsilon$ with $0 < \gamma < 1$ and $0 < \epsilon < 1$. According to [2, Lemma 2.3], for every $\epsilon_1 > 0$ there exists $N_1$ such that for every $r \geqslant N_1$, whenever $x \in G$ satisfies $|x^G| \geqslant |G|^{\gamma}$, then $\Delta(x) > \gamma - \epsilon_1$. It is sufficient to choose $\epsilon_1$ such that $\gamma - \epsilon_1 > (1-\epsilon)\gamma$. This is the case when $\epsilon_1 < \gamma\epsilon$. □

We need the following bounds of Stirling found in [1, 2.9].

**Lemma 2.2.** *For every positive integer $n$, we have*

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \leqslant n! \leqslant 2\sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

We are now in position to prove the main result of this section.

**Proposition 2.3.** *For all $\epsilon > 0$, there exists $\delta > 0$ such that whenever $G$ is an alternating group and $x \in G$ with $|x^G| \leqslant |G|^{\delta}$, then*

$$|G|^{\Delta(x)(1-\epsilon)} \leqslant |x^G| \leqslant |G|^{\Delta(x)(1+\epsilon)}.$$

*Proof.* Fix $\epsilon > 0$.

We may assume that $r$, the degree of the alternating group $G$, is sufficiently large. For if $r \leqslant c$ with a universal constant $c$, then by choosing $\delta$ less than $1/c$ the condition of the lemma implies that $x = 1$. The statement is clear for $x = 1$. Let us assume that $x \neq 1$.

Let $\delta_0$ be such that $|x^G| = |G|^{\delta_0}$. We may assume that $\delta_0 > 0$, for otherwise $x = 1$. The upper bound of the proposition amounts to showing that $\delta_0 \leqslant \Delta(x)(1+\epsilon)$. For every $\epsilon_1 > 0$, there exists

$N_1$ such that whenever $r \geqslant N_1$ then $\Delta(x) > (1-\epsilon_1)\delta_0$ by Lemma 2.1. Thus it suffices to choose $\epsilon_1$ such that $1 < (1-\epsilon_1)(1+\epsilon)$. This is the case when $\epsilon_1 < \epsilon/(1+\epsilon)$.

It remains to establish the lower bound of the proposition. We first prove the same statement for the symmetric group $H$ of degree $r$. For each integer $i$ with $1 \leqslant i \leqslant r$, let $c_i$ be the number of cycles of length $i$ in the disjoint cycle decomposition of $x$. We have

$$|C_H(x)| = \left(\prod_{i=1}^{r} c_i!\right)\left(\prod_{i=1}^{r} i^{c_i}\right) \leqslant \left(\sum_{i=1}^{r} c_i\right)!\left(\prod_{i=2}^{r} i^{c_i}\right) = t!\left(\prod_{i=2}^{r} i^{c_i}\right), \tag{1}$$

where $t$ is the number of cycles in the disjoint cycle decomposition of $x$. Observe that $t = r(1-\Delta(x))$. This and Lemma 2.2 give

$$\begin{aligned} t! &\leqslant 2\sqrt{2\pi t}\left(\frac{t}{e}\right)^t \leqslant 2\sqrt{2\pi r}\left(\frac{r}{e}\right)^t = 2\sqrt{2\pi r}\left(\frac{r}{e}\right)^{r(1-\Delta(x))} = \\ &= 2\left(\sqrt{2\pi r}\right)^{\Delta(x)}\left(\sqrt{2\pi r}\left(\frac{r}{e}\right)^r\right)^{1-\Delta(x)} \leqslant 2\left(\sqrt{2\pi r}\right)^{\Delta(x)}|H|^{1-\Delta(x)}. \end{aligned} \tag{2}$$

We have

$$2\left(\sqrt{2\pi r}\right)^{\Delta(x)} \leqslant |H|^{(\epsilon/2)\Delta(x)} \tag{3}$$

for every large enough $r$. By considering the derivative of the function $f(x) = x^{1/x}$, we see that $i^{1/i} \leqslant e^{1/e}$ for every positive integer $i$. It follows that

$$\prod_{i=1}^{r} i^{c_i} = \prod_{i=2}^{r} i^{(ic_i)/i} \leqslant \prod_{i=2}^{r} e^{ic_i/e} = e^{(\sum_{i=2}^{r} ic_i)/e}. \tag{4}$$

Now $\sum_{i=2}^{r} ic_i \leqslant \sum_{i=2}^{r} 2(i-1)c_i = 2(\sum_{i=1}^{r}(i-1)c_i) = 2\Delta(x)r$. Applying this to (4) gives

$$\prod_{i=1}^{r} i^{c_i} \leqslant e^{2\Delta(x)r/e} < |H|^{(\epsilon/2)\Delta(x)}, \tag{5}$$

holding for every sufficiently large $r$. By (1), (2), (3), and (5), we obtain

$$|C_H(x)| < |H|^{(\epsilon/2)\Delta(x)} \cdot |H|^{1-\Delta(x)} \cdot |H|^{(\epsilon/2)\Delta(x)} = |H|^{1-\Delta(x)(1-\epsilon)}.$$

Thus, $|H|^{\Delta(x)(1-\epsilon)} < |x^H|$. This proves the claim for the symmetric group $H$.

We proved above that for all $\epsilon_1 > 0$ there exists $\delta_1 > 0$ such that if $|x^H| \leqslant |H|^{\delta_1}$, then

$$|H|^{\Delta(x)(1-\epsilon_1)} \leqslant |x^H|. \tag{6}$$

We fixed $\epsilon > 0$. Take $\epsilon_1 = \epsilon/2$ and $\delta < \delta_1/2$. Inequality (6) gives $|x^G| > |H|^{\Delta(x)(1-(\epsilon/2))}/2$, which is at least $|G|^{\Delta(x)(1-\epsilon)}$ for every sufficiently large $r$, by noting that $\Delta(x) \geqslant 1/r$. This proves the lower bound of the proposition. □

## 3 | BOUNDING CONJUGACY CLASS SIZES IN SIMPLE CLASSICAL GROUPS

The purpose of this section is to extend Proposition 2.3 for the case when $G$ is a simple classical group. We also record a consequence.

Let $n \geqslant 2$ be an integer and $q$ a prime power. Let $G$ be one of the classical groups $\mathrm{L}_n^{\pm}(q)$, $\mathrm{PSp}_n(q)$ or $\mathrm{P}\Omega_n^{\pm}(q)$. Let $V = V_n(q^u)$ be the natural module for the lift of $G$ 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 $\mathrm{GL}(V)$. In [6], the support $\nu(x)$ of $x$ is defined to be

$$\nu(x) = \nu_{V,\overline{\mathbb{F}}}(x) = \min\{\mathrm{codim}(\ker(\hat{x} - \lambda I)) : \lambda \in \overline{\mathbb{F}}^*\}.$$

Define $a = a(G)$ to be 1 if $G = \mathrm{L}_n^{\pm}(q)$ and $1/2$ otherwise.

The following is [6, Proposition 3.4].

**Proposition 3.1.** *For any $\epsilon > 0$, there exists $\delta > 0$ such that if $x$ is an element of a simple classical group $G$ with $|x^G| \leqslant |G|^\delta$, then*

$$q^{(2a-\epsilon)n\nu(x)} \leqslant |x^G| \leqslant q^{(2a+\epsilon)n\nu(x)}.$$

For $x \in G$ where $G$ is a simple classical group, let

$$\Delta(x) = \frac{\nu(x) \cdot 2a \cdot n \cdot \log q}{\log |G|}.$$

We may now state the main result of this section.

**Proposition 3.2.** *For all $\epsilon > 0$ there exists $\delta > 0$ such that whenever $G$ is an alternating group or a simple classical group and $x \in G$ with $|x^G| \leqslant |G|^\delta$, then*

$$|G|^{\Delta(x)(1-\epsilon)} \leqslant |x^G| \leqslant |G|^{\Delta(x)(1+\epsilon)}.$$

*Proof.* Fix $\epsilon > 0$. We may assume that $G$ is a simple classical group with parameters $n$, $q$ and $a$, by Proposition 2.3. As $|G|^{\Delta(x)} = q^{2an\nu(x)}$, the conclusion of the proposition is

$$q^{2an\nu(x)(1-\epsilon)} \leqslant |x^G| \leqslant q^{2an\nu(x)(1+\epsilon)}. \tag{7}$$

Let $\epsilon_1 > 0$ be such that $\epsilon_1 < 2a\epsilon$. Choose $\delta > 0$ for $\epsilon_1$ such that Proposition 3.1 is satisfied. Assume that $|x^G| \leqslant |G|^\delta$. Then (7) follows from Proposition 3.1. □

We will need the following technical consequence of Proposition 3.2.

**Corollary 3.3.** *There exists $\delta > 0$ such that whenever $G$ is a (finite) alternating or simple classical group and $x_1, \ldots, x_k \in G$ such that $|x_1^G| \cdots |x_k^G| \leqslant |G|^\delta$, then there exists $z \in x_1^G \cdots x_k^G$ with $\Delta(z) = \Delta(x_1) + \cdots + \Delta(x_k)$.*

*Proof.* Choose $\delta > 0$ such that whenever $G$ is an alternating group or a simple classical group and $x \in G$ with $|x^G| \leqslant |G|^\delta$, then $\Delta(x) < 1/4$. Such a $\delta$ exists by Proposition 3.2.

Let $x_1, \ldots, x_k$ be elements in an alternating or simple classical group $G$ such that $|x_1^G| \cdots |x_k^G| \leqslant |G|^\delta$. For each $i$ with $1 \leqslant i \leqslant k$, let $s_i = \Delta(x_i)$. Put $s = \sum_{i=1}^k s_i$.

For every $i$ with $1 \leqslant i \leqslant k$, the inequality $|x_i^G| \leqslant |G|^\delta$ implies that $s_i < 1/4$. Let $i$ and $j$ be two distinct indices from $\{1, \ldots, k\}$. We have $|x_i^G x_j^G| \leqslant |x_i^G||x_j^G| \leqslant |G|^\delta$, $s_i < 1/4$ and $s_j < 1/4$. As both $s_i$ and $s_j$ are less than $1/4$, the normal set $x_i^G x_j^G$ contains a conjugacy class $y^G$ with $y \in G$ and $\Delta(y) = s_i + s_j$ by [6, Lemma 3.5], for classical groups $G$. The same statement holds when $G$ is an alternating group. As $|y^G| \leqslant |G|^\delta$, we have $s_i + s_j = \Delta(y) < 1/4$. Continuing in this way, we find that there is an element $z \in G$ such that $z^G$ is contained in $x_1^G \cdots x_k^G$, and $z$ satisfies $\Delta(z) = s_1 + \cdots + s_k = s$ and $s$ is less than $1/4$. □

## 4 | LOWER BOUNDS ON CONJUGACY CLASS SIZES IN SIMPLE GROUPS

Let $G$ be a non-abelian finite simple group different from a sporadic group. We define the rank of $G$ to be its untwisted Lie rank if it is a group of Lie type and to be its degree if it is an alternating group (and not a group of Lie type).

**Lemma 4.1.** *Every nontrivial conjugacy class of a non-abelian finite simple group of rank $r$ has size at least $|G|^{1/16r}$.*

*Proof.* Let $G = G_r(q)$ be a finite simple group of Lie type of rank $r$ defined over $\mathbb{F}_q$, the finite field of order $q$. Let $x$ be an arbitrary nontrivial element in $G$. We have

$$q^{r/2} \leqslant |x^G| \leqslant |G| \leqslant q^{8r^2}$$

by [3, Proposition 2.2]. The result follows in this case. Let $G$ be the alternating group of degree $r \geqslant 5$. As the minimal index of a proper subgroup of $G$ in $G$ is $r$, every nontrivial conjugacy class of $G$ has size at least $r > r^{1/16} \geqslant |G|^{1/16r}$. □

The following is [6, Theorem 2.2].

**Lemma 4.2.** *For any $\epsilon > 0$, there exists $N$ such that if $G$ is a non-abelian finite simple group of rank at least $N$ and $B$ is a nonempty normal subset of $G$, then $B$ contains a conjugacy class of $G$ of size at least $|B|^{1-\epsilon}$.*

We are in position to prove the following result.

**Proposition 4.3.** *For any $\epsilon > 0$, there exists $\delta > 0$ such that whenever $B_1, \ldots, B_k$ are nonempty normal subsets in a non-abelian finite simple group $G$ with*

$$|B_1| \cdots |B_k| \leqslant |G|^\delta,$$

*then there exists $z \in B_1 \cdots B_k$ such that*

$$|z^G| \geqslant (|B_1| \cdots |B_k|)^{1-\epsilon}.$$

*Proof.* Fix $\epsilon > 0$. We may assume that $\epsilon < 1$. Let $G$ be a non-abelian finite simple group. Let $k$ be a positive integer and let $B_1, \dots, B_k$ be nonempty normal subsets in $G$. For each $i$ with $1 \leqslant i \leqslant k$, let $x_i$ be a member of a largest conjugacy class in $B_i$. We may assume that each $x_i$ is different from 1.

Assume first that $|G|$ is bounded from above by a constant $c$. If $\delta$ is chosen to be less than $1/c$, then $|G|^\delta < 2$, and the statement is clear. Thus from now on we may assume that $|G|$ is unbounded. In particular, we assume that $G = G_r(q)$ is a finite simple group of Lie type of rank $r$ defined over $\mathbb{F}_q$, the finite field of order $q$, or $G$ is the alternating group of degree $r \geqslant 5$.

Assume first that $r$ is bounded from above by a constant $c$. If $\delta$ is chosen to be less than $1/16c$, then the statement follows from Lemma 4.1. Thus, from now on we may assume that $r$ is sufficiently large, that is, $G$ is a finite simple classical group whose lift acts naturally on a vector space of large enough dimension, or $G$ is the alternating group of large enough degree.

We may assume by Lemma 4.2 that for every $i$ with $1 \leqslant i \leqslant k$ we have $|x_i^G| \geqslant |B_i|^{1-\epsilon_1}$ for any fixed $\epsilon_1 > 0$. If there exists $z \in x_1^G \cdots x_k^G$ such that

$$|z^G| \geqslant (|x_1^G| \cdots |x_k^G|)^{1-(\epsilon/2)}, \tag{8}$$

then

$$|z^G| \geqslant (|B_1| \cdots |B_k|)^{(1-\epsilon_1)(1-(\epsilon/2))} \geqslant (|B_1| \cdots |B_k|)^{1-\epsilon}$$

whenever $\epsilon_1$ is chosen such that $\epsilon_1 \leqslant \epsilon/(2-\epsilon)$.

In the rest of the proof, we will find an element $z \in x_1^G \cdots x_k^G$ such that (8) holds.

We may assume that $|x_1^G| \cdots |x_k^G| \leqslant |G|^{\delta_1}$ where $\delta_1$ is a constant whose existence is assured by Corollary 3.3. Let $z \in x_1^G \cdots x_k^G$ such that $\Delta(z) = \sum_{i=1}^k \Delta(x_i)$. For each $i$ with $1 \leqslant i \leqslant k$, let $s_i = \Delta(x_i)$. Put $s = \sum_{i=1}^k s_i$.

Let $\epsilon_2 > 0$ be such that $\epsilon_2 < \epsilon/(4-\epsilon)$. Let $\delta_2 > 0$ be a constant whose existence is assured by Proposition 3.2 for $\epsilon_2$. Let $\delta$ be the minimum of $\delta_1$ and $\delta_2$. On one hand, Proposition 3.2 gives

$$|z^G| \geqslant |G|^{(1-\epsilon_2)s} \tag{9}$$

and on the other,

$$|x_1^G| \cdots |x_k^G| \leqslant |G|^{(1+\epsilon_2)\sum_{i=1}^k s_i} = |G|^{(1+\epsilon_2)s}. \tag{10}$$

Finally, inequality (8) is satisfied because $(1-\epsilon_2)s > (1+\epsilon_2)s(1-(\epsilon/2))$. ☐

## 5 | PROOF OF THEOREM 1.1

Gill, Pyber, Short, and Szabó [4, Theorem 4.3] proved the following important result.

**Proposition 5.1.** *Let $A$ and $B$ be finite sets in a group $G$ with $B$ normal in $G$. Suppose that $|AB| \leqslant K|A|$ for some positive number $K$. Then there exists a nonempty subset $X$ of $A$ such that $|XB^k| \leqslant K^k|X|$ for $k \geqslant 1$. In particular, $|B^2| \leqslant K|B|$ implies that $|B^k| \leqslant K^k|B|$ for $k \geqslant 1$.*

*Proof of Theorem* 1.1. Fix $\epsilon > 0$. We may assume that $\epsilon < 1$. Choose $\delta_1$ satisfying the statement of Proposition 4.3 with $\epsilon/2$. Let $\delta = (\epsilon/2) \cdot (1 + (\epsilon/2))^{-1}\delta_1$. Let $G$ be a non-abelian finite simple group. Let $B$ be a normal subset in $G$ and let $A$ be a subset of $G$, both of size at most $|G|^{\delta}$. The result is clear if $B = 1$. Thus, assume that $B \neq 1$. Let $k$ be the smallest positive integer for which $|A| \leqslant |B|^{(\epsilon/2)k}$. Then $|B|^{(\epsilon/2)(k-1)} \leqslant |A|$ and so

$$|B|^{(\epsilon/2)k} \leqslant |A||B|^{\epsilon/2} \leqslant |G|^{\delta}|G|^{\delta(\epsilon/2)} = |G|^{(1+(\epsilon/2))\delta} = |G|^{(\epsilon/2)\delta_1}. \tag{11}$$

Let $K > 0$ be the number defined by $|AB| = K|A|$. Let $X$ be a subset of $A$ whose existence is assured by Proposition 5.1. We get

$$|B^k| \leqslant |XB^k| \leqslant K^k|X| \leqslant K^k|A| \leqslant K^k|B|^{(\epsilon/2)k} \tag{12}$$

by Proposition 5.1. We have

$$|B^k| \geqslant |B|^{(1-(\epsilon/2))k} \tag{13}$$

by (11) and Proposition 4.3. Inequalities (12) and (13) provide $|B|^{(1-(\epsilon/2))k} \leqslant K^k|B|^{(\epsilon/2)k}$, and so $K \geqslant |B|^{1-\epsilon}$. The result follows. □


## ACKNOWLEDGMENTS

The project leading to this application has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreement Number: 741420). The second and third authors were also supported by the National Research, Development and Innovation Office (NKFIH), Grant Number: K138596. The second author was also funded by Grant Numbers: K132951 and K138828.



## JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.


## REFERENCES


1. W. Feller, *An introduction to probability theory and its applications*, 3rd ed., vol. 1, Wiley, New York, 1968.
2. M. Garonzi and A. Maróti, *Alternating groups as products of four conjugacy classes*, Arch. Math. (Basel) **116** (2021), no. 2, 121–130.
3. 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.
4. 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.
5. M. W. Liebeck, N. Nikolov, and A. Shalev, *Product decompositions in finite simple groups*, Bull. Lond. Math. Soc. **44** (2012), no. 3, 469–472.
6. M. W. Liebeck, G. Schul, and A. Shalev, *Rapid growth in finite simple groups*, Trans. Amer. Math. Soc. **369** (2017), no. 12, 8765–8779.
7. M. W. Liebeck and A. Shalev, *Diameters of finite simple groups: sharp bounds and applications*, Ann. of Math. (2) **154** (2001), 383–406.
8. A. Shalev, *Word maps, conjugacy classes, and a noncommutative Waring-type theorem*, Ann. of Math. (2) **170** (2009), 1383–1416.