# A GENERALIZATION OF THE DIAMETER BOUND OF LIEBECK AND SHALEV FOR FINITE SIMPLE GROUPS

ATTILA MARÓTI AND LÁSZLÓ PYBER

ABSTRACT. Let $G$ be a non-abelian finite simple group. A famous result of Liebeck and Shalev is that there is an absolute constant $c$ such that whenever $S$ is a non-trivial normal subset in $G$ then $S^k = G$ for any integer $k$ at least $c \cdot (\log |G| / \log |S|)$. This result is generalized by showing that there exists an absolute constant $c$ such that whenever $S_1, \ldots, S_k$ are normal subsets in $G$ with $\prod_{i=1}^{k} |S_i| \geq |G|^c$ then $S_1 \cdots S_k = G$.

*To the memory of Jan Saxl.*

## 1. INTRODUCTION

A normal subset of a finite group $H$ is defined to be any union of conjugacy classes of $H$. A normal subset is called trivial if it is equal to the identity. A well-known theorem of Liebeck and Shalev [14, Theorem 1.1] is that there is a constant $c$ such that whenever $S$ is a non-trivial normal subset in a non-abelian finite simple group $G$ then $S^k = G$ for any integer $k$ at least $c \cdot (\log |G| / \log |S|)$.

Gill, Pyber and Szabó propose the following conjecture [5, Conjecture 2].

**Conjecture 1.1.** *There exists a constant $c$ such that if $S_1, \ldots, S_k$ are normal subsets of a non-abelian finite simple group $G$ satisfying $\prod_{i=1}^{k} |S_i| \geq |G|^c$, then $S_1 \cdots S_k = G$.*

This is a weaker form of another conjecture of Gill, Pyber, Szabó [5, Conjecture 1] which is stated as follows. There exists a constant $c$ such that if $S_1, \ldots, S_k$ are subsets of a non-abelian finite simple group $G$ satisfying $\prod_{i=1}^{k} |S_i| \geq |G|^c$, then there are elements $g_1, \ldots, g_k \in G$ such that $(S_1)^{g_1} \cdots (S_k)^{g_k} = G$. This is known to hold [5, Theorem 2] for finite simple groups of Lie type of bounded rank.

Rodgers [19, Corollary 2.4] shows that if $C_1, \ldots, C_k$ are conjugacy classes of the symmetric group $\mathrm{Sym}(n)$ of degree $n \geq 5$ and $\prod_{i=1}^{k} |C_i| > n^{6(n-2)}$, then $C_1 \cdots C_k$ is equal to the alternating group $\mathrm{Alt}(n)$ of degree $n$ or to $\mathrm{Sym}(n) \setminus \mathrm{Alt}(n)$. Let $H$

be a non-solvable special linear group $\mathrm{SL}(n,q)$ or a projective special linear group $\mathrm{PSL}(n,q)$ with $n \geq 2$ and $q$ a prime power. Rodgers and Saxl [20] prove that if $C_1, \ldots, C_k$ are conjugacy classes of $H$ with the property that $\prod_{i=1}^{k} |C_i| \geq |H|^{12}$ then $C_1 \cdots C_k = H$.

This in particular implies that the constant $c$ in the Liebeck-Shalev theorem [14, Theorem 1.1] may be taken to be 12 in the case of $\mathrm{PSL}(n,q)$. It would be interesting to show that the theorem holds with a similar small constant $c$ for all non-abelian finite simple groups.

The aim of this paper is to prove Conjecture 1.1.

**Theorem 1.2.** *Conjecture 1.1 is true.*

The argument relies on the Liebeck-Shalev Theorem [14, Theorem 1.1] via [4, Proposition 5.2], on deep character theoretic results of Guralnick, Larsen and Tiep [7, Theorem 1.3] and of Liebeck and Shalev [15, Theorem 1.1], and in the case of alternating groups on results of Rodgers [19]. We actually give a new, different proof of the result of Rodgers and Saxl [20] with a weaker, non-explicit constant in the exponent.

A by-product of the proof of Theorem 1.2 is the following result.

**Theorem 1.3.** *Let $G$ be a non-abelian finite simple group. There exists a constant $\delta$ with $0 < \delta < 1$ such that if $S_1, \ldots, S_8$ are normal subsets in $G$ each of size at least $|G|^{\delta}$, then $S_1 \cdots S_8 = G$ in case $G$ is an alternating group and $S_1 S_2 S_3 = G$ in case $G$ is different from an alternating group.*

For $G$ a classical simple group, Theorem 1.3 was obtained independently using different techniques by Larsen, Shalev, Tiep in [12, Theorem 7.4].

Note that if $\delta$ is chosen appropriately, Theorem 1.3 is trivially true for groups of orders less than any given universal constant and it is easy to establish for groups of Lie type of bounded rank, in particular for exceptional groups.

Theorem 1.3 implies various results in [21]. In particular, it improves the following key result [21, Corollary 2.5]. For every $\epsilon > 0$ there is a number $r(\epsilon)$ such that whenever $G$ is a finite simple group of Lie type of Lie rank $r \geq r(\epsilon)$ defined over the field with $q$ elements, $C_1$, $C_2$, $C_3$ are conjugacy classes of $G$, $x_1 \in C_1$, $x_2 \in C_2$, $x_3 \in C_3$, and $|C_G(x_1)||C_G(x_2)||C_G(x_3)| \leq q^{(4-\epsilon)r}$, then $C_1 C_2 C_3 = G$.

Theorem 1.3 could be considered as an alternative approach to a conjecture of Thompson. Let $G$ be a non-abelian finite simple group. Thompson's Conjecture states that $G$ has a conjugacy class $C$ such that $C^2 = G$. This is established for alternating groups [22] and for finite simple groups of Lie type [3] defined over fields of size larger than 8.

There are other results in the literature which may be considered as approximations of Thompson's conjecture. For every sufficiently large $G$ there is a conjugacy class $C$ such that $C^3 = G$ by [21, Corollary 2.3]. It is also known [8, Theorem 1.4] that for every $G$ there are conjugacy classes $C$ and $D$ of $G$ such that $CD \cup \{1\} = G$ (this is an extension of results in [16] and also of [11, Theorem 1.1.4]).

It would be interesting to find the smallest integer $r$ with $3 \leq r \leq 8$ such that in Theorem 1.3 we get $S_1 \cdots S_r = G$. (Note that if $S_1$ and $S_2$ are conjugacy classes (of size at least $|G|^\delta$) with $S_1 \neq S_2^{-1}$ then $S_1 S_2 \neq G$.) It would also be interesting to determine the smallest value of $\delta$ for which Theorem 1.3 holds.

## 2. SMALL NORMAL SETS

In this section it is shown that in order to prove Theorem 1.2 we may assume that each normal subset $S_i$ of $G$ is large.

The starting point is [4, Proposition 5.2].

**Lemma 2.1** (Gill, Pyber, Short, Szabó)**.** *For every $\delta$ with $0 < \delta < 1$ there exists $\epsilon > 0$ such that for any non-abelian finite simple group $G$ and subsets $A$ and $B$ of $G$ with $B$ normal in $G$ and $|A| \leq |G|^\delta$ we have*

$$|AB| \geq |A||B|^\epsilon.$$

Note again that the proof of Lemma 2.1 depends on [14, Theorem 1.1]. In the course of the proof of Theorem 1.2 this is the only place where [14, Theorem 1.1] is used.

Fix $\delta$ and let $\epsilon > 0$ be a constant whose existence is assured by Lemma 2.1.

**Lemma 2.2.** *Let $G$ be a non-abelian finite simple group and $t$ an integer at least 2. If $A_1, \ldots, A_t$ are normal subsets in $G$ with $|A_1 \cdots A_{t-1}| \leq |G|^\delta$, then*

$$|A_1 \cdots A_t| \geq (|A_1| \cdots |A_t|)^\epsilon.$$

*Proof.* This follows by applying Lemma 2.1 $t - 1$ times. $\square$

Lemma 2.2 has an immediate consequence.

**Corollary 2.3.** *Let $G$ be a non-abelian finite simple group and let $A_1, \ldots, A_t$ be normal subsets in $G$. If $|A_1| \cdots |A_t| > |G|^{1/\epsilon}$, then $|A_1 \cdots A_t| \geq |G|^\delta$.*

*Proof.* Since $0 < \epsilon \leq 1$, we may assume that $t \geq 2$. If $|A_1 \cdots A_t| < |G|^\delta$, then $|A_1 \cdots A_t| \geq (|A_1| \cdots |A_t|)^\epsilon > |G|$ by Lemma 2.2. A contradiction. $\square$

Corollary 2.3 is applied in the following.

**Lemma 2.4.** *In proving Theorem 1.2 (i.e. Conjecture 1.1) we may assume that each normal subset $S_i$ has size at least $|G|^\delta$.*

*Proof.* Assume that there exists a constant $a$ such that whenever $j$ is an integer at least $a$ and $A_1, \ldots, A_j$ are normal subsets of $G$ satisfying $|A_i| \geq |G|^\delta$ for every $i$ with $1 \leq i \leq j$, then $A_1 \cdots A_j = G$.

Let $S_1, \ldots, S_k$ be arbitrary normal subsets in $G$ such that $\prod_{i=1}^k |S_i| \geq |G|^{a(1+1/\epsilon)}$. We claim that $S_1 \cdots S_k = G$.

We choose the smallest number $t_1$ such that $|S_1| \cdots |S_{t_1}| > |G|^{1/\epsilon}$. It is clear that $|S_1| \cdots |S_{t_1}| \leq |G|^{1+1/\epsilon}$ and by Corollary 2.3 we have $|S_1 \cdots S_{t_1}| \geq |G|^\delta$.

Similarly, we choose numbers $0 = t_0, t_1, \ldots, t_j$ with $1 \leq t_1 < t_2 < \ldots < t_j \leq k$ such that for every $i$ with $0 \leq i \leq j-1$ we have $|G|^{1/\epsilon} < |S_{t_i+1}| \cdots |S_{t_{i+1}}| \leq |G|^{1+1/\epsilon}$ and hence $|A_{i+1}| \geq |G|^\delta$ where $A_{i+1} = S_{t_i+1} \cdots S_{t_{i+1}}$.

The condition $\prod_{i=1}^{k} |S_i| \geq |G|^{a(1+1/\epsilon)}$ implies $j \geq a$. The lemma now follows from the first paragraph of the proof. $\square$

Theorem 1.2 follows from Lemma 2.4 together with Theorem 1.3. The rest of the paper is devoted to the proof of Theorem 1.3.

## 3. Groups of bounded rank

Theorem 1.3 is true for every non-abelian simple group $G$ of order less than $2^{1/(1-\delta)}$. To see this observe that under this condition each $S_i$ has size larger than $|G|/2$, and apply the following lemma found in [9, p. 58; 10].

**Lemma 3.1.** *If $A$ and $B$ are subsets of a finite group $G$ with $|A| + |B| > |G|$, then $AB = G$.*

*Proof.* Fix $g \in G$. Since $|A| + |gB^{-1}| > |G|$, we have $A \cap gB^{-1} \neq \emptyset$ and therefore $g = ab$ for some $a \in A$ and $b \in B$. $\square$

It is mentioned in the Introduction that a stronger form of Conjecture 1.1 is known to hold for finite simple groups of Lie type of bounded rank. This is proved by Gill, Pyber, Szabó [5, Theorem 2] using the Product Theorem established independently by Pyber, Szabó [18] and Breuillard, Green, Tao [2].

We now prove Theorem 1.3 for finite simple groups of bounded rank. Together with Lemma 2.4 this yields a shorter and more direct proof of Conjecture 1.1 in this case.

It is observed by Nikolov and Pyber in [17] that a result of Gowers [6] implies the following.

**Lemma 3.2.** *Let $G$ be a finite group and let $m$ denote the dimension of the smallest non-trivial complex irreducible representation of $G$. If $A$, $B$, $C$ are subsets of $G$ such that $|A||B||C| \geq |G|^3/m$, then $ABC = G$.*

Let $G$ be a finite simple group of Lie type of rank $r$. As noted in [5, Section 2], using Lemma 3.2, it follows that if $A$, $B$, $C$ are subsets of $G$ each of size larger than $|G|^{1-1/(24r^2)}$, then $ABC = G$.

Choose $\delta$ such that $\delta > 1 - 1/(24r^2)$ holds. Theorem 1.3 then follows for finite simple groups of Lie type of rank at most $r$ since $S_1 S_2 S_3 = G$ by the previous paragraph.

**Lemma 3.3.** *In proving Theorem 1.3 we may assume that $G$ is an alternating group $\mathrm{Alt}(n)$ or $G$ is a classical simple group $\mathrm{Cl}(n, q)$ and in both cases we may assume that $n$ is sufficiently large.*

From now on assume that $G$ is an alternating or a classical simple group.

## 4. LARGE CONJUGACY CLASSES

The aim of this section is to pass in Theorem 1.3 from (large) normal subsets to large conjugacy classes.

Let $k(H)$ denote the number of conjugacy classes of a finite group $H$. Part (i) of the next lemma is due to Kovács and Robinson [10, Lemma 1.1], while part (ii) follows from a special case of a result of Liebeck and Pyber [13, Theorem 1.1].

**Lemma 4.1.** *The following hold.*

   (i) $k(\mathrm{Alt}(n)) \leq 2^{n-1}$ *for* $n \geq 5$.
   (ii) $k(\mathrm{Cl}(n, q)) \leq q^{dn}$ *for some constant* $d$.

Fix $\alpha$ with $0 < \alpha < \delta < 1$.

**Lemma 4.2.** *If $A$ is a normal subset of $G$ with $|A| \geq |G|^{\delta}$, then $A$ contains a conjugacy class $C$ of $G$ with $|C| \geq |G|^{\alpha}$, at least for $n$ sufficiently large.*

*Proof.* Any normal subset $A$ of $G$ contains a conjugacy class $C$ of $G$ of size at least $|A|/k(G)$. If in addition it is assumed that $|A| \geq |G|^{\delta}$, then $|C| \geq |G|^{\alpha}$ by Lemma 4.1, at least for $n$ sufficiently large. $\qquad\square$

Assume that there is a choice of $\alpha$ such that whenever $C_1, \ldots, C_r$ are conjugacy classes in $G$ each of size at least $|G|^{\alpha}$, then $C_1 \cdots C_r = G$. For sufficiently large $n$, each $S_i$ contains a conjugacy class $C_i$ of $G$ of size at least $|G|^{\alpha}$ by Lemma 4.2. Thus $S_1 \cdots S_r \supseteq C_1 \cdots C_r = G$.

The following is proved.

**Lemma 4.3.** *In proving Theorem 1.3 we may assume that each of the normal subsets $S_i$ is a conjugacy class of size at least $|G|^{\alpha}$.*

## 5. ALTERNATING GROUPS

In this section we prove Theorem 1.3 in the case when $G = \mathrm{Alt}(n)$ and $n \geq 9$ is sufficiently large.

For each index $i$ with $1 \leq i \leq 8$, the normal set $S_i$ is a conjugacy class by Lemma 4.3 with
$$|S_i| \geq |G|^{\alpha} = |\mathrm{Alt}(n)|^{\alpha} = \left(\frac{n!}{2}\right)^{\alpha} > \frac{1}{2}\left(\frac{n}{2}\right)^{\alpha n} > n^{\beta n},$$
for any constant $\beta$ with $\beta < \alpha$, provided that $n$ is sufficiently large.

A key invariant in [19] is the following. Let $C$ be a conjugacy class of $\mathrm{Alt}(n)$ or of $\mathrm{Sym}(n)$. Define $\delta(C)$ to be $n - t$ where $t$ is the number of orbits of $\langle x \rangle$ (on the underlying set $\{1, \ldots, n\}$) for an element $x \in C$. It is implicit in the proof of [19, Corollary 2.4] that $|C| \leq n^{2\delta(C)}$.

The previous two paragraphs imply $\delta(S_i) > \beta n/2$ for every $i$ with $1 \leq i \leq 8$.

A special case of [19, Theorem 2.3] is the following.

**Lemma 5.1** (Rodgers). *Let $C_1, \ldots, C_r$ be conjugacy classes of $\mathrm{Sym}(n)$ such that every conjugacy class is contained in $\mathrm{Alt}(n)$. If $\sum_{i=1}^{r} \delta(C_i) > 3(n-2)$ and $n \geq 5$, then $C_1 \cdots C_r = \mathrm{Alt}(n)$.*

Let $\ell \geq 0$ be the number of $S_i$ which are conjugacy classes not only of $\mathrm{Alt}(n)$ but also of $\mathrm{Sym}(n)$. Without loss of generality, let these classes be $S_1, \ldots, S_\ell$.

Each $S_i$ with $i$ between $\ell + 1$ and 8 has the property that it is not a conjugacy class in $\mathrm{Sym}(n)$, that is, for every $x \in S_{\ell+1} \cup \ldots \cup S_8$ the disjoint cycles in $x$ have pairwise different odd lengths.

Let $x$ be an arbitrary element in $S_{\ell+1} \cup \ldots \cup S_8$. Let $t$ be the number of orbits of $\langle x \rangle$. We claim that $t \leq \sqrt{n}$. Let $s$ be the largest odd integer such that

$$(s+1)^2/4 = 1 + 3 + \ldots + (s-2) + s \leq n.$$

If $t > (s+1)/2$, then $x$ must act on at least $(s+1)^2/4 + (s+2) > n$ points. This is a contradiction, so $t \leq (s+1)/2 \leq \sqrt{n}$.

We claim that for any $i$ and $j$ with $\ell + 1 \leq i < j \leq 8$ and any $n \geq 9$, there is a conjugacy class $C_{i,j}$ of $\mathrm{Sym}(n)$ and also of $\mathrm{Alt}(n)$ such that $C_{i,j} \subseteq S_i S_j$ and

$$\delta(C_{i,j}) \geq n - 2\sqrt{n} - 2.$$

Let $x$ and $y$ be elements of $S_i$ and $S_j$ respectively, chosen in such a way that in the disjoint cycle decompositions of $x$ and $y$ the numbers 1 through $n$ are in increasing order and the cycle lengths are in decreasing order. If $n \geq 9$, then the numbers 1, 2, 3, 4 all appear in the longest cycles of $x$ and $y$. Let $y'$ be the conjugate permutation $y^{(12)(34)} \in S_j$. The permutation $xy' \in S_i S_j$ fixes 1 and 3 and thus, having at least two fixed points, the conjugacy class $C_{i,j}$ of $\mathrm{Alt}(n)$ containing $xy'$ is also a conjugacy class of $\mathrm{Sym}(n)$. Observe that the number of orbits of $\langle xy' \rangle$ is at most the number of integers $i$ with $1 \leq i \leq n$ such that $i(xy') \leq i$. This is at most

$$|\{i \ : \ ix \leq i\}| + |\{i \ : \ ix > i \text{ and } (ix)y' < ix\}| \leq$$

$$\leq |\{i \ : \ ix \leq i\}| + |\{i \ : \ iy' \leq i\}| \leq 2\sqrt{n} + 2$$

since both $\langle x \rangle$ and $\langle y \rangle$ have at most $\sqrt{n}$ orbits. It follows that $\delta(C_{i,j}) \geq n - 2\sqrt{n} - 2$.

Let $\Delta$ be $\delta(C_{\ell+1,\ell+2}) + \cdots + \delta(C_{7,8})$ if $\ell$ is even and $\delta(C_{\ell+1,\ell+2}) + \cdots + \delta(C_{6,7})$ if $\ell$ is odd. In any case, $\Delta \geq [(8-\ell)/2](n - 2\sqrt{n} - 2)$ where $[(8-\ell)/2]$ denotes the integer part of $(8-\ell)/2$.

The above gives

$$\delta(S_1) + \cdots + \delta(S_\ell) + \Delta \geq \frac{\beta\ell}{2} n + \Big[\frac{8-\ell}{2}\Big](n - 2\sqrt{n} - 2).$$

Now choose $\beta$ larger than $7/8$.

Since $\beta > 7/8$ and $\ell \leq 8$, we have

$$\frac{\beta\ell}{2} n + \Big[\frac{8-\ell}{2}\Big](n - 2\sqrt{n} - 2) > \Big(\frac{7}{2} - \frac{\ell}{16}\Big) \cdot n > 3(n-2),$$

for every sufficiently large $n$. Finally Lemma 5.1 gives

$$S_1 \cdots S_8 \supseteq S_1 \cdots S_\ell \cdot C_{\ell+1,\ell+2} \cdots C_{7,8} = \mathrm{Alt}(n)$$

if $\ell$ is even and

$$S_1 \cdots S_7 \supseteq S_1 \cdots S_\ell \cdot C_{\ell+1,\ell+2} \cdots C_{6,7} = \mathrm{Alt}(n)$$

if $\ell$ is odd.

This finishes the proof of Theorem 1.3 in case $G = \mathrm{Alt}(n)$.

## 6. Classical simple groups

In this section the proof of Theorem 1.3 and Theorem 1.2 is completed.

It may be assumed by Lemma 3.3 and the previous section that $G$ is a classical simple group $\mathrm{Cl}(n, q)$ with sufficiently large $n$.

A special case of [7, Theorem 1.3] is the following.

**Lemma 6.1** (Guralnick, Larsen, Tiep)**.** *There exists a $\mu > 0$ such that whenever $G$ is a classical simple group and $g \in G$ satisfies $|C_G(g)| \leq |G|^{\mu}$, then $|\chi(g)| \leq \chi(1)^{1/10}$ for every $\chi \in \mathrm{Irr}(G)$.*

Let $\zeta^H(t) = \sum_{\chi \in \mathrm{Irr}(H)} \chi(1)^{-t}$ for any finite group $H$. A special case of [15, Theorem 1.1] is the following.

**Lemma 6.2** (Liebeck, Shalev)**.** *For any sequence of non-abelian finite simple groups $H \neq \mathrm{PSL}(2, q)$ and any $t > 2/3$, $\zeta^H(t) \to 1$ as $|H| \to \infty$.*

Let $D_1$, $D_2$, $D_3$ be conjugacy classes of $G$ each of size at least $|G|^{1-\mu}$ where $\mu$ is as in Lemma 6.1.

**Lemma 6.3.** *We have $D_3 \subseteq D_1 D_2$ for every sufficiently large $n$.*

*Proof.* Let $d_1 \in D_1$, $d_2 \in D_2$, and $d_3 \in D_3$. The conjugacy class $D_3$ is contained in the normal set $D_1 D_2$ if and only if the non-negative rational number

$$f(D_1, D_2, D_3) := \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(d_1)\chi(d_2)\chi(d_3^{-1})}{\chi(1)} = 1 + \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \frac{\chi(d_1)\chi(d_2)\chi(d_3^{-1})}{\chi(1)}$$

is positive, by [1, p. 43].

Let $g \in D_1 \cup D_2 \cup D_3$ be arbitrary. We have $|C_G(g)| \leq |G|^{\mu}$. Thus $|\chi(g)| \leq \chi(1)^{1/10}$ for every $\chi \in \mathrm{Irr}(G)$ by Lemma 6.1.

It follows that

$$\Big| \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \frac{\chi(d_1)\chi(d_2)\chi(d_3^{-1})}{\chi(1)} \Big| \leq \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \Big| \frac{\chi(d_1)\chi(d_2)\chi(d_3^{-1})}{\chi(1)} \Big| =$$

$$= \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(d_1)||\chi(d_2)||\chi(d_3^{-1})|}{\chi(1)} \leq \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \chi(1)^{-7/10} = \zeta^G(7/10) - 1.$$

We have $\zeta^G(7/10) - 1 \to 0$ as $n \to \infty$, by Lemma 6.2. Thus $f(D_1, D_2, D_3) > 0$, provided that $n$ is sufficiently large. $\square$

Choose $\gamma > 0$ (and thus $\alpha$) such that $0 < 1 - \mu \leq \gamma < \alpha < 1$ where $\mu > 0$ is a constant whose existence is assured by Lemma 6.1.

The following lemma finishes the proof of Theorem 1.3.

**Lemma 6.4.** *We have $S_1 S_2 S_3 = G$ for every sufficiently large $n$.*

*Proof.* Let $n$ be sufficiently large.

By Lemma 4.3 we may assume that $S_1$, $S_2$ and $S_3$ are conjugacy classes of size at least $|G|^\alpha$. The normal set $S_1 S_2$ contains every conjugacy class of $G$ of size at least $|G|^\gamma$ by Lemma 6.3. Thus

$$|S_1 S_2| \geq |G| - k(G)|G|^\gamma \geq |G| - q^{dn}|G|^\gamma$$

by Lemma 4.1. Observe that there is an absolute positive constant $e$ such that $|G| > q^{en^2}$. Since $n$ is sufficiently large, $|G|^{\alpha - \gamma} > q^{dn}$. It follows that

$$|S_1 S_2| + |S_3| \geq |G| - q^{dn}|G|^\gamma + |G|^\alpha > |G|.$$

Now, Lemma 3.1 gives $(S_1 S_2)S_3 = G$. $\qquad\qquad\square$

This also completes the proof of Theorem 1.2.

## References

[1] Z. Arad, M. Herzog, J. Stavi, Powers and products of conjugacy classes in groups. Products of conjugacy classes in groups, 6–51, Lecture Notes in Math., 1112, Springer, Berlin, 1985.

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

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

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

[5] N. Gill, L. Pyber, 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.

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

[7] R. M. Guralnick, M. Larsen, P. H. Tiep, Character levels and character bounds. II. ArXiv:1904.08070v2.

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

[9] N. Jacobson, Basic algebra. I. Second edition. W. H. Freeman and Company, New York, 1985.

[10] L. G. Kovács, G. R. Robinson, On the number of conjugacy classes of a finite group. *J. Algebra* **160** (1993), no. 2, 441–460.

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

[12] M. Larsen, A. Shalev, P. H. Tiep, Products of normal subsets and derangements. ArXiv:2003.12882.

[13] M. W. Liebeck, L. Pyber, Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra* **198** (1997), no. 2, 538–562.

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

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

[16] G. Malle, J. Saxl, T. Weigel, Generation of classical groups. *Geom. Dedicata* **49** (1994), no. 1, 85–116.

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

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

[19] D. M. Rodgers, Generating and covering the alternating or symmetric group. *Comm. Algebra* **30** (2002), no. 1, 425–435.

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

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

[22] Xu Cheng-hao, The commutators of the alternating group. *Sci. Sinica* **14** (1965), 339–342.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, REÁLTANODA UTCA 13-15, H-1053, BUDAPEST, HUNGARY

*Email address*: `maroti.attila@renyi.mta.hu`

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, REÁLTANODA UTCA 13-15, H-1053, BUDAPEST, HUNGARY

*Email address*: `pyber.laszlo@renyi.mta.hu`