A generalization of a theorem of Rodgers and Saxl for simple groups of bounded rank

Bull. London Math. Soc. 52 (2020) 464–471 doi:10.1112/blms.12338

A generalization of a theorem of Rodgers and Saxl for simple groups of bounded rank

N. Gill, L. Pyber and E. Szabó

Abstract

We prove that if G is a finite simple group of Lie type and $S_1, \ldots, S_k$ are subsets of G satisfying $\prod_{i=1}^{k} |S_i| \geqslant |G|^c$ for some c depending only on the rank of G, then there exist elements $g_1, \ldots, g_k$ such that $G = (S_1)^{g_1} \cdots (S_k)^{g_k}$. This theorem generalizes an earlier theorem of the authors and Short.

We also propose two conjectures that relate our result to one of Rodgers and Saxl pertaining to conjugacy classes in $\mathrm{SL}_n(q)$, as well as to the Product Decomposition Conjecture of Liebeck, Nikolov and Shalev.

1. *Introduction*

This note is inspired by two earlier results. One of them is the following theorem of Rodgers and Saxl [13]:

Theorem 1. *Suppose that $\mathcal{C}_1, \ldots, \mathcal{C}_k$ are conjugacy classes in $\mathrm{SL}_n(q)$ such that $\prod_{i=1}^{k} |\mathcal{C}_i| \geqslant |\mathrm{SL}_n(q)|^{12}$. Then $\prod_{i=1}^{k} \mathcal{C}_i = \mathrm{SL}_n(q)$.*

The other is a result of Gill, Pyber, Short and Szabó [2]:

Theorem 2. *Fix a positive integer r. There exists a constant $c = c(r)$ such that if G is a finite simple group of Lie type of rank r and S is a subset of G of size at least two, then G is a product of N conjugates of S for some $N \leqslant c \log |G| / \log |S|$.*

Our main result is a generalization of Theorem 2 in the spirit of Rodgers and Saxl:

Theorem 3. *Let $G = G_r(q)$ be a finite simple group of Lie type of rank r. There exists $c = f(r)$ such that if $S_1, \ldots, S_k$ are subsets of G satisfying $\prod_{i=1}^{k} |S_i| \geqslant |G|^c$, then there exist elements $g_1, \ldots, g_k$ such that $G = (S_1)^{g_1} \cdots (S_k)^{g_k}$.*

Theorem 3 differs to that of Rodgers and Saxl in three important respects, two good, one not so good: First, our result pertains to all finite simple groups G of Lie type. Second, our result does not just pertain to conjugacy classes, but to subsets of the group, provided we are free to take conjugates.

Received 29 January 2019; revised 23 January 2020; published online 21 May 2020.

2010 *Mathematics Subject Classification* 20D06, 20D40 (primary), 20E45 (secondary).

N. Gill was supported by EPSRC Grant EP/N010957/1. L. Pyber and E. Szabó were supported by the National Research, Development and Innovation Office (NKFIH) Grant K115799. E. Szabó was also supported by the NKFIH Grant K120697. 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 No 741420).

The third difference is a weak point: our result replaces the constant '12' in Theorem 1 with an unspecified constant that depends on the rank of the group G. We conjecture that we should be able to do better, and not just for finite simple groups of Lie type, but for alternating groups as well:

Conjecture 1. Let G be a non-abelian finite simple group. There exists c such that if $S_1, \dots, S_k$ are subsets of G satisfying $\prod_{i=1}^k |S_i| \geqslant |G|^c$, then there exist elements $g_1, \dots, g_k$ such that $G = (S_1)^{g_1} \cdots (S_k)^{g_k}$.

Conjecture 1 seems out of reach at the moment. Indeed, it is a significant generalization of a conjecture that already exists in the literature — the Product Decomposition Conjecture of Liebeck, Nikolov and Shalev [**8**] — and which already appears to be very challenging.

In light of the undoubted difficulty of proving Conjecture 1, we propose a second, weaker conjecture. A proof of this conjecture, as well as being of interest in its own right, would represent a significant staging post in the pursuit of a proof of Conjecture 1.

Conjecture 2. Let G be a non-abelian finite simple group. There exists c such that if $S_1, \dots, S_k$ are normal subsets of G satisfying $\prod_{i=1}^k |S_i| \geqslant |G|^c$, then $G = S_1 \cdots S_k$.

Note that S is a *normal* subset of the group G if it is invariant under conjugation by elements of G; in other words, S is a union of conjugacy classes of G. Conjecture 2 is a generalization of an important theorem of Liebeck and Shalev [**9**].

1.1. *Structure of the paper*

In § 2 we give the necessary background results used to prove Theorem 3. In §§ 3, 4 and 5, we give partial results towards a proof of Theorem 3, depending on the size of the sets $S_1, \dots, S_k$: we use different techniques if these sets are 'small', 'medium-sized' or 'large'. Finally, in § 6 we prove Theorem 3.

2. *Necessary background*

We will use a theorem of Petridis [**11**, Theorem 1.7]:

Theorem 4. *Let A and B be finite sets in a group G. Suppose that*

(1) $|AB| \leqslant \alpha |A|$;
(2) $|AbB| \leqslant \beta |A|$ *for all* $b \in B$;
(3) $|A| \leqslant \gamma |B|$.

Then there exists $S \subseteq A$ such that for all $h > 1$,

$$|SB^h| \leqslant \alpha^{8h-9} \beta^{h-1} \gamma^{4h-5} |S|,$$

where B^h denotes the product of h copies of B.

From here on G is a finite group. Let minclass(G) denote the size of the smallest non-trivial conjugacy class in G, and let mindeg(G) denote the dimension of the smallest non-trivial complex irreducible representation of G.

As observed in [**10**], a result of Gowers [**3**] implies the following.

Proposition 2.1. *Let G be a finite group and let $k = \mathrm{mindeg}(G)$. Take $A, B, C \subseteq G$ such that $|A| \cdot |B| \cdot |C| \geqslant \frac{|G|^3}{k}$. Then $G = ABC$.*

The following two results give useful facts about simple groups of Lie type. Note that, if we write $G_r(q)$ for a simple group of Lie type of rank r over $\mathbb{F}_q$, then there are multiple conventions for the definition of r and the definition of q. We have stated the following results very conservatively — they are valid for whichever standard definition of these two parameters one cares to take (and this also explains the difference in the statement of the first, from that which appears in [2]).

The first result follows for the classical groups from [6, Table 5.2.A] for the classical results (taking into account the corrections listed in [18]), and for the exceptional groups from [15–17].

The second result is proved using the lower bounds on projective representations given by Landazuri and Seitz [7] (taking into account the corrections listed in [6, Table 5.3.A]).

Proposition 2.2. *Let $G = G_r(q)$ be a simple group of Lie type of rank r over $\mathbb{F}_q$, the finite field of order q. We have $q^{r/2} \leqslant \mathrm{minclass}(G) < |G| \leqslant q^{8r^2}$.*

Proposition 2.3. *Let $G = G_r(q)$ be a simple group of Lie type of rank r over $\mathbb{F}_q$, the finite field of order q. Let $k = \mathrm{mindeg}(G)$. Then $|G| < k^{8r^2}$.*

Note that Propositions 2.1 and 2.3 imply that if A, B, C are subsets of $G = G_r(q)$ with $|A|, |B|, |C| > |G|^{1-\frac{1}{24r^2}}$, then $G = ABC$.

The next result was obtained independently in [4, 14]. The subsequent corollary is an easy consequence, and can be found in [2]. Note that, by the *translate* of a set S in a group G, we mean a set of form $Sg := \{sg \mid s \in S\}$ where g is some element of G.

Proposition 2.4. *Each finite simple group G is $\frac{3}{2}$-generated; that is, for any non-trivial element g of G there exists h in G such that $\langle g, h\rangle = G$.*

Corollary 2.5. *Let G be a finite simple group and let S be a subset of G of size at least two. Then some translate of S generates G.*

Finally, we need the Product Theorem, proved independently in [1] and [12].

Theorem 5. *Fix a positive integer r. There exists a positive constant $\eta = \eta(r)$ such that, for G a finite simple group of Lie type of rank r and S a generating set of G, either $S^3 = G$ or $|S^3| \geqslant |S|^{1+\eta}$.*

3. *Medium-sized sets*

Lemma 3.1. *Fix $r > 0$. There exists $\varepsilon > 0$ such that if A and B are subsets of $G = G_r(q)$, a finite simple group of Lie type of rank r, with $2 \leqslant |B| \leqslant |A|$, then one of the following holds.*

(1) $|A| \geqslant |B|^{1+\varepsilon}$.
(2) *There exists $g \in G$ such that $|A \cdot B^g| \geqslant |A| \cdot |B|^{\varepsilon}$.*
(3) $|A| \geqslant |G|^{1/26} \cdot |B|^{25/26}$.
(4) *There exists $g \in G$ such that $|A \cdot B^g| \geqslant |G|^{1/25} \cdot |A|^{24/25}$.*

Proof. Appealing to Corollary 2.5, let $B_0 = Bx$ be a translate of B that generates G. Define $\gamma = |A|/|B|$, $\alpha = |AB|/|A|$ and $\beta = \max\{|A \cdot B^{b^{-1}}|/|A| \mid b \in B\}$. We apply Theorem 4 with $h = 3$ to obtain that there exists $S \subset A$ such that

$$|S \cdot B_0^3| \leqslant \alpha^{15}\beta^2\gamma^7|S|.$$

This implies in particular that

$$|B_0^3| \leqslant \alpha^{15}\beta^2\gamma^7|A|. \tag{1}$$

Now, since B_0 generates G, Theorem 5 gives two possibilities for B_0^3.

First, suppose $|B_0^3| \geqslant |B|^{1+\eta}$. We obtain that

$$|B|^\eta \leqslant \alpha^{15}\beta^2\gamma^8.$$

We conclude that at least one of α, β or γ is greater than or equal to $|B|^{\eta/25}$, and this implies that either $|A| \geqslant |B|^{1+\eta/25}$, or else there exists $g \in G$ such that $|A \cdot B^g| \geqslant |A| \cdot |B|^{\eta/25}$. Taking $\varepsilon = \eta/25$, we obtain one of the first two listed possibilities.

The second possibility is that $B_0^3 = G$. Now (1) implies

$$|G| \leqslant \alpha^{15}\beta^2\gamma^7|A|.$$

We conclude that at least one of α, β or γ is greater than or equal to $(|G|/|A|)^{1/25}$, and some simple rearranging yields the final two listed possibilities. □

Lemma 3.2. *Fix $r > 0$ and $0 < \delta < 1$. There exists $\eta = f(r, \delta) > 0$ such that if A and B are subsets of $G = G_r(q)$, a finite simple group of Lie type of rank r, with $2 \leqslant |B| \leqslant |A|$, then one of the following holds.*

(1) $|A| \geqslant |B|^{1+\eta}$.
(2) *There exists $g \in G$ such that $|A \cdot B^g| \geqslant |A| \cdot |B|^\eta$ and there exists $h \in G$ such that $|B^h \cdot A| \geqslant |A| \cdot |B|^\eta$;*
(3) $|B| \geqslant |G|^\delta$.

Proof. Let ε be the positive number whose existence is guaranteed by Lemma 3.1. Define $\eta = \min\{\frac{1-\delta}{26\delta}, \varepsilon\}$. Then $\delta \leqslant \frac{1}{1+26\eta}$, and we apply Lemma 3.1. If the third option of that lemma holds, then we obtain that either $|A| \geqslant |B|^{1+\eta}$ or else

$$|G|^{1/26} \cdot |B|^{25/26} < |B|^{1+\eta}$$

and, rearranging, we get that $|B| \geqslant |G|^{\frac{1}{1+26\eta}} \geqslant |G|^\delta$, as required.

Similarly, if the fourth option of Lemma 3.1 holds, then we obtain that either $|A \cdot B^g| \geqslant |A| \cdot |B|^\eta$ or else

$$|G|^{1/25}|A|^{24/25} < |A| \cdot |B|^\eta,$$

in which case we obtain that $|G| < |A| \cdot |B|^{25\eta}$. Then either $|A| \geqslant |B|^{1+\eta}$ (and so (1) holds), or else we obtain that $|G| < |B|^{1+26\eta}$ and we obtain (3) as before.

If the first option of Lemma 3.1 holds, then the first option holds here. Finally, suppose that the second option of Lemma 3.1 holds. We obtain immediately that the first part of option (2) holds here. To see that the second part holds, observe that

$$|B^h \cdot A| = |A^{-1} \cdot (B^{-1})^h|.$$

Now we can apply Lemma 3.1 to the two sets A^{-1} and B^{-1}. If the first, third or fourth option holds, then the argument given above implies that the item (1) or (3) holds here for A^{-1} and B^{-1}, hence also for A and B. On the other hand, if the second option holds, then we obtain the second part of item (2) here, and we are done. □

Lemma 3.3. *Fix $0 < \zeta < \delta < 1$ and r a positive integer. Then there exists $c = f(\zeta, \delta, r) > 0$ such that if $S_1, \ldots, S_t \subset G$, where*

(1) *G is a finite simple group of Lie type of rank r;*
(2) $|S_i| \geqslant |G|^\zeta$;
(3) $\prod_{i=1}^t |S_i| \geqslant |G|^c$;

then there exist elements $g_1, \ldots, g_t \in G$ and positive integers k_1, k_2, k_3 such that $t = k_1 + k_2 + k_3$ and

$$\min\{|T_1|, |T_2|, |T_3|\} \geqslant |G|^\delta$$

where $T_1 = S_1^{g_1} \cdots S_{k_1}^{g_{k_1}}$, $T_2 = S_{k_1+1}^{g_{k_1+1}} \cdots S_{k_1+k_2}^{g_{k_1+k_2}}$ and $T_3 = S_{k_1+k_2+1}^{g_{k_1+k_2+1}} \cdots S_t^{g_t}$.

Note that no attempt is made in the subsequent proof to optimize c.

Proof. Let $\eta = f(r, \delta)$ be the constant whose existence is guaranteed by Lemma 3.2. Let $S_1, \ldots, S_t$ be subsets of G satisfying condition (2).

Let $\kappa = \log|S_i| / \log|G|$, where S_i is the smallest set in $S_1, \ldots, S_t$. By supposition, $\kappa \geqslant \zeta$. We will apply Lemma 3.2 a number of times so as to produce a new family of larger sets $S'_1, \ldots, S'_{\lfloor \frac{t}{2} \rfloor}$: For each even i between 2 and t, let A be the larger of S_i and S_{i-1}, and let B be the smaller. Lemma 3.2 gives three possibilities.

If the first possibility holds, then $|A| \geqslant |G|^{\kappa(1+\eta)}$, and we let $S'_{i/2} = S_{i-1}S_i$. If the second possibility holds and $A = S_{i-1}$, then we choose g so that $|A \cdot B^g|$ is as large as possible, and we set $S'_{i/2} = S_{i-1}S_i^g$; if the second possibility holds and $A = S_i$, then we choose h so that $|B^h \cdot A|$ is as large as possible, and we set $S'_{i/2} = S_{i-1}^h S_i$. Note that in both of these cases we end with $|S'_{i/2}| \geqslant |G|^{\kappa(1+\eta)}$. If the third possibility holds, then $|B| \geqslant |G|^\delta$ and we set $S'_{i/2} = S_{i-1} \cdot S_i$.

Observe that there are $\lfloor t/2 \rfloor \geqslant t/3$ sets in our new family, and that the minimum size of a set in the new family is at least $|G|^{\min\{\kappa(1+\eta), \delta\}}$.

We repeat this process as long as $\kappa < \delta$. We must choose c to ensure that we end with at least three sets in our final family: all of these, by construction, will have size at least $|G|^\delta$, and the result follows. Note first that the minimum size of a set in the family produced after i iterations is at least $|G|^{\zeta(1+\eta)^i}$. Now $\zeta(1+\eta)^i \geqslant \delta$ if and only if

$$i \geqslant I := \frac{\log \delta - \log \zeta}{\log(1+\eta)}.$$

On the other hand, after each iteration, the number of sets diminishes by at most a third, so if we start with at least 3^{I+1} sets, then we will definitely end with at least three sets, as required. To ensure that we start with this number of sets, then we can take $c = 3^{I+1}$, and we are done. □

4. *Large sets*

To deal with large sets, we will use 'the Gowers trick', Proposition 2.1. When combined with our work on medium-sized sets, we obtain the conclusion that we need.

Proposition 4.1. *Fix $0 < \zeta < 1$ and r a positive integer. Then there exists $c = f(r, \zeta) > 0$ such that if $S_1, \ldots, S_t \subset G$, where*

1. *G is a finite simple group of Lie type of rank r;*
2. *$|S_i| \geqslant |G|^\zeta$;*
3. *$\prod_{i=1}^t |S_i| \geqslant |G|^c$;*

then there exist elements $g_1, \ldots, g_t \in G$ such that

$$S_1^{g_1} \cdots S_t^{g_t} = G.$$

Proof. Set $\delta = 1 - \frac{1}{24r^2}$ and apply Lemma 3.3. The resulting three sets T_1, T_2, T_3 satisfy the property that $\min\{|T_1|, |T_2|, |T_3|\} \geqslant |G|^\delta$ and Propositions 2.1 and 2.3 imply that $T_1 \cdot T_2 \cdot T_3 =$

G (see the remark after Proposition 2.3). But, given the definition of the sets T_1, T_2 and T_3, the desired conclusion follows immediately. □

5. *Small sets*

In this section, we use a variant of the 'greedy lemma' argument of [2]. First we need an easy little lemma.

Lemma 5.1. *If A and B are finite subsets of a group G, then*

$$|AB||A^{-1}A \cap BB^{-1}| \geqslant |A||B|.$$

Note that a similar result is stated by Helfgott in [5, Lemma 2.2].

Proof. Let $m = |AB|$. Choose elements $a_1, \dots, a_m$ of A and $b_1, \dots, b_m$ of B such that $AB = \{a_1b_1, \dots, a_mb_m\}$. Let $A^{-1}A \cap BB^{-1} = \{x_1, \dots, x_n\}$. Consider the map

$$\Theta : AB \times (A^{-1}A \cap BB^{-1}) \to G \times G, \qquad (a_ib_i, x_j) \mapsto (a_ix_j^{-1}, x_jb_i).$$

The map Θ is injective, because, given an element $(a_ix_j^{-1}, x_jb_i)$ we can recover the element $a_ib_i = a_ix_j^{-1}x_jb_i$. Since the elements $a_1, \dots, a_m$ and $b_1, \dots, b_m$ are fixed and each element of AB has a unique expression of the form a_kb_k we recover the elements a_i and b_i, along with the element x_j, and injectivity follows. Therefore,

$$|AB||A^{-1}A \cap BB^{-1}| = |AB \times (A^{-1}A \cap BB^{-1})| = |\Theta(AB \times (A^{-1}A \cap BB^{-1}))|.$$

We complete the proof by establishing that $A \times B$ is in the image of Θ. Given (a, b) in $A \times B$ we can choose i such that $ab = a_ib_i$. Therefore, $a^{-1}a_i = bb_i^{-1}$; this element belongs to $A^{-1}A \cap BB^{-1}$, and hence is equal to x_j, for some j. Therefore, $(a, b) = \Theta(a_ib_i, x_j)$, as required. □

Lemma 5.2. *Given subsets A and B of a finite group G, we have*

$$\sum_{C \in \mathcal{C}(G)} \frac{|A \cap C||B \cap C|}{|C|} = \frac{1}{|B^G|} \sum_{B' \in B^G} |A \cap B'|,$$

where $\mathcal{C}(G)$ is the set of conjugacy classes in G, and B^G denotes the set of G-conjugates of B.

Proof. First observe that

$$\sum_{C \in \mathcal{C}(G)} \frac{|A \cap C||B \cap C|}{|C|} = \sum_{C \in \mathcal{C}(G)} \sum_{a \in A \cap C} \frac{|B \cap C|}{|C|} = \sum_{a \in A} \frac{|B \cap a^G|}{|a^G|}.$$

Now,

$$\bigcup_{B' \in B^G} \{(a', B') : a' \in a^G, a' \in B'\} = \bigcup_{a' \in a^G} \{(a', B') : B' \in B^G, a' \in B'\},$$

and comparing cardinalities gives $|B^G||B \cap a^G| = |a^G| \sum_{B' \in B^G} 1_{B'}(a)$ where we define

$$1_{B'}(a) := \begin{cases} 1, & a \in B', \\ 0, & \text{otherwise}. \end{cases}$$

It follows that

$$\sum_{a \in A} \frac{|B \cap a^G|}{|a^G|} = \frac{1}{|B^G|} \sum_{a \in A} \sum_{B' \in B^G} 1_{B'}(a)$$

$$= \frac{1}{|B^G|} \sum_{B' \in B^G} \sum_{a \in A} 1_{B'}(a)$$

$$= \frac{1}{|B^G|} \sum_{B' \in B^G} |A \cap B'|,$$

as required. □

PROPOSITION 5.3. *Suppose A and B are subsets of a finite group G. Suppose, in addition, that $|A|, |B| < (\mathrm{minclass}(G))^{1/4}$. Then there exists $g \in G$ such that $|A \cdot B^g| = |A| \cdot |B|$.*

Proof. Suppose that we cannot find such a g. This implies that, for every B_* conjugate to B, $|AB_*| < |A| \cdot |B|$. Now Lemma 5.1 yields

$$|A| \cdot |B||A^{-1}A \cap B_* B_*^{-1}| > |AB||A^{-1}A \cap B_* B_*^{-1}| \geqslant |A||B|.$$

We obtain that $|A^{-1}A \cap B_* B_*^{-1}| \geqslant 2$. As before, let $\mathcal{C}(G)$ be the set of conjugacy classes in G, and let $\mathcal{C}^*(G)$ be the set of non-trivial conjugacy classes in G. Lemma 5.2 implies

$$\sum_{C \in \mathcal{C}(G)} \frac{|C \cap A^{-1}A| \cdot |C \cap BB^{-1}|}{|C|} = \frac{1}{|(BB^{-1})^G|} \sum_{X \in (BB^{-1})^G} |A^{-1}A \cap X| \geqslant 2$$

$$\Longrightarrow \sum_{C \in \mathcal{C}^*(G)} \frac{|C \cap A^{-1}A| \cdot |C \cap BB^{-1}|}{|C|} + 1 \geqslant 2$$

$$\Longrightarrow \sum_{C \in \mathcal{C}^*(G)} \frac{|C \cap A^{-1}A|}{|C|} \geqslant \frac{1}{|BB^{-1}|}.$$

In particular, we obtain that $|A^{-1}A| \geqslant \min_{C \in \mathcal{C}^*(G)} \frac{|C|}{|BB^{-1}|}$. Now, since $|A^{-1}A| \leqslant |A|^2$ and $|BB^{-1}| \leqslant |B|^2$, the result follows. □

6. *A proof of Theorem* 3

Proof of Theorem 3. Let $\zeta = \frac{1}{32r}$, and note that Proposition 2.2 implies $|G|^\zeta < (\mathrm{minclass}(G))^{1/4}$. Let c_0 be the constant whose existence is guaranteed by Proposition 4.1. We define $c = 2c_0 + \zeta$; observe that, since ζ depends only on r, c also depends only on r.

Suppose, first of all, that there exists i such that $|S_i|, |S_{i+1}| \leqslant |G|^\zeta$. Then Proposition 5.3 implies that there exists g such that $|S_i \cdot S_{i+1}^g| = |S_i| \cdot |S_{i+1}|$. Thus, we replace S_i and S_{i+1} with this product; this does not affect the ordering of the sets, nor does it affect the product of the cardinalities of the sets. We repeat this process until there are no 'adjacent' sets of cardinality less than $|G|^\zeta$.

If k is even, then, for every even i between 1 and k we replace S_{i-1} and S_i by the product of the two. This results in a family of sets with the same ordering, all of which have order at least $|G|^\zeta$, and for which the product of cardinalities is at least $|G|^{c_0+\zeta/2}$. Now Proposition 4.1 implies the result.

If k is odd and $|S_k| \geqslant |G|^\zeta$, then, for every even i between 1 and k, we replace S_{i-1} and S_i by the product of the two and we retain S_k. We obtain a family with the same properties as in the previous paragraph and, once again, Proposition 4.1 implies the result.

If k is odd and $|S_k| < |G|^\zeta$, then for every even i between 1 and $k-3$ we replace S_{i-1} and S_i by the product of the two; we also replace S_{k-2}, S_{k-1} and S_k by the product of the three. This results in a family of sets with the same ordering, all of which have order at least $|G|^\zeta$, and for which the product of cardinalities is at least $|G|^{c_0}$. Now Proposition 4.1 implies the result and we are done. □

References

1. E. Breuillard, B. Green and T. Tao, 'Approximate subgroups of linear groups', *Geom. Funct. Anal.* 21 (2011) 774–819.

2. N. Gill, L. Pyber, I. Short and E. Szabó, 'On the product decomposition conjecture for finite simple groups', *Groups Geom. Dyn.* 7 (2013) 867–882.

3. W. T. Gowers, 'Quasirandom groups', *Combin. Probab. Comput.* 17 (2008) 363–387.

4. R. M. Guralnick and W. M. Kantor, 'Probabilistic generation of finite simple groups', *J. Algebra* 234 (2000) 743–792. (Special issue in honor of Helmut Wielandt.)

5. H. Helfgott, 'Growth in linear algebraic groups and permutation groups: Towards a unified perspective', *Groups St Andrews* 2017 *in Birmingham*, London Mathematical Society Lecture Note Series (eds C. Campbell, C. Parker, M. Quick, E. Robertson and C. Roney-Dougal; Cambridge University Press, Cambridge, 2019) 300–345.

6. P. B. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series 129 (Cambridge University Press, Cambridge, 1990).

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

8. M. W. Liebeck, N. Nikolov and A. Shalev, 'Product decompositions in finite simple groups', *Bull. Lond. Math. Soc.* 44 (2012) 469–472.

9. M. W. Liebeck and A. Shalev, 'Diameters of finite simple groups: sharp bounds and applications', *Ann. of Math.* (2) 154 (2001) 383–406.

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

11. G. Petridis, 'New proofs of Plünnecke-type estimates for product sets in groups', *Combinatorica* 32 (2012) 721–733.

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

13. D. M. Rodgers and J. Saxl, 'Products of conjugacy classes in the special linear groups', *Comm. Algebra* 31 (2003) 4623–4638.

14. A. Stein, '$1\frac{1}{2}$-generation of finite simple groups', *Beitr. Algebra Geom.* 39 (1998) 349–358.

15. A. V. Vasil'ev, 'Minimal permutation representations of finite simple exceptional groups of types G_2 and F_4', *Algebra Logika* 35 (1996) 663–684.

16. A. V. Vasil'ev, 'Minimal permutation representations of finite simple exceptional groups of types E_6, E_7, and E_8', *Algebra Logika* 36 (1997) 518–530.

17. A. V. Vasil'ev, 'Minimal permutation representations of finite simple exceptional twisted groups', *Algebra Logika* 37 (1998) 17–35.

18. A. V. Vasil'ev and V. D. Mazurov, 'Minimal permutation representations of finite simple orthogonal groups', *Algebra Logic* 33 (1994) 337–350.

N. Gill
Department of Mathematics
University of South Wales
Treforest, CF37 1DL
United Kingdom

nick.gill@southwales.ac.uk

L. Pyber and E. Szabó
A. Rényi Institute of Mathematics
Hungarian Academy of Sciences
P.O. Box 127
Budapest H-1364
Hungary

pyber@renyi.hu
endre@renyi.hu