

The diameter of products of finite simple groups

Daniele Dona * 

*Einstein Institute of Mathematics, Edmond J. Safra Campus Givat Ram,
The Hebrew University of Jerusalem, 9190401 Jerusalem, Israel*

Received 27 April 2021, accepted 14 January 2022, published online 11 August 2022

Abstract

Following partially a suggestion by Pyber, we prove that the diameter of a product of non-abelian finite simple groups is bounded linearly by the maximum diameter of its factors. For completeness, we include the case of abelian factors and give explicit constants in all bounds.

Keywords: Finite simple groups, diameter.

Math. Subj. Class. (2020): 20F69, 20D06

1 Introduction

An important area of research in finite group theory in the last decades has been the production of upper bounds for the diameter of Cayley graphs of such groups. For any finite group G , the maximum diameter over all Cayley graphs defined by *symmetric* sets of generators of G (i.e. sets S with $S = S^{-1}$ and $e \in S$) is called the *diameter* of G . Arguably the best known conjecture in the area is Babai's conjecture [1]: every non-abelian finite simple group G has diameter $\leq \log^k |G|$, where k is an absolute constant; the conjecture is still open, despite great progress towards a solution both for alternating groups and for groups of Lie type.

A more modest question is that of producing bounds for the diameter of direct products of finite simple groups, depending on the diameter of their factors. This is not an idle question, for bounds of this sort have been used more than once as intermediate steps towards the proof of bounds for simple groups themselves: Babai and Seress have done so in [2, Lemma 5.4], as well as Helfgott more than two decades later in [5, Lemma 4.13]. We improve on both results in the following theorem, which also features explicit constants.

*The author was partially supported by the European Research Council under Programme H2020-EU.1.1., ERC Grant ID: 648329 (codename GRANT). He was also supported by the Israel Science Foundation Grant No. 686/17 of A. Shalev, and by the Emily Erskine Endowment Fund.

E-mail address: daniele.dona@mail.huji.ac.il (Daniele Dona)

Theorem 1.1. *Let $n \geq 2$. Let $G = \prod_{i=1}^n T_i$, where the T_i are finite simple groups.*

- (a) *If the T_i are all abelian (say $G = \prod_{j=1}^s (\mathbb{Z}/p_j\mathbb{Z})^{e_j}$, where the p_j are distinct primes and $e_j \geq 1$), then:*

$$\text{diam}(G) < \frac{2}{3} \max\{e_j \mid 1 \leq j \leq s\} \prod_{j=1}^s p_j.$$

- (b) *If the T_i are all non-abelian, call $d = \max\{\text{diam}(T_i) \mid 1 \leq i \leq n\}$; then:*

$$\text{diam}(G) < \frac{196}{243} n^3 \max\{C_A, C_L, C_S\} (4d + 1) + d,$$

where:

$$C_A = \begin{cases} \max\{3, \lfloor \frac{m}{2} \rfloor\} & \text{if there are alternating groups among the } T_i \\ & \text{and where } m \text{ is their maximum degree,} \\ 0 & \text{if there are no alternating groups among the } T_i, \end{cases}$$

$$C_L = \begin{cases} 8(5r + 7) & \text{if there are groups of Lie type among the } T_i \\ & \text{and where } r \text{ is their maximum untwisted rank,} \\ 0 & \text{if there are no groups of Lie type among the } T_i, \end{cases}$$

$$C_S = \begin{cases} 6 & \text{if there are sporadic or Tits groups among the } T_i, \\ 0 & \text{if there are no sporadic or Tits groups among the } T_i. \end{cases}$$

- (c) *If there are abelian and non-abelian T_i , write $G = G_A \times G_{NA}$, where G_A collects the abelian factors and G_{NA} collects the non-abelian ones; then:*

$$\text{diam}(G) \leq d_A + 4d_{NA},$$

where $d_A = \text{diam}(G_A)$, $d_{NA} = \text{diam}(G_{NA})$.

The result of part (a) is known and elementary: see [2, Lemma 5.2], where the constant is marginally worse only due to the fact that sets of generators are not required to be symmetric (cfr. also [5, Lemma 4.14], which treats the case of $G = (\mathbb{Z}/p\mathbb{Z})^e$ under this assumption). Part (c) is quite natural, given the different (in some sense, opposite) behaviour of abelian and non-abelian factors, as it can be readily observed in its short proof.

Part (b) is where the novelty of the result resides. Dependence on the maximum of the diameter of the components, instead of dependence on their product as Schreier’s lemma (see Lemma 2.1) would naturally give us, was already established in [2, Lemma 5.4]: in that case, the diameter was bounded as $O(d^2)$, where the dependence of the constant on n was polynomial as in our statement. This result was improved in [5, Lemma 4.13] to $O(d)$, but only in the case of alternating groups: this was done in part to fix a mistake in the use of the previously available result in Babai-Seress, which is why only alternating groups were considered, as permutation subgroups were the sole concern in both papers; a suggestion by Pyber, reported in Helfgott’s paper, points at the results by Liebeck and Shalev [8] as a way to prove a bound of $O(d)$ for a product of arbitrary non-abelian finite simple groups.

Indeed, the general approach that we follow in our proof owes its validity to [8, Theorem 1.6], although we do not explicitly use the statement of that theorem: rather, we closely follow the proof of [5, Lemma 4.13] and show that the same reasoning applies to groups of Lie type as well. The way that the lemma is related to Liebeck-Shalev is through the use of the fact that every element in $\text{Alt}(m)$ is a commutator ([5, Lemma 4.12], first proved in [9, Theorem I]), which is essentially [8, Theorem 1.6] with $w = xyx^{-1}y^{-1}$ and a c that is just equal to 1 for $\text{Alt}(m)$; the same can be said for all non-abelian finite simple groups (i.e., $c = 1$ in general) since Ore’s conjecture [10] was established to be true in [7], a fact yet unproved at the time of [8].

2 Preliminaries

Before we turn to the proof of Theorem 1.1, we will need a certain number of group-theoretic results.

Lemma 2.1 (Schreier’s Lemma). *Let G be a finite group, let $N \trianglelefteq G$, and let S be a set of generators of G with $e \in S = S^{-1}$. Then $S^{2d+1} \cap N$ generates N , where $d = \text{diam}(G/N)$.*

Proof. This is a standard result dating back to Schreier [11], written in various fashions across the literature according to the needs of the user; let us prove here the present version.

Calling $\pi: G \rightarrow G/N$ the natural projection, by definition we have $\pi(S)^d = G/N$; this equality means that S^d contains at least one representative for each coset gN in G . For any coset gN , choose a representative $\tau(g) \in S^d$. Then, for any $h \in N$ and any way to write h as a product of elements $s_i \in S$, we have:

$$\begin{aligned} h &= s_1 s_2 \dots s_k \\ &= (s_1 \tau(s_1)^{-1}) \cdot (\tau(s_1) s_2 \tau(\tau(s_1) s_2)^{-1}) \cdots (\tau(\tau(\tau(\dots) s_{k-2}) s_{k-1}) s_k). \end{aligned}$$

Each element of the form $\tau(x) s_i \tau(\tau(x) s_i)^{-1}$ is contained in $S^{2d+1} \cap N$, so the same can be said about the last element of the form $\tau(x) s_k$ (since h itself is in N); therefore $S^{2d+1} \cap N$ is a generating set of N . □

Proposition 2.2 (Ore’s Conjecture). *Let G be a finite non-abelian simple group. Then, for any $g \in G$, there exist $g_1, g_2 \in G$ such that $g = [g_1, g_2]$.*

Proof. See [7], for references to previously known results and for the proof of the final case. □

Notice that, for any finite non-abelian simple group G , any nontrivial conjugacy class C must generate the whole G (because $\langle C \rangle$ would be a normal subgroup). This observation justifies the following definition.

Definition 2.3. Let G be a finite non-abelian simple group. The conjugacy diameter $\text{cd}(G)$ is the smallest m such that $(C \cup C^{-1} \cup \{e\})^m = G$ for all nontrivial conjugacy classes C .

We will need to have bounds for $\text{cd}(G)$.

Proposition 2.4. *Let G be a finite non-abelian simple group.*

- (a) *If G is an alternating group of degree m , then $\text{cd}(G) \leq \max \{3, \lfloor \frac{m}{2} \rfloor\}$.*
- (b) *If G is a group of Lie type of untwisted rank r , then $\text{cd}(G) \leq 8(5r + 7)$.*

(c) If G is a sporadic group or the Tits group, then $\text{cd}(G) \leq 6$.

Proof. First of all, $\text{cd}(G)$ is trivially bounded by definition by the covering number of G , which is defined as $\text{cn}(G) = \min\{m \mid \forall C \neq \{e\} (C^m = G)\}$; therefore it suffices to give bounds for $\text{cn}(G)$.

For (a), see [4, Theorem 9.1] (our specific result is credited therein to a manuscript by J. Stavi). For (b), see [6, Theorem 1]. To prove (c), the sporadic groups all satisfy $\text{cn}(G) \leq 6$: this inequality can be checked directly from [13, Table 1]; if $G = {}^2F_4(2)'$ is the Tits group, we can show the same inequality using [13, Lemma 3] and the character values reported in the ATLAS of Finite Groups [3]. □

Let us also perform a side computation separately from the proof of the main theorem, so as not to bog down the exposition there.

Lemma 2.5. *Let $n \geq 2$. Then:*

$$\sum_{i=1}^{n-1} 4^{\lceil \log_2 i \rceil} < \frac{196}{243} n^3.$$

Proof. Call $m = \lceil \log_2(n - 1) \rceil$, and write $n - 1 = 2^{m-1} + l$, where $1 \leq l \leq 2^{m-1}$; $\lceil \log_2 i \rceil = j$ for all $i \in (2^{j-1}, 2^j]$, hence we can rewrite the sum in the statement as:

$$\begin{aligned} \sum_{i=1}^{n-1} 4^{\lceil \log_2 i \rceil} &= 1 + \sum_{j=1}^{m-1} 4^j 2^{j-1} + 4^m l = \frac{1}{2} + \frac{1}{2} \frac{8^m - 1}{7} + 4^m (2^{\log_2(n-1)} - 2^{m-1}) \\ &= \frac{3}{7} + 4^m 2^{\log_2(n-1)} - \frac{3}{7} 8^m = \frac{3}{7} + 2^{2m'} \left(1 - \frac{3}{7} 2^{m'}\right) (n-1)^3, \end{aligned}$$

where $m' = m - \log_2(n - 1) \in [0, 1)$. We have $x^2 (1 - \frac{3}{7}x) \leq \frac{196}{243}$ for $x \in [1, 2)$, and $\frac{3}{7} < \frac{196}{243}(3n^2 - 3n + 1)$ for all $n \geq 2$, so the result is proved. □

3 Proof of the main theorem

Proof of Theorem 1.1(a). Let $G = (\mathbb{Z}/p_1\mathbb{Z})^{e_1} \times (\mathbb{Z}/p_2\mathbb{Z})^{e_2} \times \dots \times (\mathbb{Z}/p_s\mathbb{Z})^{e_s}$, with primes $p_1 < p_2 < \dots < p_s$; we have:

$$G = A_1 A_2 \dots A_s \tag{3.1}$$

(we are using multiplicative notation even if G is abelian) where the A_i are any sets such that:

$$A_{i,i} = (\mathbb{Z}/p_i\mathbb{Z})^{e_i} \qquad A_{i,j} = (0)^{e_j} \quad (\forall j < i) \tag{3.2}$$

where $A_{i,j}$ is the projection of A_i to the j -th component of G .

Let S be a set of generators of G with $e \in S = S^{-1}$: $\{t^{p_1 \dots p_{i-1}} \mid t \in S\} \subseteq S^{p_1 \dots p_{i-1}}$ has elements that are all 0 on the first $i - 1$ components of G and that still generate the i -th one since $(p_1 \dots p_{i-1}, p_i) = 1$; from now on, let us focus exclusively on the i -th component. $(\mathbb{Z}/p_i\mathbb{Z})^{e_i}$ is also a vector space over $\mathbb{Z}/p_i\mathbb{Z}$, so there must be e_i generators that also form a basis: any element of the space can be written as a linear combination of those generators with coefficients in $[-\lfloor \frac{p_i}{2} \rfloor, \lfloor \frac{p_i}{2} \rfloor]$, which corresponds to a word of length $\leq e_i \lfloor \frac{p_i}{2} \rfloor$; thus,

each set A_i with the properties in (3.2) is covered in $e_i \lfloor \frac{p_i}{2} \rfloor p_1 \dots p_{i-1}$ steps. This fact and (3.1) imply that G has diameter bounded by:

$$\sum_{i=1}^s \left(e_i \lfloor \frac{p_i}{2} \rfloor \prod_{j=1}^{i-1} p_j \right) \leq \frac{1}{2} \max\{e_j | 1 \leq j \leq s\} \prod_{j=1}^s p_j \cdot \sum_{i=1}^s \left(\prod_{j=i+1}^s \frac{1}{p_j} \right). \quad (3.3)$$

The sum in (3.3) is maximized when each p_j is the j -th prime number: for $s = 1$ the sum is 1 and for $s = 2$ it is bounded by $\frac{4}{3}$; for $s \geq 3$, we use $p_s \geq 5$ and $p_j \geq 3$ for all $1 < j < s$, so that the sum is bounded by $1 + \frac{1}{5} \frac{1}{1-\frac{1}{3}} = \frac{13}{10}$. The result follows. \square

Proof of Theorem 1.1(b). Calling $G_j = \prod_{i=1}^j T_i$, we have natural projections $\pi_j: G = G_n \rightarrow G_j$ and $\rho_{j_1, j_2}: G_{j_1} \rightarrow T_{j_2}$ for any $j_1 \geq j_2$. As in (3.1), we write G as a product of subsets A_i with $\rho_{n,i}(A_i) = T_i$ and $\rho_{n,j}(A_i) = \{e\}$ for all $j < i$, and our aim is to cover each one of them.

Suppose that we have two subsets X_1, X_2 of G for which $\rho_{n,i}(X_1) = \rho_{n,i}(X_2) = T_i$ for some fixed $i \in \{1, \dots, n\}$ and that have $\rho_{n,j_1}(X_1) = \{e\} = \rho_{n,j_2}(X_2)$ for all $j_1 \in I_1, j_2 \in I_2$, where I_1, I_2 are two subsets of indices in $\{1, \dots, n\} \setminus \{i\}$: then, the set $X = \{[x_1, x_2] | x_1 \in X_1, x_2 \in X_2\}$ has $\rho_{n,i}(X) = T_i$ by Proposition 2.2 (Ore’s conjecture) and $\rho_{n,j}(X) = \{e\}$ for all $j \in I_1 \cup I_2$. Now consider the set of indices $I = \{1, \dots, i-1\}$: if $|I| > 1$ we can partition I into two parts of size $\lfloor \frac{|I|}{2} \rfloor, \lceil \frac{|I|}{2} \rceil$, then partition each part I' with $|I'| > 1$ into two new parts again of size $\lfloor \frac{|I'|}{2} \rfloor, \lceil \frac{|I'|}{2} \rceil$, and continue until we reach a subdivision where all sets have size 1; the tree of partitions that we constructed to reach this subdivision will have exactly $\lceil \log_2 |I| \rceil$ layers. Notice that, given any two parts I_1, I_2 inside the tree, if we have two subsets X_1, X_2 (as described before) that are covered by a certain S^a , the resulting set X will be covered by S^{4a} : this observation, together with the information about the layers, tells us that if we can cover sets $X_{i,j}$ with $\rho_{n,i}(X_{i,j}) = T_i$ and $\rho_{n,j}(X_{i,j}) = \{e\}$ in a steps (for a fixed $i > 1$ and all $j < i$) then we are able to cover a set A_i defined as at the beginning of the proof in $4^{\lceil \log_2(i-1) \rceil} a$ steps as well.

Let us start now with a generating set S with $e \in S = S^{-1}$ and fix two indices $i \geq j$: $\pi_i(S)$ is a set of generators for G_i , and the set $\pi_i(S)^{2d+1}$ contains generators for the whole $T_1 \times \dots \times T_{j-1} \times \{e\} \times T_{j+1} \times \dots \times T_i = G_i \cap \ker(\rho_{i,j})$ by Lemma 2.1 (Schreier’s lemma), where d is as in the statement. In particular, there is an element $x \in S^{2d+1}$ with $\rho_{n,i}(x) \neq e$ and $\rho_{n,j}(x) = e$; by hypothesis $\rho_{n,i}(S^d) = T_i$, which means that there is a set $S' = \{yxy^{-1} | y \in S^d\} \cup \{yx^{-1}y^{-1} | y \in S^d\} \cup \{e\} \subseteq S^{4d+1}$ with $\rho_{n,i}(S') = C \cup C^{-1} \cup \{e\}$ and $\rho_{n,j}(S') = \{e\}$, where C is the conjugacy class of $\rho_{n,i}(x)$. By Proposition 2.4, $\rho_{n,i}(S^{\max\{3, \lfloor \frac{m_i}{2} \rfloor\}}) = T_i$ if $T_i = \text{Alt}(m_i)$, $\rho_{n,i}(S^{8(5r_i+7)}) = T_i$ if T_i is of Lie type of untwisted rank r_i , and $\rho_{n,i}(S'^6) = T_i$ otherwise; in all three cases, the projection to T_j is still $\{e\}$, therefore we managed to cover a set $X_{i,j}$ of the aforementioned form.

A set A_1 is reached in d steps, hence the final count for the whole G following the reasoning above is:

$$\text{diam}(G) \leq d + \sum_{i=2}^n 4^{\lceil \log_2(i-1) \rceil} x_i (4d + 1),$$

where x_i is either $\max\{3, \lfloor \frac{m_i}{2} \rfloor\}$, $8(5r_i + 7)$ or 6, accordingly. The result follows by Lemma 2.5. \square

A note on the connection between the proof given above and [8]. As mentioned before, Pyber pointed at [8] as a way to prove linear dependence on d for products of arbitrary non-abelian finite simple groups. In particular, [8, Theorem 1.6] seems to fit the bill: it states that for any word w that is not a law in a finite simple group T there is $c_w \in \mathbb{N}$, depending on w but not on T , such that any element of T can be written as a product of at most c_w values of w . We use this property, in disguise, when we want to pass from two subsets being indentially e at indices I_1, I_2 and filling an entire component T_i to a third subset that also fills the same component and is e for the whole $I_1 \cup I_2$: the creation of the new subset is made possible by taking c_w values of a word w , so that T_i remains filled, where w has two distinct letters x_1, x_2 and presents the same number of x_i and x_i^{-1} for $i \in \{1, 2\}$, so that when any one x_i is equal to e on a given factor of the product G the result is e on that factor; in our case, w was the shortest nontrivial word with these characteristics, namely the commutator $[x_1, x_2] = x_1x_2x_1^{-1}x_2^{-1}$ (not a law for any non-abelian group), and $c_w = 1$ by Ore’s conjecture. In this sense $w = [x_1, x_2]$ is also computationally the best word we can expect, for it yields the lowest possible value of $|w|c_w$, the 4 that we find in Lemma 2.5.

Proof of Theorem 1.1(c). Define the two projections π_A, π_{NA} in the obvious way; for any generating set S of G , by definition there is a subset $X_A \subseteq S^{d_A}$ with $\pi_A(X_A) = G_A$ and there is a subset $X_{NA} \subseteq S^{d_{NA}}$ with $\pi_{NA}(X_{NA}) = G_{NA}$, and then:

$$G = X_A[X_{NA}, X_{NA}] \subseteq S^{d_A+4d_{NA}},$$

again by the fact that $[T, T] = T$ for non-abelian finite simple groups by Ore’s conjecture and $[T, T] = \{e\}$ for abelian groups. □

4 Concluding remarks

One could wonder how tight the inequalities in Theorem 1.1 are. The results are essentially in line with what is generally expected from the behaviour of the diameter of finite groups. The abelian case is tight up to constant: for the group $G(x) = \prod_{p \leq x} \mathbb{Z}/p\mathbb{Z}$ (nontrivial for $x \geq 2$) one generator $s = (1, 1, \dots, 1)$ is enough, and then the diameter of $\text{Cay}(G(x), \{s, s^{-1}, e\})$ is $\frac{1}{2}|G(x)|$; the fact that abelian groups behave in the worst possible way, i.e. linearly in the size of the group, should not be a surprise for anyone.

The non-abelian bound of case (b) also matches what is anticipated in general. Babai’s conjecture posits a polylogarithmic bound on the diameter of finite simple groups: the natural extension to direct products of such groups would suggest a bound of the form $n^k d$, which is exactly what we have obtained. Case (c) also fits into the same idea, as a product $|G| = |G_A||G_{NA}|$ becomes a sum of the corresponding diameters.

The dependence on d in Theorem 1.1(b) is almost best possible by definition (we cannot drop the “almost”, as m, r are not independent from d). It would be more interesting to understand which power of n is the correct one: here we have proved $O_{m,r,d}(n^3)$, and we can quickly show that the bound is $\Omega_{m,r,d}(n)$, as illustrated in the following example.

Example 4.1. If $G = (\text{Alt}(m))^n$ then $\text{diam}(G) = \Omega(m^2n)$. We prove it for $m \geq 5$ odd and n even, but the proof is analogous for the general case.

Consider the two permutations $\sigma = (1\ 2\ 3\ \dots\ m)$ and $\tau = (1\ 2\ 3\ \dots\ m - 2)$; they

generate $\text{Alt}(m)$, and the elements:

$$\begin{aligned} s_0 &= (\sigma, \sigma, \dots, \sigma, \sigma), \\ s_1 &= (\tau, \sigma, \dots, \sigma, \sigma), \\ s_2 &= (\sigma, \tau, \dots, \sigma, \sigma), \\ &\dots \\ s_n &= (\sigma, \sigma, \dots, \sigma, \tau) \end{aligned}$$

generate G . Let $S = \{e\} \cup \{s_i, s_i^{-1}\}_{0 \leq i \leq n}$: to prove the lower bound on the diameter of G , we construct a function $f: G \rightarrow \mathbb{N}$ such that there are two elements $g_1, g_2 \in G$ with $|f(g_1) - f(g_2)|$ large and such that $|f(g) - f(gs)|$ is small for any $g \in G, s \in S$; this is a known technique to prove lower bounds for the diameter of $\text{Sym}(m)$, as shown for instance in [12, Proposition 3.6].


Call $c(g, i, j) = (g(i))(j)$ the image of $j \in \{1, \dots, m\}$ under the i -th component of $g \in G$, for $1 \leq i \leq n$; define:

$$f(g) = \sum_{j=1}^m \sum_{i=1}^n \|c(g, i+1, j) - c(g, i, j)\|_{\mathbb{Z}/m\mathbb{Z}},$$

where $\|a\|_{\mathbb{Z}/m\mathbb{Z}} = \min\{a, m-a\}$ (in the case $i = n, c(g, n+1, j)$ means $c(g, 1, j)$). First, $f(e) = 0$; also, if we call e_m the identity element in $\text{Alt}(m)$ and $\eta = (1 \frac{m+1}{2}) (2 \frac{m+3}{2}) \dots (\frac{m-1}{2} m-1)$, for $g \in G$ that has e_m at all odd components and η at all even ones we have $f(g) = \frac{1}{2}(m-1)^2n$. Finally, notice that σ simply adds 1 modulo m to all the elements of $\{1, \dots, m\}$, so that $f(g) = f(gs_0^{\pm 1})$, while τ is defined so that it adds 1 for $m-3$ elements, adds 3 (modulo m) for one element and fixes two elements, which means that $|f(g) - f(gs_i^{\pm 1})| \leq 10$; these facts taken together imply that $\text{diam}(G, S) \geq \frac{1}{20}(m-1)^2n$.

The correct (or even expected) order of magnitude for a bound of the form $\text{diam}(G) = O_{m,r}(n^k d)$ for a generic product G is not known to the author, besides knowing that $1 \leq k \leq 3$ by Theorem 1.1 and Example 4.1.

ORCID iDs

Daniele Dona  <https://orcid.org/0000-0001-7966-3357>

References

- [1] L. Babai and A. Seress, On the diameter of Cayley graphs of the symmetric group, *J. Comb. Theory Ser. A* **49** (1988), 175–179, doi:10.1016/0097-3165(88)90033-7.
- [2] L. Babai and A. Seress, On the diameter of permutation groups, *Eur. J. Comb.* **13** (1992), 231–243, doi:10.1016/s0195-6698(05)80029-0.
- [3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Clarendon Press, Oxford (UK), 1985.
- [4] Y. Dvir, Covering properties of permutation groups, in: Z. Arad and M. Herzog (eds.), *Products of Conjugacy Classes in Groups*, Springer-Verlag, Berlin (Germany), pp. 197–221, 1973, doi:10.1007/bfb0072288.

- [5] H. A. Helfgott, Growth in linear algebraic groups and permutation groups: towards a unified perspective, in: C. M. Campbell, C. W. Parker, M. R. Quick, E. F. Robertson and C. M. Roney-Dougal (eds.), *Groups St Andrews 2017 in Birmingham*, Cambridge University Press, Cambridge, volume 455 of *London Mathematical Society Lecture Note Series*, pp. 300–345, 2019.
- [6] R. Lawther and M. W. Liebeck, On the diameter of a Cayley graph of a simple group of Lie type based on a conjugacy class, *J. Combin. Theory Ser. A* **83** (1998), 118–137, doi:10.1006/jcta.1998.2869.
- [7] M. W. Liebeck, E. A. O’Brien, A. Shalev and P. H. Tiep, The Ore conjecture, *J. Eur. Math. Soc. (JEMS)* **12** (2010), 939–1008, doi:10.4171/jems/220.
- [8] M. W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Ann. of Math. (2)* **154** (2001), 383–406, doi:10.2307/3062101.
- [9] G. A. Miller, On the commutators of a given group, *Bull. Am. Math. Soc.* **6** (1899), 105–109, doi:10.1090/s0002-9904-1899-00683-9.
- [10] O. Ore, Some remarks on commutators, *Proc. Am. Math. Soc.* **2** (1951), 307–314, doi:10.2307/2032506.
- [11] O. Schreier, Die Untergruppen der freien Gruppen, *Abh. Math. Semin. Univ. Hambg.* **5** (1927), 161–183, doi:10.1007/bf02952517.
- [12] Y. S. Tan, On the diameter of Cayley graphs of finite groups, 2011, {<http://www.math.uchicago.edu/~may/VIGRE/VIGREREU2011.html>}.
- [13] I. Zisser, The covering numbers of the sporadic simple groups, *Israel J. Math.* **67** (1989), 217–224, doi:10.1007/bf02937296.