COPRIME INVARIABLE GENERATION AND MINIMAL-EXPONENT GROUPS

ELOISA DETOMI, ANDREA LUCCHINI AND COLVA M. RONEY-DOUGAL

ABSTRACT. A finite group G is *coprimely invariably generated* if there exists a set of generators $\{g_1, \dots, g_u\}$ of G with the property that the orders $|g_1|, \dots, |g_u|$ are pairwise coprime and that for all $x_1, \dots, x_u \in G$ the set $\{g_1^{x_1}, \dots, g_u^{x_u}\}$ generates G.

We show that if G is coprimely invariably generated, then G can be generated with three elements, or two if G is soluble, and that G has zero presentation rank. As a corollary, we show that if G is any finite group such that no proper subgroup has the same exponent as G, then G has zero presentation rank. Furthermore, we show that every finite simple group is coprimely invariably generated by two elements, except for $\mathrm{O}_8^+(2)$ which requires three elements.

Along the way, we show that for each finite simple group S, and for each partition $\pi_1, \dots, \pi_u$ of the primes dividing $|S|$, the product of the number $k_{\pi_i}(S)$ of conjugacy classes of π_i-elements satisfies

$$\prod_{i=1}^{u} k_{\pi_i}(S) \leq \frac{|S|}{2|\mathrm{Out}\, S|}.$$

1. INTRODUCTION

Following [11], we say that a subset $\{g_1, \dots, g_u\}$ of a finite group G *invariably generates* G if $\{g_1^{x_1}, \dots, g_u^{x_u}\}$ generates G for every choice of $x_i \in G$.

Any finite group G contains an invariable generating set (consider the set of representatives of each of the conjugacy classes). Several papers deal with the question of bounding the the minimal cardinality of an invariable generating set for a finite group together with an analysis of the probability that d independently and uniformly randomly chosen elements of a group G generate G with good probability (see for example [12], [11], [17], [18], [23], [29]). The related *Chebotarev invariant* $C(G)$ of G (defined as the expected value of the random variable n that is minimal subject to the requirement that n randomly chosen elements of G invariably generate G) has some relevance to the problem of determining the Galois group of a polynomial with integer coefficients (see [11] and [19]).

In this paper we deal with finite groups admitting an invariable generating set consisting of elements of coprime orders.

We thank the anonymous referee for their helpful suggestions, which have improved the paper. Colva Roney-Dougal acknowledges the support of EPSRC grant EP/I03582X/1.

Definition 1.1. A finite group G is *coprimely invariably generated* if there exists a set of invariable generators $\{g_1, \dots, g_u\}$ of G with the property that the orders $|g_1|, \dots, |g_u|$ are pairwise coprime.

Our main result says that a coprimely invariably generated group can be generated with very few elements. Let $d(G)$ denote the minimal number of generators of G.

Theorem 1.2. *Let G be a coprimely invariably generated group. Then $d(G) \leq 3$.*

Notice that coprime invariable generation is the combination of two properties: the existence of an invariable generating set and the existence of a set of generators of coprime orders. It is worth noticing than neither of these properties suffices to obtain an upper bound on the smallest cardinality of generators of a finite group G. We have already observed that any finite group G is invariably generated, but conversely for every $t \in \mathbb{N}$ there exists a finite (supersoluble) group G with the property that $d(G) = t$ and G can be generated with t elements of coprime order (see Proposition 3.3).

For general G, the bound on $d(G)$ given in Theorem 1.2 cannot be improved: there exist infinitely many coprimely invariably generated groups G with $d(G) = 3$ (see Proposition 3.2). However, better resuls hold under additional assumptions. For example, we have a stronger result for finite soluble groups.

Theorem 1.3. *Let G be a coprimely invariably generated group. If G is soluble, then $d(G) \leq 2$.*

A motivation for our interest in coprime invariable generation is the fact that this property is satisfied by finite groups without proper subgroups of the same exponent (we shall call these groups *minimal exponent groups*). Indeed, assume that G is a minimal exponent group with $e := \exp(G) = p_1^{n_1} \cdots p_t^{n_t}$. Then for every i, the group G contains an element g_i of order $p_i^{n_i}$. Clearly $\exp\langle g_1^{x_1}, \dots, g_t^{x_t}\rangle = e$, for every $x_1, \dots, x_t \in G$. Hence our assumption that no proper subgroup of G has exponent e implies that $G = \langle g_1^{x_1}, \dots, g_t^{x_t}\rangle$, so G is coprimely invariably generated. In particular, as a corollary of Theorems 1.2 and 1.3, we deduce a result already proved in [25] and [10]: each finite group G contains a 3-generated subgroup H with $\exp(G) = \exp(H)$, and if G is soluble then there exists a 2-generated subgroup H of G with $\exp(G) = \exp(H)$.

Notice that the examples given in Proposition 3.2 of coprimely invariably generated groups G which are not 2-generated are all not minimal exponent. Indeed, the property of being minimal exponent is much stronger than coprime invariable generation.

Whereas the bound $d(G) \leq 3$ in Theorem 1.2 cannot be improved, we have no example of a finite minimal exponent group G which cannot be generated by 2 elements and the following interesting question is open: *is it* *true that any finite group G contains a 2-generated proper subgroup with the same exponent?* We think that the study of coprimely invariably generated groups could help to answer this question.

The minimal exponent property is not inherited by quotients; conversely, all epimorphic images of a coprimely invariably generated group (and consequently of a minimal exponent group) are coprimely invariably generated. From this point of view, studying coprimely invariably generated groups yields information about quotients of minimal exponent groups.

Another result in this paper concerns the presentation rank of coprimely invariably generated groups. The *presentation rank* $pr(G)$ of a finite group G is an invariant whose definition comes from the study of relation modules (see [6] for more details). Let I_G denote the augmentation ideal of $\mathbb{Z}G$, and $d(I_G)$ the minimal number of elements of I_G needed to generate I_G as a G-module, then $d(G) = d(I_G) + pr(G)$ [28]. It is known that $pr(G) = 0$ for many groups G, including all soluble groups, all Frobenius groups and all 2-generated groups.

Theorem 1.4. *Let G be a coprimely invariably generated group. Then G has zero presentation rank.*

As an immediate corollary, we get the following.

Theorem 1.5. *Let G be a finite group such that no proper subgroup has the same exponent as G. Then G has zero presentation rank.*

As a further contribution to the understanding of coprimely invariably generated groups, we present the following theorem.

Theorem 1.6. *Let G be a finite simple group. The group G is coprimely invariably generated by two elements if and only if $G \not\cong \mathrm{O}_8^+(2)$. The group $\mathrm{O}_8^+(2)$ is coprimely invariably generated by three elements.*

In [17] and [18] (independently) it is proved that every finite simple group is invariably generated by two elements, and it is reasonably straightforward to check that in almost all cases those elements either have coprime orders, or can be replaced by powers with coprime orders.

Finally, the following result on conjugacy classes of finite simple groups may be of independent interest. If G is a group and $\pi = \{p_1, \dots, p_k\}$ a set of primes, then $|G|_\pi$ denotes the π-part of $|G|$ and an element of G whose order is $p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, for some $\alpha_1, \dots, \alpha_k \in \mathbb{Z}_{\geq 0}$, is a π-element. Notice that the identity is a π-element. We let $k_\pi(G)$ denote the number of conjugacy classes of π-elements of G.

Theorem 1.7. *Let S be a finite simple group and let $\pi_1, \dots, \pi_u$ be a partition of $\pi(S)$. Then*

$$\prod_{i=1}^{u} k_{\pi_i}(S) \leq \frac{|S|}{2|\mathrm{Out}\, S|}.$$

This paper is structured as follows. In Section 2 we present some background information needed for our proofs. In Section 3 we construct two interesting families of examples, exploring the necessity and sufficiency of coprime invariable generation in controlling minimal generation and exponent. In Section 4 we prove Theorem 1.3, then in Section 5 we prove Theorems 1.2 and 1.4. Finally, in Sections 6 and 7 we prove Theorems 1.6 and 1.7, respectively.

2. Background material

In this section we introduce primitive monolithic groups and crown-based powers, and collect some information about their minimal number of generators, and about their presentation rank.

A group L is *primitive monolithic* if L has a unique minimal normal subgroup A, and trivial Frattini subgroup. We define the *crown-based power* of L of *size* t to be

$$L_t = \{(l_1, \dots, l_t) \in L^t \mid l_1 A = \cdots = l_t A\} = A^t \operatorname{diag}(L^t).$$

In [6] it was proved that, given a finite group G, there exist a primitive monolithic group L and a positive integer t such the crown-based power L_t of size t is an epimorphic image of G and $d(G) = d(L_t) > d(L/\operatorname{soc}(L))$.

The minimal number of generators of a crown-based power L_t in the case where A is abelian can be computed with the following formula:

Theorem 2.1. [8, Proposition 6] *Let L be a primitive monolithic group with abelian socle A, and let t be as above. Define*

$$r_L(A) = \dim_{\mathrm{End}_{L/A}(A)} A \qquad s_L(A) = \dim_{\mathrm{End}_{L/A}(A)} H^1(L/A, A)$$

and set $\theta = 0$ if A is a trivial L/A-module, and $\theta = 1$ otherwise. Then

$$d(L_t) = \max\left(d(L/A), \theta + \left\lceil \frac{t + s_L(A)}{r_L(A)} \right\rceil\right)$$

where $\lceil x \rceil$ denotes the smallest integer greater or equal to x.

A result of Aschbacher and Guralnick [1] assures us that $s_L(A) < r_L(A)$:

Theorem 2.2. [1] *Let p be a prime and G be a finite group. If A is a faithful irreducible G-module over $\mathbb{F}_p$, then $|H^1(G, A)| < |A|$.*

For soluble G we will use the following (the proof can be found in [30]):

Theorem 2.3 (Gaschütz)**.** *Let p be a prime. If G is a finite p-soluble group and A is a faithful irreducible G-module over $\mathbb{F}_p$, then $|H^1(G, A)| = 0$.*

When A is non-abelian, $d(L_t)$ can be evaluated using the following, where $P_{L,A}(k)$ denotes the conditional probability that k randomly chosen elements of L generate L, given that they project onto generators for L/A.

Theorem 2.4. [6, Theorem 2.7] *Let L be a monolithic primitive group with non-abelian socle A, and let $d \geq d(L)$. Then $d(L_t) \leq d$ if and only if*

$$t \leq \frac{P_{L,A}(d)|A|^d}{|C_{\operatorname{Aut} L}(L/A)|}.$$

Bounds on $P_{L,A}(d)$ were studied in [10] and [27], achieving the strong result:

Theorem 2.5. [10] *Let L be a primitive monolithic group with socle A. Then $P_{L,A}(d) \geq 1/2$.*

We finish this introductory section with a result on presentation rank.

Theorem 2.6. *Let G be a finite group and let L_t be a crown based power of a primitive monolithic group L such that L_t is a homomorphic image of G and $d(G) = d(L_t) > d(L/\operatorname{soc}(L))$. If $\operatorname{soc}(L)$ is abelian, then $pr(G) = 0$.*

Proof. For an irreducible G-module M, we set

$$r_G(M) = \dim_{\operatorname{End}_G(M)} M \qquad s_G(M) = \dim_{\operatorname{End}_G(M)} H^1(G, M)$$

and define

$$h_G(M) = \theta + \left\lceil \frac{s_G(M)}{r_G(M)} \right\rceil$$

where $\theta = 0$ if M is a trivial and $\theta = 1$ otherwise.

Assume that $A = \operatorname{soc}(L)$ is abelian. Let $\delta_G(A)$ be the largest integer k such that the crown based power L_k is a homomorphic image of G, and note that

$$d(L_{\delta_G(A)}) = d(L_t) = d(G).$$

By [9, Proposition 9], the integer $\delta_G(A)$ is the number of complemented chief factors G-isomorphic to A in any chief series of G. Since

$$r_G(A) = r_L(A)$$

and

$$s_G(A) = \dim_{\operatorname{End}_G(A)} H^1(G, A) = \delta_G(A) + \dim_{\operatorname{End}_{L/A}(A)} H^1(L/A, A)$$

(see Section 1 in [22], for example), it follows that

$$h_G(A) = \theta + \left\lceil \frac{\delta_G(A) + s_L(A)}{r_G(A)} \right\rceil.$$

By Theorem 2.1 we conclude that

$$d(G) = d(L_{\delta_G(A)}) = h_G(A).$$

By a result of Cossey, Gruenberg and Kovács [5, Theorem 3]

$$d(I_G) = \max\{h_G(M) \mid M \text{ an irreducible } G\text{-module}\}$$

thus, in particular, $d(I_G) \geq h_G(A) = d(G)$. Since $d(I_G) \leq d(G)$, we have an equality, hence $pr(G) = 0$. □

3. Examples

In this section, we start by constructing an infinite family of groups that show that the bound given in Theorem 1.2 cannot be improved. The same groups provide examples of coprimely invariably generated groups which are not minimal-exponent. We then construct a family of examples which demonstrate that the property of coprime generation alone is not enough to constrain the minimal number of generators of a finite group.

Lemma 3.1. *Let p be a prime and H be a finite group with $d(H) = 2$ that is invariably generated by elements of order coprime to p. Assume that V is a faithful irreducible H-module over $\mathbb{F}_p$ with $|H^1(H, V)| > 0$, and set $L = V \rtimes H$. Then the crown-based power $L_t \cong V^t \rtimes H$ of size $t = \dim_{\mathrm{End}_H(V)} V$ is coprimely invariably generated and $d(L_t) = 3$.*

Proof. By [15, Lemma 7.12], V^t is a cyclic module for $t = \dim_{\mathrm{End}_H(V)} V$. Since $|H^1(H, V)| > 0$, it follows from [1] that $d(L_t) = 3$.

If $w \in V^t$ is a generator for the H-module V^t, then w together with the coprime invariable generators of H of order coprime to p form a coprime invariable generating set for L_k. □

Proposition 3.2. *Let $r > 1$ be an integer and $L = V \rtimes \mathrm{SL}_2(2^r)$, where $V = \mathbb{F}_{2^r}^2$. Then the crown-based power $L_r \cong V^r \rtimes \mathrm{SL}_2(2^r)$ of L of size r is coprimely invariably generated and $d(L_r) = 3$. Moreover, L_r has a proper subgroup with the same exponent.*

Proof. The simple group $H = \mathrm{SL}_2(2^r)$ is coprimely invariably generated by two elements of order 2^r-1 and 2^r+1, respectively. Moreover, $|H^1(H, V)| > 0$ by [20]. Therefore Lemma 3.1 implies that L_r is coprimely invariably generated and $d(L_r) = 3$.

Finally, the subgroup $\{(l, \dots, l) \in L_r \mid l \in L\}$ is a proper subgroup of L_r with the same exponent as L_r. □

Proposition 3.3. *For any $t \in \mathbb{N}$ there exists a finite supersoluble group G such that G can be coprimely generated with $d(G) = t$ elements.*

Proof. Let $n = p_1 \cdots p_t$ be the product of the first t prime integers and let p be a prime such that n divides $p - 1$ (the prime p exists by Dirichlet's theorem). The cyclic group $C = \mathrm{C}_n$ has a fixed point free multiplicative action on $V = \mathbb{F}_p$; set L to be the monolithic group $V \rtimes C$. Let G be the crown-based power L_t, then $d(G) = t + 1$ by Theorem 2.1.

Consider a generating set $\{x_1, \dots, x_{t+1}\}$ of C with $|x_i| = p_i$ if $i \leq t$ and $x_{t+1} = 1$. A well-known theorem of W. Gaschütz [14] states that if F is a free group with n generators, H is a group with n generators, and N is a finite normal subgroup of H, then every homomorphism of F onto H/N is induced by a homomorphism of F onto H. It follows that there exist $w_1, \dots, w_{t+1}$ such that $G = \langle x_1w_1, \dots, x_{t+1}w_{t+1}\rangle$. Clearly $|x_{t+1}w_{t+1}| = p$; on the other hand if $i \leq t$, then $C_{x_i}(V) = \{0\}$, and this implies that $|x_iw_i| = |x_i| = p_i$. □

4. Proof of Theorem 1.3

Theorem 4.1. *Let $L = A \rtimes H$ be a primitive monolithic group with abelian socle A and let $t \in \mathbb{N}$. If L_t is coprimely invariably generated, then*

$$t \leq \dim_{\mathrm{End}_H(A)} A.$$

Proof. Let A be a p-group, and set $G = L_t$. Assume that $\{g_1, \dots, g_u\}$ is a set of pairwise coprime elements that invariably generate G where g_i is a p'-element for every $i \neq 1$. Set $V = A^t$.

Note that, if $|g_i|$ is coprime to p and $g_i = vh$ where $v \in V$ and $h \in H$, then g_i is conjugate to an element of $\langle h \rangle$, since $\langle h \rangle$ is a Hall p'-subgroup of $V\langle h \rangle$; in particular g_i is conjugate to an element of H. Therefore, as $\{g_1, g_2, \dots, g_u\}$ invariably generates G, by taking suitable conjugates of $g_2, \dots, g_u$, we can assume that $g_2, \dots, g_u \in H$.

Consider $g_1 = vh$, where $v \in V$ and $h \in H$, and set $K = \langle h, g_2, \dots, g_u \rangle$. Since $KV = G = HV$ and $K \leq H$, we deduce that $K = H = \langle h, g_2, \dots, g_u \rangle$. Therefore,

$$G = \langle vh, g_2, \dots, g_u \rangle \leq \langle v, h, g_2, \dots, g_u \rangle \leq \langle v \rangle^H H$$

hence $G = \langle v \rangle^H H$ and $\langle v \rangle^H = V$, that is, v is a cyclic generator for the $\mathbb{F}_p H$-module $V = A^t$. Let $v = (v_1, \dots, v_t)$. Switching to additive notation, the fact that v is a cyclic generator for the $\mathbb{F}_p H$-module V implies that the elements $v_1, v_2, \dots, v_t$ are linearly independent elements of the $\mathrm{End}_H(A)$-vector space A. In particular $t \leq \dim_{\mathrm{End}_H(A)} A$, as required. □

Proof of Theorem 1.3. Let G be a soluble, coprimely invariably generated group. Let L_t be a crown-based power such that L_t is a homomorphic image of G and $d(G) = d(L_t) > d(L/A)$. Then L_t is coprimely invariably generated and L has abelian socle. Let $r_L(A)$ and $s_L(A)$ be as in Theorem 2.1.

Since L is soluble, we see from Theorem 2.3 that $s_L(A) = 0$. Moreover Theorem 4.1 implies that $t \leq r_L(A)$, and thus $\lceil (t + s_L(A))/r_L(A) \rceil = 1$. As $d(L_t) > d(L/A)$, by Theorem 2.1 we conclude that

$$d(L_t) = \theta + \left\lceil \frac{t + s_L(A)}{r_L(A)} \right\rceil \leq 2,$$

as required. □

5. Proof of Theorems 1.2 and 1.4

Let L be a finite monolithic group whose socle A is non-abelian and let π be a set of primes. For every $l \in L$, define a_l to be the number of A-conjugacy classes of π-elements L which are contained in lA. Then set

$$a_\pi = \max\{a_l \mid l \in L\}.$$

As usual, for an integer n, the set of prime divisors of n is denoted $\pi(n)$.

Theorem 5.1. *Let L be a finite monolithic group whose socle A is non-abelian and let t be a positive integer. If the set $\{g_1, \dots, g_u\}$ invariably generates L_t, then $t \leq \prod_i a_{\pi(|g_i|)}$.*

Proof. Assume that $\{g_1, \dots, g_u\}$ invariably generates L_t, and set $\pi(|g_i|) = \pi_i$, for every i. Note that, by the definition of L_t, $g_i = (x_{i1}, \dots, x_{it})$ where $x_{i1}, \dots, x_{it}$ belong to the same coset l_iA for some $l_i \in L$; in particular $x_{i1}, \dots, x_{it}$ are π_i-elements of l_iA.

If there exist r and s such that $x_{is} = x_{ir}^y$ for some $y \in A$, then by replacing g_i by a suitable conjugate we can assume that $x_{is} = x_{ir}$ (more precisely, we take the conjugate of g_i by the element $\overline{y} = (1, \dots, y, \dots, 1) \in L_t$, where y is in the r-th position). Let $a = \prod_i a_{\pi_i}$. If $t > a$, then it follows from the definition of a_π that there exist $r, s \in \{1, \dots, t\}$ with $r \neq s$ such that $x_{ir} = x_{is}$ for every $i \in \{1, \dots, u\}$. But then $\langle g_1, \dots, g_u \rangle \leq \{(l_1, \dots, l_t) \in L_t \mid l_r = l_s\}$ which is a proper subgroup of L_t, a contradiction. □

Lemma 5.2. *Let L be a monolithic primitive group with non-abelian socle A and let π be a set of primes. Then*

$$a_\pi \leq k_\pi(A).$$

Proof. Let l be a π-element of L such that $a_l = a_\pi$. Set $X = \langle l \rangle A$. Let $x \in lA$. Since $X/A = \langle xA \rangle$, we have $X = AC_X(x)$ whence every X-conjugacy class in lA is a single A-orbit. In particular a_l coincides with the number of X-conjugacy classes of π-elements in the coset lA.

By [13, Theorem 1.6], a_l is precisely the number of A-conjugacy classes of π-elements in A which are invariant under X, whence $a_l \leq k_\pi(A)$. □

Lemma 5.3. *Let L be a monolithic primitive group with non-abelian socle $A = S^n$, and let $\pi_1, \dots, \pi_u$ be disjoint sets of primes. Then*

$$\prod_{i=1}^{u} a_{\pi_i} \leq \frac{|A|}{2n|\operatorname{Out} S|}.$$

Proof. By Lemma 5.2, we may bound $a_{\pi_i} \leq k_{\pi_i}(A)$ for all i. As $A = S^n$, we get $k_{\pi_i}(A) = k_{\pi_i}(S)^n$. Now consider a partition $\tilde{\pi}_1, \dots, \tilde{\pi}_u$ of $\pi(|S|)$ with the property that $\tilde{\pi}_i \supset \pi_i \cap \pi(|S|)$: clearly $k_{\pi_i}(S) \leq k_{\tilde{\pi}_i}(S)$. It follows from Theorem 1.7 (whose proof is in Section 7) that

$$\prod_{i=1}^{u} k_{\tilde{\pi}_i}(S) \leq \frac{|S|}{2|\operatorname{Out} S|}.$$

Therefore

$$\prod_{i=1}^{u} a_{\pi_i} \leq \prod_{i=1}^{u} k_{\pi_i}(A) = \prod_{i=1}^{u} k_{\pi_i}(S)^n \leq \prod_{i=1}^{u} k_{\tilde{\pi}_i}(S)^n \leq \frac{|S|^n}{2^n|\operatorname{Out} S|^n} \leq \frac{|A|}{2n|\operatorname{Out} S|}$$

as required. □

Lemma 5.4. *Let L be a monolithic primitive group with non-abelian socle $A = S^n$. If L_t is minimally d-generated (i.e. $d(L_t/N) < d(L_t) = d$ for every $1 \neq N \lhd L_t$) and*

$$t \leq \frac{|A|}{2n|\mathrm{Out}\, S|}$$

then $d = 2$ (and $t = 1$).

Proof. Set $d_L = d(L)$ and note that $d_L \geq 2$ since L has non-abelian socle. Let X be the subgroup of $\mathrm{Aut}\, S$ induced by the conjugation action of $N_G(S_1)$ on the first factor S_1 of $A = S_1 \times \cdots \times S_n$, with $S \cong S_i$ for each $1 \leq i \leq n$. As in the proof of Lemma 1 in [7],

$$|C_{\mathrm{Aut}\, A}(L/A)| \leq n|S|^{n-1}|C_{\mathrm{Aut}\, S}(X/S)|$$

and therefore

$$|C_{\mathrm{Aut}\, A}(L/A)| \leq n|S|^{n-1}|\,\mathrm{Aut}\, S| = n|A||\mathrm{Out}\, S|.$$

By Theorem 2.5, $P_{L,A}(d_L) \geq 1/2$. So the assumptions give that

$$t \leq \frac{1}{2}\frac{|A|}{n|\mathrm{Out}\, S|} \leq \frac{P_{L,A}(d_L)|A|^2}{n|A||\mathrm{Out}\, S|} \leq \frac{P_{L,A}(d_L)|A|^{d_L}}{|C_{\mathrm{Aut}\, A}(L/A)|}.$$

By Theorem 2.4 this implies that $d = d(L_t) = d_L$. As L_t is minimally d-generated, it follows that $t = 1$; in particular, L is minimally d-generated. Now, by the main theorem in [24], $d(L) = \max\{2, d(L/A)\}$, and again by minimality, we conclude that $d = d(L) = 2$. □

Proof of Theorem 1.2. Let G be a coprimely invariably generated group and let $d = d(G)$. As remarked in Section 2, there exists a monolithic primitive group L with socle A and an integer t, such that L_t is a quotient of G and $d = d(L_t) > d(L/A)$. Moreover L_t is coprimely invariably generated.

If A is abelian, then we can apply Theorem 2.1: since $d(L_t) > d(L/A)$ and, by Theorems 2.2 and 4.1, $s_L(A) < r_L(A)$ and $t \leq r_L(A)$, it follows that

$$d(G) = d(L_t) = \theta + \left\lceil \frac{t + s_L(A)}{r_L(A)} \right\rceil \leq \theta + 2 \leq 3.$$

If A is non-abelian and $\{g_1, \ldots, g_u\}$ are coprime invariable generators of L_t, then by Theorem 5.1, $t \leq \prod_{i=1}^{u} a_{\pi(|g_i|)}$. Then by Lemma 5.3

$$\prod_{i=1}^{u} a_{\pi(|g_i|)} \leq \frac{|A|}{2n|\mathrm{Out}\, S|}.$$

Thus

$$t \leq \frac{|A|}{2n|\mathrm{Out}\, S|}$$

and by Lemma 5.4 we conclude that $d(G) = d(L_t) = 2$. □

Proof of Theorem 1.4. Let G be a coprimely invariably generated group. Assume, by way of contradiction, that $pr(G) > 0$. Let L and $t \in \mathbb{N}$ be such that L is a monolithic primitive group with socle A and L_t is a homomorphic image of G, with $d(L_t) = d(G) = d$ and $d > d(L/N)$.

If A is abelian, then $pr(G) = 0$ by Theorem 2.6, a contradiction. If A is non-abelian, then arguing as in the proof of the non-abelian case of Theorem 1.2, we conclude that $d = d(L_t) = 2$. Thus again $pr(G) = 0$. □

6. Proof of Theorem 1.6

In the following proof, by $[a, b]$ we denote the lowest common multiple of integers a and b.

Proof of Theorem 1.6. We make use of the invariable generators given in [18], where it is proved that every finite simple group is invariably generated by two elements. For the classical groups, the orders given in [18] are for the quasisimple groups, so we must adjust their values to get projective orders.

For the alternating groups, the generators given in [18, Proof of Lemma 5.2] are of coprime orders.

For the special linear groups in dimension $n \geq 3$, the invariable generators in [18] have orders $(q^n - 1)/((q-1, n)(q-1))$ and $(q^{n-1} - 1)/(q-1)$, which are coprime. The given generators for $\mathrm{PSL}_2(q)$ are also always of coprime order. For the unitary groups and the orthogonal groups other than $\mathrm{O}^-_{4k+2}(q)$ with q odd and $\mathrm{O}^+_8(q)$ with $q \leq 3$, the given generators are coprime. For $\mathrm{O}^-_{4k+2}(q)$ it suffices to take the square of the second generator in [18] to produce coprime invariable generators.

For the symplectic groups in dimension $2m \geq 4$, the given generators have orders $(q^m + 1)/(q-1, 2)$ and $[q^{m-1} + 1, q + 1]$, which are coprime when m is even but need not be when m is odd. However, it follows from [16, Lemma 2.8] that except when $(n, q) = (6, 2)$ or $(6, 3)$ we may replace the element of order $(q^m + 1)/(q-1, 2)$ by its power of order a maximal divisor s of $q^m + 1$, subject to being coprime with $q^i - 1$ for $i < 2m$, and the result will hold. We may generate $\mathrm{S}_6(2)$ with an element of order 8 and an element of order 15, since by [4] the unique maximal subgroup (up to conjugacy) to contain elements of both of these orders is S_8, which contains a unique conjugacy class of elements of order 8, whilst $\mathrm{S}_6(2)$ contains two. We may generate $\mathrm{S}_6(5)$ with an element of order 7 and one of order 13, since by [3, Tables 8.28, 8.29] there are no maximal subgroups whose order is divisible by both 7 and 13.

Of the classical groups, this leaves only $\mathrm{O}^+_8(2)$ and $\mathrm{O}^+_8(3)$. For $G := \mathrm{O}^+_8(2)$, it is straightforward to run a computer search in MAGMA [2] which tests that each pair of G-conjugacy classes of coprime elements intersects at least one maximal subgroup nontrivially. Running the same test on triples of conjugacy classes of coprime elements reveals 117 coprime invariant generating conjugacy class triples (many of which are automorphic twists of each other). One such consists of class `5A`, class `7A`, and a choice of four of the seven G-classes of order 12. To see this, note that the only maximal subgroups to contain elements of order 5, 7 and 12 are $2^6{:}\mathrm{A}_8$, $\mathrm{S}_6(2)$ and A_9. There are three copies of each of these, cycled by the triality automorphism. Each of them contains exactly one of the three classes of 5-elements, so class `5A` selects one G-class of each isomorphism type. The groups $2^6{:}\mathrm{A}_8$ contain two classes of elements of order 12, the groups $\mathrm{S}_6(2)$ contain three, two of which are conjugate in $\mathrm{O}_8^+(2)$, and the groups A_9 contain only one. Thus in total we have accounted for at most five of the seven classes of elements of order 12, leaving at least two (in fact, four) from which to choose a third coprime invariable generator.

The group $\mathrm{O}_8^+(3)$ contains one class of elements of order 7 and fourteen classes of elements of order 9, which form orbits of lengths $6, 4$ and 4 under the outer automorphisms. We may choose elements from classes `9A`, `9G` and `9K` as $\mathrm{Aut}\,\mathrm{O}_8^+(3)$-orbit representatives, which have centraliser orders $2^2 \cdot 3^6$, 3^6 and 3^4, respectively. We shall show that $\mathrm{O}_8^+(3)$ is invariably generated by classes `7A` and `9G`. There are three maximal subgroups which contain elements of order 7 and 9, namely $\mathrm{O}_7(3)$, $\mathrm{O}_8^+(2)$ and $2.\mathrm{U}_4(3).2^2$. The group $\mathrm{O}_7(3)$ contains four classes of elements of order 9. Two have these have even centraliser orders, so must lie in the `9A` orbit. The remaining two can be checked using MAGMA to lie in the `9K` orbit. The group $\mathrm{O}_8^+(2)$ contains three classes of elements of order 9, all conjugate under triality. These all lie in the `9K` orbit. Finally, in the group $2.\mathrm{U}_4(3).2^2$ all elements of order 9 have even centraliser orders, so lie in the `9A` orbit. Thus class `9G` lies in none of these subgroups.

For all of the exceptional groups except $\mathrm{E}_7(q)$, the invariable generators given in [18] are coprime. Thus we need only consider $\mathrm{E}_7(q)$. By [16, Table 6], elements of order $(q+1)(q^6-q^3+1)/(2,q-1)$ are contained only in a copy of ${}^2\mathrm{E}_6(q)_{sc}.\mathrm{D}_{q+1}$. Since the order of $\mathrm{E}_7(q)$ is divisible by $q^{14}-1$, we may find an element of order a Zsigmondy prime for $q^{14}-1$ in $\mathrm{E}_7(q)$. Such a prime does not divide the order of ${}^2\mathrm{E}_6(q)$ or $q+1$, so gives a pair of invariable generators for $\mathrm{E}_7(q)$.

For the sporadics and the Tits group, [16, Table 9] lists carefully chosen conjugacy classes of elements of the sporadics groups, together with a complete list of the maximal subgroups containing those conjugacy classes. It suffices to check that in each case there exists an element of order coprime to the given one that lies in none of the listed maximal subgroups. □

7. Proof of Theorem 1.7

In this section we prove Theorem 1.7. First, we need a preliminary lemma.

Lemma 7.1. *Assume that G is a finite group and let $\pi \subseteq \pi(G)$. Then $k_\pi(G) \leq |G|_\pi$. In particular if $\pi = \{p\} \cup \tilde{\pi}$, then $k_\pi(G) \leq k_p(G) \cdot |G|_{\tilde{\pi}}$.*

Proof. We prove that $k_\pi(G) \leq |G|_\pi$ by induction on $|\pi|$. The case $|\pi| = 1$ is an immediate consequence of the Sylow Theorems. Assume $\pi = \{p\} \cup \tilde{\pi}$. Let g by a π-element of G; we may write $g = ab$ where a is a p-element and

b is a $\tilde{\pi}$-element and both are powers of g. Up to conjugacy we have at most $k_p(G)$ choices for a. For a fixed choice of a we have to count the number of b. Notice that $b \in H = C_G(a)$. Moreover if b_1 and b_2 are conjugate in H then ab_1 and ab_2 are conjugate in G. Hence the number of choices of b is bounded by the number of conjugacy classes of $\tilde{\pi}$ elements in H, and by induction this number is at most $|H|_{\tilde{\pi}} \leq |G|_{\tilde{\pi}}$. Thus $k_\pi(G) \leq |G|_\pi$ as required.

By the same argument, we now have that

$$k_\pi(G) \leq k_p(G) k_{\tilde{\pi}}(H) \leq k_p(G)|H|_{\tilde{\pi}} \leq k_p(G)|G|_{\tilde{\pi}}.$$

□

We in fact prove a slightly stronger version of Theorem 1.7, which we state now. Let $\mathcal{S} = \{\mathrm{A}_n \ : \ n \leq 7\} \cup \{\mathrm{L}_2(q) \ : \ q \in \{7, 8, 11, 27\}\} \cup \{\mathrm{L}_3(4)\}$.

Theorem 7.2. *Let S be a finite simple group and let $\pi_1, \ldots, \pi_u$ be a partition of $\pi(S)$. Then*

$$\prod_{i=1}^{u} k_{\pi_i}(S) \leq \frac{|S|}{2|\mathrm{Out}\, S|}.$$

Furthermore, if $S \notin \mathcal{S}$, then there exists a prime p dividing $|S|$ such that

$$k_p(S) \leq \frac{|S|_p}{2|\mathrm{Out}\, S|}.$$

Proof. For groups in $\mathcal{S}$, this is a direct calculation using their conjugacy classes. For the remaining groups, the first claim follows from the second and Lemma 7.1. The alternating case is considered in Lemma 7.3, below. The linear and unitary groups and the symplectic and orthogonal groups are dealt with in Lemmas 7.4 and 7.5, respectively. The exceptional case is completed in Lemma 7.6. For the sporadics, this is a straightforward exercise, using [4]. □

Lemma 7.3. *Let $S = \mathrm{A}_n$ for some $n \geq 7$. Then there exists a prime r dividing $|S|$ such that S has at most one conjugacy class of nontrivial r-elements. Furthermore, if $n \geq 8$ then there exists a prime p dividing $|S|$ such that*

$$k_p(S) \leq \frac{|S|_p}{2|\mathrm{Out}\, S|}.$$

Proof. First let $k = \lfloor n/2 \rfloor$. Then Bertrand's postulate states that for $k \geq 4$, there exists a prime r such that $k \leq n/2 < r < 2k - 2 \in \{n-2, n-3\}$, so the first claim follows (after verifying that $r = 5$ works when $n = 7$).

As for the second claim, note that $|\mathrm{Out}\, S| = 2$. For $n = 8$, we use $k_2(S) = 5$ whilst $|S|_2 = 2^6$. For $n = 9$, we use $k_3(S) = 6$ whilst $|S|_3 = 3^4$. For $n \in \{10, 11, 12, 13\}$ we use $k_5(S) = 3$. We may therefore assume that $n \geq 14$ and $n - 2 > p = r \geq 11$. Thus $k_p(S) = 2$, whilst $\frac{|S|_p}{2|\mathrm{Out}\, S|} \geq 11/4 > 2$, so the result follows. □

Lemma 7.4. *Let $S \cong \mathrm{L}_n(p^e), \mathrm{U}_n(p^e)$ be simple, and assume that $S \notin \{\mathrm{L}_2(q) \ : \ q \in \{4,5,7,8,9,11,27\}\} \cup \{\mathrm{L}_3(4)\}$. Then*

$$k_p(S) \leq \frac{|S|_p}{2|\mathrm{Out}\, S|}.$$

Proof. By [21, Lemma 1.4], $k_p(S) \leq np(n) + 1$, where $p(n)$ is the partition function of n. Since $p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + \cdots$, where the sum is over the pentagonal numbers less than n and the sign of the kth term is $(-1)^{\lfloor (k-1)/2 \rfloor}$, we may bound $np(n) + 1 \leq n2^n$.

First suppose that $n = 2$, so that $|S|_p = q$. Then without loss of generality $S \cong \mathrm{L}_2(p^e)$. Here $k_p(S) = 2$ for $p = 2$, and 3 for p odd, whilst $|\mathrm{Out}\, S|$ is e for $p = 2$ and $2e$ for p odd. Thus for $p = 2$ we must check that $2^e \geq 2 \cdot 2e$, which holds for all $e \geq 4$. For p odd we require $p^e \geq 12e$, which clearly holds for all e when $p \geq 13$. If $p = 3$ this yields $e \geq 4$, and when $5 \leq p \leq 11$ this yields $e \geq 2$.

Next suppose that $n = 3$, so that $|S|_p = q^3$. Suppose first that $S \cong \mathrm{L}_3(p^e)$. If $q \equiv 1 \bmod 3$ then $k_p(S) = 5$ and $|\mathrm{Out}\, S| = 6e$, so we require $p^{3e} \geq 60e$, which holds for all such $q > 4$. If $q \equiv 0, 2 \bmod 3$ then $k_p(S) = 3$ and $|\mathrm{Out}\, S| = 2e$, so we require $p^{3e} \geq 12e$, which holds for all $q > 2$ (but recall that $S \not\cong \mathrm{L}_3(2) \cong \mathrm{L}_2(7)$). Suppose next that $S \cong \mathrm{U}_3(p^e)$. In this case, if $q \equiv 2 \bmod 3$ then $k_p(S) = 5$, whilst if $q \equiv 0, 1 \bmod 3$ then $k_p(S) = 3$. Since $\mathrm{U}_3(2)$ is not simple, and $|\mathrm{Out}\, S| = (3, q+1) \cdot 2e$, the result follows by a similar calculation to that for $\mathrm{L}_3(q)$.

We now consider the general case. We bound k_p by $np(n) + 1 \leq n2^n$, whilst the order of a Sylow p-subgroup of S is $q^{n(n-1)/2}$ and

$$|\mathrm{Out}\, S| \leq 2(q-1)\log_p q < q^2.$$

If $n2^n \geq q^{n^2/2 - n/2 - 2}/2$ then $(n, q) \in \{(4,2), (4,3), (5,2)\}$. In fact $k_2(\mathrm{L}_4(2)) = 5 < 2^6/4$, whilst $k_3(\mathrm{L}_4(3)) = 7 < 3^6/8$ and $k_2(\mathrm{L}_5(2)) = 7 < 2^{10}/4$, so the result follows. □

Lemma 7.5. *Let S be a simple symplectic or orthogonal group, of rank n over $\mathbb{F}_{p^e}$. Then*

$$k_p(S) \leq \frac{|S|_p}{2|\mathrm{Out}\, S|}.$$

Proof. Here $|S|_p \geq q^{n^2 - n}$ and $|\mathrm{Out}\, S| \leq 2(q-1, 2)^2 \log_p q$, which is less than q^2 for all q. By [21, Lemmas 1.4 and 1.5] if S is symplectic then

$$k_p(S) \leq p(2n)2^{(2n)^{1/2}} < 6^n$$

(where $p(n)$ is the partition function of n), whilst if S is orthogonal then

$$k_p(S) \leq 2(n,2)p(2n+1)2^{(2n+1)^{1/2}} < 6^n.$$

If $n = 2$ then $q > 2$ and S is symplectic, so that $|S|_p = q^4$ and $|\mathrm{Out}\, S| = 2(q, 2)\log_p q$, whilst $k_p(S) \leq 7$, so the result follows for all q.

If $n = 3$ then $k_p(S) \leq 60, 187$ for S symplectic or orthogonal, respectively, so the result is immediate for $q \geq 5$, and for the remaining q we check that in fact $k_p(S) \leq 16$.

If $n = 4$ then $k_p(S) \leq 156$ for S symplectic and 960 for S orthogonal, so the result is immediate for $q \geq 7$. For $2 \leq q \leq 5$ we verify that in fact $k_p(S) \leq 81$, which completes the proof.

If $n \geq 5$ the result follows immediately from the 6^n bounds, for all q. □

Lemma 7.6. *Let $S \cong {}^rX_l(p^e)$ be a simple group of exceptional type. Then*

$$k_p(S) \leq \frac{|S|_p}{2|\mathrm{Out}\, S|}.$$

Proof. We use the results cited in [21, Proof of Lemma 1.5] to bound $k_p(S)$ for each family. Let $q = p^e$.

If $S \cong \mathrm{F}_4(q), \mathrm{E}_6(q), {}^2\mathrm{E}_6(q), \mathrm{E}_7(q), \mathrm{E}_8(q)$, then $|S|_p \geq q^{24}$ and $|\mathrm{Out}\, S| \leq 6 \log_p q < q^3$, whilst $k_p(S) \leq 202$ so the result is clear.

If $S \cong \mathrm{G}_2(q)$ then $|S|_p = q^6$ and $|\mathrm{Out}\, S| \leq 2 \log_p q < q$, whilst $k_p(S) \leq 9$. If $S \cong {}^2\mathrm{B}_2(q)$ then $|S|_p = q^2$ and $|\mathrm{Out}\, S| = \log_p q$, whilst $k_p(S) = 4$, so the result holds for all $q > 2$, however ${}^2\mathrm{B}_2(2)$ is not simple. If $S \cong {}^2\mathrm{D}_4(q)$ then $|S|_p = q^{12}$ and $|\mathrm{Out}\, S| = 3 \log_p q < q^2$, whilst $k_p(S) \leq 8$, so the result is clear. If $S \cong {}^2\mathrm{G}_2(q)$ then $q \geq 27$ with $|S|_p = q^3$ and $|\mathrm{Out}\, S| = \log_p q$, whilst $k_p(S) \leq 10$, so the result holds for all q. Finally, if $S \cong {}^2\mathrm{F}_4(q)$ then $|S|_p = q^{12}$ and $|\mathrm{Out}\, S| = \log_p q$, whilst $k_p(S) < 35$. □

References

1. M. Ascbacher & R. Guralnick. Some applications of the first cohomology group. *J. Algebra* **90** (1984) 446–460.
2. W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.
3. J.N. Bray, D.F. Holt, C.M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups.* London Mathematical Society Lecture Note Series **407**, Cambridge University Press, Cambridge 2013.
4. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker & R.A. Wilson. *An 𝔸𝕋𝕃𝔸𝕊 of Finite Groups.* Clarendon Press, Oxford, 1985; reprinted with corrections 2003.
5. J. Cossey, K. W. Gruenberg & L. G. Kovács. The presentation rank of a direct product of finite groups. *J. Algebra* **28** (1974) 597–603.
6. F. Dalla Volta & A. Lucchini. Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc. Ser. A* **64:1** (1998) 82–91.
7. F. Dalla Volta & A. Lucchini. The smallest group with non-zero presentation rank. *J. Group Theory* **2:2** (1999) 147–155.
8. F. Dalla Volta, A. Lucchini & F. Morini. On the probability of generating a minimal d-generated group. *J. Aust. Math. Soc.* **71:2** (2001) 177–185.
9. E. Detomi & A. Lucchini. Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra* **265** (2003) 651–668.
10. E. Detomi & A. Lucchini. Probabilistic generation of finite groups with a unique minimal normal subgroup. *J. London Math. Soc.* **87:3** (2013) 689–706.
11. J.D. Dixon. Random sets which invariably generate the symmetric group. *Discrete Math.* **105** No.1-3 (1992) 25–39.

12. J. Fulman & R. Guralnick, Derangements in simple and primitive groups, in: A.A. Ivanov, M.W. Liebeck, J. Saxl (Eds.), *Groups, Combinatorics and Geometry*, Durham 2001, World Sci. Publ., River Edge, NJ, 2003, pp. 99–121.
13. J. Fulman & R. Guralnick. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* **364:6** (2012) 3023–3070.
14. W. Gaschütz. Zu einem von B.H. und H. Neumann gestellten Problem. *Math. Nachr.* **14** (1955) 249–252.
15. K. Gruenberg, Relation modules of finite groups, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 25. American Mathematical Society, Providence, R.I., 1976.
16. R. Guralnick & G. Malle. Products of conjugacy classes and fixed point spaces. *J. Amer. Math. Soc.* **25:1** (2011) 77–121.
17. R. Guralnick & G. Malle, Simple groups admit Beauville structures, *J. Lond. Math. Soc.* **(2) 85** (2012), no. 3, 694–721.
18. W.M. Kantor, A. Lubotzky & A. Shalev. Invariable generation and the Chebotarev invariant of a finite group. *J. Algebra* **348** (2011) 302–314.
19. E. Kowalski & D. Zywina, The Chebotarev invariant of a finite group. *Exp. Math.* **21** (2012), no. 1, 38–56.
20. W. Jones & B. Parshall, On the 1-cohomology of finite groups of Lie type. *Proceedings of the Conference on Finite Groups* (Univ. Utah, Park City, Utah, 1975), pp. 313–328. Academic Press, New York, 1976.
21. M.W. Liebeck & L. Pyber. Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra* **198** (1997) 538–562.
22. A. Lucchini. Generating wreath products and their augmentation ideals. *Rend. Sem. Mat. Univ. Padova* **98** (1997) 67–87.
23. T. Luczak & L. Pyber, On random generation of the symmetric group, *Combin. Probab. Comput.* **2** (1993) 505–512.
24. A. Lucchini & F. Menegazzo. Generators for finite groups with a unique minimal normal subgroup. *Rend. Sem. Mat. Univ. Padova* **98** (1997) 173–191.
25. A. Lucchini, M. Morigi & P. Shumyatsky. Boundedly generated subgroups of finite groups. *Forum Math.* **24:4** (2012) 875–887.
26. G. Malle, J. Saxl & T. Weigel. Generation of classical groups. *Geom. Dedicata* **49** (194) 85–116.
27. N.E. Menezes, M. Quick & C.M. Roney-Dougal. The probability of generating a finite simple group. *Israel J. Math.* **198:1** (2013) 371–392.
28. K. W. Roggenkamp, Integral representations and presentations of finite groups, Lecture notes in Math. 744 (Springer, Berlin 1979)
29. A. Shalev, A theorem on random matrices and some applications, *J. Algebra* **199** (1998) 124–141.
30. U. Stammbach, Cohomological characterisations of finite solvable and nilpotent groups, *J. Pure Appl. Algebra* **11** (1977/78), no. 1–3, 293–301.

(1) Eloisa Detomi and Andrea Lucchini, Università degli Studi di Padova, Dipartimento di Matematica, Via Trieste 63, 35121 Padova, Italy
(2) Colva M. Roney-Dougal, University of St Andrews, Mathematical Institute, St Andrews, Fife KY16 9SS, Scotland