Bull. Aust. Math. Soc. **108** (2023), 449–458
doi:10.1017/S0004972723000126

FINITE GROUPS WITH INDEPENDENT GENERATING SETS OF ONLY TWO SIZES

ANDREA LUCCHINI and PABLO SPIGA

(Received 8 December 2022; accepted 5 January 2023; first published online 23 February 2023)

Abstract

A generating set S for a group G is independent if the subgroup generated by $S \setminus \{s\}$ is properly contained in G for all $s \in S$. We describe the structure of finite groups G such that there are precisely two numbers appearing as the cardinalities of independent generating sets for G.

2020 *Mathematics subject classification*: primary 20F05; secondary 20D60, 20E34.

Keywords and phrases: simple groups, generating sets, Engel elements.

1. Introduction

The *minimal number of generators* of a finite group G is denoted by $d(G)$. A generating set S for a group G is *independent* (sometimes called *irredundant*) if

$$\langle S \setminus \{s\}\rangle < G \quad \text{for all } s \in S.$$

Let $m(G)$ denote the *maximal size of an independent generating set* for G.

The finite groups with $m(G) = d(G)$ are classified by Apisa and Klopsch.

THEOREM 1.1 (Apisa–Klopsch, [1, Theorem 1.6]). *If $d(G) = m(G)$, then G is soluble. Moreover, either*

- *$G/\operatorname{Frat}(G)$ is an elementary abelian p-group for some prime p; or*
- *$G/\operatorname{Frat}(G) = PQ$, where P is an elementary abelian p-group and Q is a nontrivial cyclic q-group for distinct primes p and q, such that Q acts by conjugation faithfully on P and P (viewed as a module for Q) is a direct sum of $m(G) - 1$ isomorphic copies of one simple Q-module.*

In view of this result, Apisa and Klopsch suggest a natural 'classification problem': given a nonnegative integer c, characterise all finite groups G which satisfy $m(G) - d(G) \leq c$. The particular case $c = 1$ has been recently highlighted by Glasby (see [7, Problem 2.3]).

A nice result in universal algebra, due to Tarski and known as the *Tarski irredundant basis theorem* (see for example [3, Theorem 4.4]), implies that, for every positive integer k with $d(G) \leq k \leq m(G)$, G contains an independent generating set of cardinality k. So the condition $m(G) - d(G) = 1$ is equivalent to the fact that there are only two possible cardinalities for an independent generating set of G.

Let G be a finite group. We recall that the *socle* of G, denoted $\mathrm{soc}(G)$, is the subgroup generated by the minimal normal subgroups of G; moreover, G is said to be *monolithic primitive* if G has a unique minimal normal subgroup and the Frattini subgroup $\mathrm{Frat}(G)$ of G is the identity.

In this paper, we prove the following two main results.

THEOREM 1.2. *Let G be a finite group with $\mathrm{Frat}(G) = 1$ and $m(G) = d(G) + 1$. If G is not soluble, then $d(G) = 2$, G is a monolithic primitive group and $G/\mathrm{soc}(G)$ is cyclic of prime power order.*

It was proved by Whiston and Saxl [15] that $m(\mathrm{PSL}(2, p)) = 3$ for any prime p with p not congruent to ± 1 modulo 8 or 10. In particular, as $d(S) = 2$ for every nonabelian simple group, we deduce that there are infinitely many nonabelian simple groups G with $m(G) = d(G) + 1$. We also give examples of nonsimple groups G having $m(G) = d(G) + 1$ in Section 4.

THEOREM 1.3. *Let G be a finite group with $\mathrm{Frat}(G) = 1$ and $m(G) = d(G) + 1$. If G is soluble, then one of the following occurs:*

(1) *$G \cong V \rtimes P$, where P is a finite noncyclic p-group and V is an irreducible P-module, which is not a p-group; in this case, $d(G) = d(P)$;*
(2) *$G \cong V^t \rtimes H$, where V is a faithful irreducible H-module, $m(H) = 2$ and either $t = 1$ or H is abelian; in this case, $d(G) = t + 1$;*
(3) *there exist two normal subgroups N_1, N_2 such that $1 \lneq N_1 \leq N_2$, N_1 is an abelian minimal normal subgroup of G, $N_2/N_1 \leq \mathrm{Frat}(G/N_1)$ and $G/N_2 \cong V^t \rtimes H$, where V is an irreducible H-module and H is a nontrivial cyclic group of prime power order; in this case, $d(G) = t + 1$.*

In Section 4, we give examples of finite soluble groups G with $m(G) = d(G) + 1$ for each of the three possibilities arising in Theorem 1.3.

2. Preliminary results

Let L be a monolithic primitive group and let A be its unique minimal normal subgroup. For each positive integer k, let L^k be the k-fold direct product of L. The *crown-based power* of L of size k is the subgroup L_k of L^k defined by

$$L_k := \{(l_1, \ldots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \bmod A\}.$$

In [4], it is proved that for every finite group G, there exists a monolithic group L and a homomorphic image L_k of G such that

https://doi.org/10.1017/S0004972723000126 Published online by Cambridge University Press

(1) $d(L/\operatorname{soc} L) < d(G)$; and
(2) $d(L_k) = d(G)$.

A group L_k with this property is called a *generating crown-based power* for G.

In [4], it is explained how $d(L_k)$ can be explicitly computed in terms of k and the structure of L. A key ingredient (when one wants to determine $d(G)$ from the behaviour of the crown-based power homomorphic images of G) is to evaluate, for each monolithic group L, the maximal k such that L_k is a homomorphic image of G. This integer k arises from an equivalence relation among the chief factors of G. In what follows, we give some details.

Given groups G and A, we say that A is a *G-group* if G acts on A via automorphisms. In addition, A is *irreducible* if G does not stabilise any nontrivial proper subgroups of A. Two G-groups A and B are *G-isomorphic* if there exists a group isomorphism $\phi : A \to B$ such that $\phi(g(a)) = g(\phi(a))$ for all $a \in A$ and $g \in G$. Following [8], we say that two irreducible G-groups A and B are *G-equivalent*, denoted $A \sim_G B$, if there is an isomorphism $\Phi : A \rtimes G \to B \rtimes G$ which restricts to a G-isomorphism $\phi\colon A \to B$ and induces the identity $G \cong AG/A \to BG/B \cong G$, in other words, such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & A \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\ & & \big\downarrow{\scriptstyle \phi} & & \big\downarrow{\scriptstyle \Phi} & & \big\| & & \\ 1 & \longrightarrow & B & \longrightarrow & B \rtimes G & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Observe that two G-isomorphic G-groups are G-equivalent, and the converse holds if A and B are abelian.

Let $A = X/Y$ be a chief factor of G. A complement U of A in G is a subgroup of G such that

$$UX = G \quad \text{and} \quad U \cap X = Y.$$

We say that $A = X/Y$ is a *Frattini* chief factor if X/Y is contained in the Frattini subgroup of G/Y; this is equivalent to saying that A is abelian and there is no complement to A in G. The number $\delta_G(A)$ of non-Frattini chief factors that are G-equivalent to A, in any chief series of G, does not depend on the particular choice of such a series.

Now, we denote by $L_G(A)$ the *monolithic primitive group associated to* A, that is,

$$L_G(A) := \begin{cases} A \rtimes (G/\mathbf{C}_G(A)) & \text{if } A \text{ is abelian,} \\ G/\mathbf{C}_G(A) & \text{otherwise.} \end{cases}$$

If A is a non-Frattini chief factor of G, then $L_G(A)$ is a homomorphic image of G. More precisely, there exists a normal subgroup N such that $G/N \cong L_G(A)$ and $\operatorname{soc}(G/N) \sim_G A$. We identify $\operatorname{soc}(L_G(A))$ with A, as G-groups.

Consider now all the normal subgroups N of G with the property that $G/N \cong L_G(A)$ and $\operatorname{soc}(G/N) \sim_G A$. The intersection $R_G(A)$ of all these subgroups has the property

https://doi.org/10.1017/S0004972723000126 Published online by Cambridge University Press

that $G/R_G(A)$ is isomorphic to the crown-based power $(L_G(A))_{\delta_G(A)}$. The socle $I_G(A)/R_G(A)$ of $G/R_G(A)$ is called the A-*crown* of G and it is a direct product of $\delta_G(A)$ minimal normal subgroups G-equivalent to A.

Note that if L is monolithic primitive and L_k is a homomorphic image of G for some $k \geq 1$, then $L \cong L_G(A)$ for some non-Frattini chief factor A of G and $k \leq \delta_G(A)$. Furthermore, if $(L_G(A))_k$ is a generating crown-based power, then so is $(L_G(A))_{\delta_G(A)}$; in this case, we say that A is a *generating chief factor* for G.

For an irreducible G-module M, set

$$\begin{aligned} r_G(M) &:= \dim_{\mathrm{End}_G(M)} M, \\ s_G(M) &:= \dim_{\mathrm{End}_G(M)} H^1(G, M), \\ t_G(M) &:= \dim_{\mathrm{End}_G(M)} H^1(G/\mathbf{C}_G(M), M). \end{aligned}$$

It can be seen that

$$s_G(M) = t_G(M) + \delta_G(M)$$

(see for example [10, 1.2]). Now, define

$$h_G(M) := \begin{cases} \delta_G(M) & \text{if } M \text{ is a trivial } G\text{-module}, \\ \left\lfloor \dfrac{s_G(M) - 1}{r_G(M)} \right\rfloor + 2 = \left\lfloor \dfrac{\delta_G(M) + t_G(M) - 1}{r_G(M)} \right\rfloor + 2 & \text{otherwise}. \end{cases}$$

By [2, Theorem A], $t_G(M) < r_G(M)$ for any irreducible G-module M, and therefore

$$h_G(M) \leq \delta_G(M) + 1. \tag{2.1}$$

The importance of $h_G(M)$ is clarified by the following proposition.

PROPOSITION 2.1 [6, Proposition 2.1]. *If there exists an abelian generating chief factor A of G, then $d(G) = h_G(A)$.*

When G admits a nonabelian generating chief factor A, a relation between $\delta_G(A)$ and $d(G)$ is provided by the following result.

PROPOSITION 2.2. *If $d(G) \geq 3$ and there exists a nonabelian generating chief factor A of G, then*

$$\delta_G(A) > \frac{|A|^{d(G)-1}}{2|\mathbf{C}_{\mathrm{Aut}\,A}(L_G(A)/A)|} \geq \frac{|A|^{d(G)-2}}{2\log_2 |A|}.$$

PROOF. Suppose that $d(G) \geq 3$ and let A be a nonabelian generating chief factor of G.

For a finite group X, let $\phi_X(m)$ denote the number of ordered m-tuples $(x_1, \ldots, x_m)$ of elements of X generating X. Define

$$\begin{aligned} L &:= L_G(A), \\ \gamma &:= |\mathbf{C}_{\mathrm{Aut}\,A}(L/A)|, \\ \delta &:= \delta_G(A), \\ d &:= d(G). \end{aligned}$$

https://doi.org/10.1017/S0004972723000126 Published online by Cambridge University Press

In [4], it is proved that if $m \geq d(L)$, then

$$d(L_k) \leq m \quad \text{if and only if} \quad k \leq \frac{\phi_{L/A}(m)}{\phi_L(m)\gamma}. \tag{2.2}$$

By the main result in [13], $d(L) = \max(2, d(L/A))$. Since A is a generating chief factor, from the definition, we have $d(L/A) < d(L_{\delta_G(A)}) = d(G)$. As $2 < d(G)$, it follows $d(L) < d(G)$. Now, by applying (2.2) with $k = \delta_G(A)$ and $m = d(G) - 1$, we deduce that

$$\delta_G(A) > \frac{\phi_{L/A}(d(G)-1)}{\phi_L(d(G)-1)\gamma}. \tag{2.3}$$

By [6, Corollary 1.2],

$$\frac{\phi_{L/A}(d(G)-1)}{\phi_L(d(G)-1)} \geq \frac{|A|^{d(G)-1}}{2}. \tag{2.4}$$

Moreover, $A \cong S^n$, where n is a positive integer and S is a nonabelian simple group. In the proof of Lemma 1 in [5], it is shown that

$$\gamma \leq n|S|^{n-1}|\mathrm{Aut}(S)|.$$

Now, [9] shows that $|\mathrm{Out}(S)| \leq \log_2(|S|)$ and hence

$$\gamma \leq n|S|^n \log_2(|S|) \leq |S|^n \log_2(|S|^n) = |A| \log_2(|A|). \tag{2.5}$$

From (2.3), (2.4) and (2.5), we obtain

$$\delta_G(A) > \frac{\phi_{L/A}(d(G)-1)}{\phi_L(d(G)-1)\gamma} \geq \frac{|A|^{d(G)-1}}{2|A| \log_2 |A|} = \frac{|A|^{d(G)-2}}{2 \log_2 |A|}. \qquad \square$$

Recall that $m(G)$ is the largest cardinality of an independent generating set of G.

THEOREM 2.3 [14, Theorem 1.3]. *Let G be a finite group. Then $m(G) \geq a + b$, where a and b are, respectively, the number of non-Frattini and nonabelian factors in a chief series of G. Moreover, if G is soluble, then $m(G) = a$.*

COROLLARY 2.4. *Assume that G is a finite group with a unique minimal normal subgroup A. If A is nonabelian, then $m(G) \geq 3$.*

PROOF. Suppose first that G is simple. Let l be an element of G of order 2. Since $G = \langle l^x \mid x \in G \rangle$, the set $\{l^x \mid x \in G\}$ contains a minimal generating set of G. Since G cannot be generated by two involutions, this minimal generating set has cardinality at least three. Thus, $m(G) \geq 3$.

Suppose next that G is not simple. Let a and b be the number of non-Frattini and nonabelian factors in a chief series of G. As G is not simple, there exists a maximal normal subgroup N of G containing A and we have a chief series $1 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{t-1} \trianglelefteq N_t = G$ with $N_1 = A$ and $N_{t-1} = N$. Then, $a \geq 2$, $b \geq 1$ and $m(G) \geq a + b \geq 3$ by Theorem 2.3. $\square$

https://doi.org/10.1017/S0004972723000126 Published online by Cambridge University Press

3. Proof of the main results

Let G be a finite group, let $d := d(G)$ and let $m := m(G)$. Suppose that $m = d + 1$. Let A be a generating chief factor of G and let $\delta := \delta_G(A)$, $L := L_G(A)$.

3.1. A is nonabelian. First, suppose that $\delta \geq 2$. By Theorem 2.3, $m \geq 2\delta$ and therefore $d \geq 2\delta - 1 \geq 3$. By Proposition 2.2,

$$\delta > \frac{|A|^{d-2}}{2\log_2 |A|} \geq \frac{|A|^{2\delta-3}}{2\log_2 |A|} \geq \frac{60^{2\delta-3}}{2\log_2 60},$$

but this is never true.

Suppose now that $\delta = 1$. In this case, by the main theorem in [13], $d = d(L) = \max(2, d(L/A)) = 2$ and therefore $m = 3$. Since L is an epimorphic image of G, we must have $m(L) \leq 3$. However, $m(L) \geq 3$ by Corollary 2.4. Hence, $m(L) = m = 3$ and therefore it follows from [11, Lemma 11] that $G/\operatorname{Frat}(G) \cong L$. Finally, by Theorem 2.3, $m(L) = 3$ implies $m(L/A) \leq 1$, and this is possible only if L/A is a cyclic p-group. This concludes the proof of Theorem 1.2.

3.2. A is abelian. It follows from Proposition 2.1 and (2.1) that

$$\delta - 1 \leq m - 1 = d = h_G(A) \leq \delta + 1.$$

If $d = \delta - 1$, then $m = \delta$ and this is possible if $G/\operatorname{Frat}(G) \cong A^\delta$. However, in this case, A would be a trivial G-module and therefore $d = h_G(A) = \delta = m$, which is a contradiction.

Now suppose that $d = \delta$. By Theorem 2.3, G is soluble and contains only one non-Frattini chief factor which is not G-isomorphic to A. If A is noncentral in G, then $G/\operatorname{Frat}(G) \cong L_\delta$ and L/A is a cyclic p-group. However, this implies $r_G(A) = 1$, $t_G(A) = 0$ and $d = h_G(A) = \delta + 1$, which is a contradiction. If A is central, then $G/\operatorname{Frat}(G) \cong V \rtimes P$, where P is a finite p-group, V is an irreducible P-module and $d(P) = d$. In particular, we obtain item (1) in Theorem 1.3.

Finally assume $d = \delta + 1$. Notice that in this case, $L = A \rtimes H$, where A is a faithful, nontrivial, irreducible H-module, and

$$m(H) \leq m - \delta = \delta + 2 - \delta = 2.$$

In particular, by Corollary 2.4, H is soluble.

If $m(H) = 2$, then $G/\operatorname{Frat}(G) \cong L_\delta$. In particular, we obtain item (2) in Theorem 1.3.

If $m(H) = 1$, then there exist two normal subgroups N_1 and N_2 of G such that $1 \leq N_1 \leq N_2, G/N_2 \cong L_\delta, N_2/N_1 \leq \operatorname{Frat}(G/N_1)$ and $N_1/\operatorname{Frat}(G)$ is an abelian minimal normal subgroup of $G/\operatorname{Frat}(G)$. As $m(H) = 1$, H is cyclic of prime power order. In particular, we obtain item (3) in Theorem 1.3.

4. Examples for Theorems 1.2 and 1.3

4.1. Monolithic groups: examples for Theorem 1.2. Let G be monolithic primitive with nonabelian socle $N = S_1 \times \cdots \times S_n$, with $S \cong S_i$ for each $1 \leq i \leq n$. The number

https://doi.org/10.1017/S0004972723000126 Published online by Cambridge University Press

$\mu(G) = m(G) - m(G/N)$ has been investigated in [12]. The group G acts by conjugation on the set $\{S_1, \dots, S_n\}$ of the simple components of N. This produces a group homomorphism $G \to \mathrm{Sym}(n)$ and the image K of G under this homomorphism is a transitive subgroup of $\mathrm{Sym}(n)$. Moreover, the subgroup X of $\mathrm{Aut}\, S$ induced by the conjugation action of $\mathbf{N}_G(S_1)$ on the first factor S_1 is an almost simple group with socle S.

By [12, Proposition 4], $\mu(G) \geq \mu(X) = m(X) - m(X/S)$. Assume $m(G) = 3$. Observe that by Theorems 1.1 and 1.2, G/N is cyclic of prime power order. If $X = S$, then

$$\begin{aligned} 3 = m(G) = m(G/N) + \mu(G) \geq m(G/N) + \mu(X) &= m(G/N) + m(S) \\ &\geq m(G/N) + 3. \end{aligned}$$

This implies that $G/N = 1$ and $G = S$ is a simple group. If $X \neq S$, then $G \neq N$ and

$$3 = m(G) \geq m(G/N) + \mu(G) \geq 1 + \mu(X).$$

Moreover, X/S is a nontrivial cyclic group of prime power order, so

$$m(X) = m(X/S) + \mu(X) \leq 1 + \mu(X) \leq 1 + 2 = 3.$$

By Corollary 2.4, $m(X) = 3$.

The groups

$$\mathrm{P\Sigma L}_2(9), M_{10}, \mathrm{Aut}(\mathrm{PSL}_2(7))$$

are currently the only known examples (to the best knowledge of the authors) of almost simple groups X with $X \neq \mathrm{soc}(X)$ and $m(X) = 3$. We believe that there are other such examples, but our current computer codes are not efficient enough to carry out a thorough investigation.

Let $S := \mathrm{PSL}_2(7)$ and $H := \mathrm{Aut}(\mathrm{PSL}_2(7))$, or let $S := \mathrm{PSL}_2(9)$ and $H \in \{\mathrm{P\Sigma L}_2(9), M_{10}\}$. Consider the wreath product $W := H \wr \mathrm{Sym}(n)$. Any element $w \in W$ can be written as $w = \pi(a_1, \dots, a_n)$, with $\pi \in \mathrm{Sym}(n)$ and $a_i \in H$ for $1 \leq i \leq n$. In particular, $N = \mathrm{soc}(W) = S_1 \times \cdots \times S_n = \{(s_1, \dots, s_n) \mid s_i \in S\}$.

PROPOSITION 4.1. *Let G be the subgroup of W generated by $N = \mathrm{soc}(W)$ and $\gamma = \sigma(a, 1, \dots, 1)$, where $\sigma = (1\,2 \cdots n) \in \mathrm{Sym}(n)$ and $a \in H \setminus S$. If $n = 2^t$ for some positive integer t, then $m(G) = 3$.*

In particular, this gives infinitely many examples of nonsimple, nonsoluble groups G with $m(G) = d(G) + 1$ in Theorem 1.2.

PROOF. Suppose that $n = 2^t$ for some positive integer t. Let $r := m(G)$; we aim to prove that $r = 3$.

Let $\{g_1, \dots, g_r\}$ be an independent generating set of G. Observe that

$$\gamma^n = (a, \dots, a) \in G \setminus N$$

and hence G/N is cyclic of order 2^{t+1}. Therefore, relabelling the elements of the independent generating set if necessary, we may assume $G = \langle g_1, N \rangle$. Hence, $g_1 = \sigma(as_1, s_2, \dots, s_n)$ with $s_1, \dots, s_n \in S$. Moreover, for $2 \leq i \leq r$, there exists

https://doi.org/10.1017/S0004972723000126 Published online by Cambridge University Press

$u_i \in \mathbb{Z}$ such that $g_i g_1^{u_i} \in N$. Observe that $\{g_1, g_2 g_1^{u_2}, \ldots, g_r g_1^{u_r}\}$ is still an independent generating set having cardinality r.

Let

$$m = (s_2 \cdots s_n, s_3 \cdots s_n, \ldots, s_{n-1} s_n, s_n, 1) \in N.$$

Then, $Y = \{g_1^m, (g_2 g_1^{u_2})^m, \ldots, (g_r g_1^{u_r})^m\}$ is another independent generating set for G having cardinality r. We have

$$y_1 := g_1^m = \sigma(b, 1, \ldots, 1),$$

with $b = a s_1 \cdots s_n \in \operatorname{Aut} S \setminus S$, and for $2 \le i \le r$, there exist $s_{i1}, \ldots s_{in} \in S$ such that

$$y_i := (g_i g_1^{u_i})^m = (s_{i1}, \ldots, s_{in}).$$

Let $Z := \{b, s_{ij} \mid 2 \le i \le r, 1 \le j \le n\}$ and $T = \langle Z \rangle$. Since $G = \langle y_1, \ldots, y_t \rangle \le T \wr \langle \sigma \rangle$, we must have $\operatorname{Aut}(S) = T$. However, $m(\operatorname{Aut}(S)) = 3$, so $\operatorname{Aut}(S) = \langle b, s_{iu}, s_{jv} \rangle$ for suitable $2 \le i, j \le r$ and $2 \le u, v \le n$.

Let $H := \langle y_1, y_i, y_j \rangle$ and, for $1 \le k \le n$, consider the projection $\pi_k : N \to S$ sending $(s_1, \ldots, s_n)$ to s_k. Notice that $\pi_1(y_1^n) = b, \pi_1((y_i)^{y_1^{1-u}}) = s_{iu}, \pi_1((y_j)^{y_1^{1-v}}) = s_{jv}$. In particular, $\pi_1(H \cap N) = S$ and $H \cap N$ is a subdirect product of $N = S_1 \times \cdots \times S_n$.

Recall that a subgroup D of $N = S_1 \times \cdots \times S_n$ is said to lie fully diagonally in N if each projection $\pi_i : D \to S_i$ is an isomorphism. To each pair (Φ, α), where $\Phi = \{B_1, \ldots, B_c\}$ is a partition of the set $\{1, \ldots, n\}$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\operatorname{Aut} S)^n$, we associate a direct product $\Delta(\Phi, \alpha) = D_1 \times \cdots \times D_c$, where each factor $D_j = \{(x^{\alpha_{i_1}}, \ldots, x^{\alpha_{i_d}}) \mid x \in S\}$ is a full diagonal subgroup of the direct product $S_{i_1} \times \cdots \times S_{i_d}$ corresponding to the block $B_j = \{i_1, \ldots, i_d\}$ in Φ.

Since $H \cap N$ is a subdirect product of N, we must have $H \cap N = \Delta(\Phi, \alpha)$ for a suitable choice of the pair (Φ, α). As $G = \langle H, N \rangle$, the action by conjugation of H on $\{S_1, \ldots, S_n\}$ is transitive and hence the partition $\{B_1, \ldots, B_c\}$ corresponds to an imprimitive system for the permutation action of $\langle \sigma \rangle$ on $\{1, \ldots, n\}$. So there exist $c = 2^\gamma$ and $d = 2^\delta$ with $c \cdot d = n$ such that

$$B_i := \{i, i + c, i + 2c, \ldots, i + (d-1)c\} \quad \text{for } 1 \le i \le c.$$

Notice that $y_1 \in H$ normalises $\Delta(\Phi, \alpha)$. In particular, y_1^c normalises $\Delta(\Phi, \alpha)$. However, y_1^c normalises $L = S_1 \times S_{1+c} \times \cdots \times S_{1+(d-1)c}$ and acts on L as $\pi \cdot l$, where π is the d-cycle $(1, 1 + c, \ldots, 1 + (d-1)c)$ and $l = (b, 1, \ldots, 1) \in L$. In particular, $\pi \cdot l$ normalises the full diagonal subgroup D_1 of L. Therefore, setting $\phi_i = \alpha_{1+(i-1)c}$, for every $s \in S$, there exists $t \in T$ such that

$$(s^{\phi_d b}, s^{\phi_1}, s^{\phi_2}, \ldots, s^{\phi_{d-1}}) = (t^{\phi_1}, t^{\phi_2}, t^{\phi_3}, \ldots, t^{\phi_d}).$$

https://doi.org/10.1017/S0004972723000126 Published online by Cambridge University Press

It follows that

$$\phi_d b \phi_1^{-1} \phi_2 = \phi_1,$$
$$\phi_d b \phi_1^{-1} \phi_3 = \phi_2,$$
$$\cdots$$
$$\phi_d b \phi_1^{-1} \phi_d = \phi_{d-1}.$$

In particular, $(\phi_1 \phi_d^{-1})^d \equiv b^{d-1}$ modulo S. If d is even, then $b \in \langle x^2 \mid x \in \mathrm{Aut}(S)\rangle = S$, against our assumption. Thus, $d = 1$ and hence $c = n$. However, this implies that $H \cap N = N$ and consequently $H = G$. Thus, $m(G) = r \leq 3$. However, $m(G) \geq 3$ by Theorem 2.3. So we conclude that $m(G) = 3$. □

4.2. Soluble groups: examples for Theorem 1.3. We give three elementary examples, but with the same ideas, one can construct more complicated examples. Let S_n be the symmetric group of degree n and let C_n be the cyclic group of order n.

The group $G := S_3 \times C_2^t = C_3 : C_2^{t+1}$ with $t \geq 1$ satisfies $d(G) = t + 1$ and $m(G) = t + 2$. This gives examples of groups satisfying item (1) in Theorem 1.3.

The group $G := S_4 = K : S_3$ with K the Klein subgroup of S_4 and the group $G := (C_3^t : C_2) \times C_2$ with C_2 acting on C_3^t by inversion also satisfy $m(G) = d(G) + 1$. These two examples yield groups satisfying item (2) in Theorem 1.3 with $m(H) = 2$ in the first case and with H abelian in the second case.

As above, let K be the Klein subgroup of S_4 and let $G := K : (S_3 \times C_2^{t-1})$. This gives examples of groups satisfying item (3) in Theorem 1.3.

References

[1] P. Apisa and B. Klopsch, 'A generalization of the Burnside basis theorem', *J. Algebra* **400** (2014), 8–16.
[2] M. Aschbacher and R. Guralnick, 'Some applications of the first cohomology group', *J. Algebra* **90**(2) (1984), 446–460.
[3] S. Burris and H. P. Sankappanavar, *A Course in Universal Algebra*, Graduate Texts in Mathematics, 78 (Springer-Verlag, New York–Berlin, 1981).
[4] F. Dalla Volta and A. Lucchini, 'Finite groups that need more generators than any proper quotient', *J. Aust. Math. Soc. Ser. A* **64** (1998), 82–91.
[5] F. Dalla Volta and A. Lucchini, 'The smallest group with non-zero presentation rank', *J. Group Theory* **2**(2) (1999), 147–155.
[6] E. Detomi and A. Lucchini, 'Probabilistic generation of finite groups with a unique minimal normal subgroup', *J. Lond. Math. Soc. (2)* **87**(3) (2013), 689–706.
[7] S. P. Glasby, 'Classifying uniformly generated groups', *Comm. Algebra* **48**(1) (2020), 101–104.
[8] P. Jiménez-Seral and J. Lafuente, 'On complemented nonabelian chief factors of a finite group', *Israel J. Math.* **106** (1998), 177–188.
[9] S. Kohl, 'A bound on the order of the outer automorphism group of a finite simple group of given order', online note (2003), available at http://www.gap-system.org/DevelopersPages/StefanKohl/preprints/outbound.pdf.
[10] A. Lucchini, 'Generating wreath products and their augmentation ideals', *Rend. Semin. Mat. Univ. Padova* **98** (1997), 67–87.
[11] A. Lucchini, 'The largest size of a minimal generating set of a finite group', *Arch. Math. (Basel)* **101**(1) (2013), 1–8.

[12] A. Lucchini, ‘Minimal generating sets of maximal size in finite monolithic groups’, *Arch. Math. (Basel)* **101**(5) (2013), 401–410.
[13] A. Lucchini and F. Menegazzo, ‘Generators for finite groups with a unique minimal normal subgroup’, *Rend. Semin. Mat. Univ. Padova* **98** (1997), 173–191.
[14] A. Lucchini and P. Spiga, ‘Independent sets of generators of prime power order’, *Expo. Math.* **40**(1) (2022), 140–154.
[15] J. Whiston and J. Saxl, ‘On the maximal size of independent generating sets of $\mathrm{PSL}_2(q)$’, *J. Algebra* **258**(2) (2002), 651–657.

ANDREA LUCCHINI, Dipartimento di Matematica, ‘Tullio Levi-Civita’,
University of Padova, Via Trieste 53, 35121 Padova, Italy
e-mail: lucchini@math.unipd.it

PABLO SPIGA, Dipartimento di Matematica Pura e Applicata,
University of Milano-Bicocca, Via Cozzi 55, 20126 Milano, Italy
e-mail: pablo.spiga@unimib.it