Advances in Group Theory and Applications
© 20xx AGTA - www.advgrouptheory.com/journal
xx (20yy), pp. 1–18 ISSN: 2499-1287
DOI: 10.4399/97888548908l7xx

Invariable generation of groups of finite rank

Eloisa Detomi — Andrea Lucchini — Marta Morigi

(*Received xxx; Accepted xxx — Communicated by xxx*)

Abstract

We prove that the minimal cardinality of an invariable generating set for a finite group G can be bounded in term of the rank of G and we discuss some related questions.

Mathematics Subject Classification (2010): 20F05
Keywords: invariable generators

1 Introduction

Following [9] we say that a subset S of a group G invariably generates G if $G = \langle s^{g(s)} \mid s \in S\rangle$ for every choice of $g(s) \in G$, $s \in S$. Any finite group G contains an invariable generating set (consider a set of representatives of each of the conjugacy classes).

Several papers deal with the question of bounding the minimal cardinality $d_I(G)$ of an invariable generating set for a finite group G together with an analysis of the probability that d independently and uniformly randomly chosen elements of G invariably generate G with good probability (see for example [5], [6], [7], [9], [10], [14], [15], [16], [18], [20], [21], [22]).

Clearly $d_I(G)$ is not less than the minimal cardinality $d(G)$ of a generating set of the finite group G. On the other hand, it follows from [15, Proposition 2.5] and [7, Theorem 1] that the difference $d_I(G) - d(G)$ can be arbitrarily large. Many results in the literature provide bounds for $d(G)$ in relation with different structural properties of G. In this paper we review some of these results and we discuss to which extent we can expect comparable results on the smallest cardinality $d_I(G)$ of an invariable generating set. Moreover, we provide a bound to $d_I(G)$ in the case where G has finite rank.

Theorem 1 *Let G be a finite group of rank d. Then $d_I(G) \leqslant 2d^2 + (13/4)d - 2$.*

We don't know how sharp the previous bound is and it particular we leave the question open whether a linear bound of $d_I(G)$ in terms of the rank $\mathrm{rk}(G)$ of G can be proved. In any case the difference $d_I(G) - \mathrm{rk}(G)$ can be arbitrarily large: for any $d \in \mathbb{N}$ there exists a finite supersoluble group G with $\mathrm{rk}(G) = d$ and $d_I(G) - \mathrm{rk}(G) = d - 1$ (Proposition 16).

The invariants $d(G)$, $d_I(G)$, $\mathrm{rk}(G)$ can be defined also for profinite groups. In this case generation and invariable generation are interpreted topologically, and these numbers can also be infinite. Theorem 1 immediately implies the following result.

Corollary 2 *If a profinite group G has finite rank d, then G is finitely invariably generated and $d_I(G) \leqslant 2d^2 + (13/4)d - 2$.*

In 1989, Guralnick [13] and Lucchini [17] independently proved that if all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d + 1$ elements. We will show that there exists a supersoluble group G whose Sylow subgroups are d-generated but $d_I(G) = 2d - 1$ (Proposition 16). But the question of a bound on $d_I(G)$ as a function only of d, when every Sylow subgroup is d-generated, is still open in the general case.

Families of groups generated by 2 elements but requiring an increasing large number of elements to be invariably generated have been constructed in [15] as a direct product of alternating groups. In [18], an analogous family of soluble groups has been constructed as a wreath product of cyclic groups of prime order, for different primes. In the language of profinite groups, these results allow to construct examples of profinite groups that can be generated by 2 elements but are not finitely invariably generated. The examples of 2-generated prosoluble groups that are not finitely invariably generated given in [7] and [18] have the following properties: they are not soluble, their rank is infinite and their order (as a supernatural number) is divisible by infinitely many primes. The first two properties are unavoidable, respectively by [7, Theorem 2] and Corollary 2, but it is not clear whether it could be possible to construct 2-generated prosoluble groups that are not finitely invariably generated and whose order is divisible by only finitely many primes. By [7, Theorem 2], for every positive integer l, there exists a finite soluble group G with derived length l and $d_I(G) \geqslant l$. We suspect that, for every l, there exists also a finite $\{2,3\}$-group G with derived length l and $d_I(G) \geqslant l$ (this would implies that the free pro-$\{2,3\}$ group of rank 2 is not finitely invariably generated). As a small contribute to the problem, in the last section of the paper we provide the construction of a 2-generated group G or order $2^{14} \cdot 3^{84}$, derived length 4, and $d_I(G) \geqslant 4$.

2 Some results on generation and invariable generation

In the sequel, $\lceil x \rceil$ denotes the smallest integer greater or equal to x and $d(G)$ the minimal size of a generating set of a group G. 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 [2] 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 3 *[3, Proposition 6] Let L be a primitive monolithic group with abelian socle A, and let L_t be the crown-based power of L of size t. Define*

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

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

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

In [4, Proposition 9] it is shown that for every non Frattini chief factor A of a finite group G there exist an integer t_A and a primitive monolithic group L_A such that the crown based power $(L_A)_{t_A}$, but not $(L_A)_{t_A+1}$, is an homomorphic image of G. Whenever A is abelian, t_A is precisely the number $\delta_G(A)$ of the chief factors G-isomorphic to A and complemented in an arbitrary chief series of G. Moreover, when G is soluble, $s_L(A) = 0$ by the following unpublished result by Gaschütz (see [23, Lemma 1]).

Lemma 4 *Let H be a finite soluble group and let V be a faithful irreducible G-module. Then $H^1(H, V) = 0$.* Therefore, if G is a finite soluble group, by [2, Theorem 1.4] and Theorem 3 we recover the following formula due to Gaschütz [12].

Proposition 5 *Let G be a finite soluble group. For every irreducible G-module V define $r_G(V) = \dim_{\mathrm{End}_G(V)} V$, set $\theta_G(V) = 0$ if V is a trivial G-module, and $\theta_G(V) = 1$ otherwise, and let $\delta_G(V)$ be the number of the chief factors G-isomorphic to V and complemented in an arbitrary chief series of G. Then*

$$d(G) = \max_V \left(\theta_G(V) + \left\lceil \frac{\delta_G(V)}{r_G(V)} \right\rceil \right)$$

where V ranges over the set of non G-isomorphic complemented chief factors of G.

When G is an arbitrary finite group, from Theorem 3 we deduce the following bound for $d(G)$.

Corollary 6 *Let G be a finite group. Then*

$$d(G) \geqslant \max_V \left(\theta_G(V) + \left\lceil \frac{\delta_G(V)}{r_G(V)} \right\rceil \right)$$

where V ranges over the set of non G-isomorphic complemented abelian chief factors of G, $\delta_G(V)$ is the number of the complemented chief factors which are G-isomorphic to V in an arbitrary chief series of G and $r_G(V) = \dim_{\mathrm{End}_G(V)} V$.

Proof — Let V be a complemented abelian chief factors of G. Then by [4, Proposition 9] there exists a primitive monolithic group L, with $\mathrm{soc}(L) \cong V$, such that L_t is an homomorphic image of G and $t = \delta_G(V)$. By Theorem 3 we have that

$$d(G) \geqslant d(L_t) \geqslant \theta + \left\lceil \frac{t + s_L(A)}{r_L(A)} \right\rceil \geqslant \theta + \left\lceil \frac{t}{r_L(A)} \right\rceil$$

and the result follows. □

Let us now consider invariable generation and denote by $d_I(G)$ the minimal size of an invariable generating set of a group G. In this contest, even the more natural relations between sets of generators fail. For example notice that $\mathrm{Sym}(4)$ is invariably generated by the two elements $a = (1, 2, 3, 4)$

and $b = (1,3,2)$, but is not invariably generated by the set $\{ab, b\}$, since $ab = (3,4)$ is conjugate to $(1,3)$ and $\langle (1,3), b\rangle \neq \mathrm{Sym}(4)$.

Clearly, if N is a normal subgroup of G, then $d_I(G/N) \leqslant d_I(G)$. When N is a normal abelian subgroup of G, $d_G(N)$ denotes the minimal number of generators of N as a G-module. The Frattini subgroup of a group G is denoted by $\mathrm{Frat}(G)$. Recall that a subset of G generates G if and only if its image in $G/\mathrm{Frat}(G)$ generates $G/\mathrm{Frat}(G)$. We collect in the following lemma some basic results on invariable generation.

Lemma 7 *Let N be a normal subgroup of a group G.*

1. $d_I(G) \leqslant d_I(G/N) + d_I(N)$.
2. *If N is abelian, then $d_I(G) \leqslant d_I(G/N) + d_G(N)$.*
3. *If N is a minimal normal subgroup, then $d_I(G) \leqslant d_I(G/N) + c$, where $c = 1$ if N is abelian and $c = 2$ if N is non-abelian.*
4. *If $N \leqslant \mathrm{Frat}(G)$, then $d_I(G) = d_I(G/N)$.*

Proof — Parts (1) and (2) follow from the proofs of [16, Lemma 2.8] and [16, Lemma 2.10], respectively. Part (3) is Theorem 3.1 in [15]. Part (4) follows immediately from the above mentioned property of $\mathrm{Frat}(G)$. □

The minimal number $d_G(N)$ of generators of a G-module is given by the following lemma.

Lemma 8 *[7, Lemma 11] Let G be a finite group. Assume that N is a direct product*

$$N = A_1^{n_1} \times \ldots \times A_r^{n_r}$$

where, for each i, A_i is a finite elementary abelian p_i-group for a prime number p_i, A_i is an irreducible $\mathbb{F}_{p_i} G$-module and A_i is not G-isomorphic to A_j for $i \neq j$. Then the minimal number of elements needed to generate N as G-module is

$$d_G(N) = \max_{i\in\{1,\dots,r\}} \left(\left\lceil \frac{n_i}{r_G(A_i)} \right\rceil \right),$$

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

The main main tool in the study of $d(G)$ is the following result, known as Gaschütz's Lemma.

Lemma 9 *[11] Let N be a normal subgroup of a finite group G and suppose $\langle g_1N, \dots, g_dN\rangle = G/N$. If $d \geqslant d(G)$, then we can find $n_1, \dots, n_d \in N$ such that $\langle g_1n_1, \dots, g_dn_d\rangle = G$.*

Unfortunately the analogous of Gaschütz's Lemma for invariable generation is false: for example $\mathrm{Sym}(3)/\mathrm{Alt}(3)$ is invariably generated by $(1,2)\,\mathrm{Alt}(3)$

and $(1,3)\,\mathrm{Alt}(3)$, but there is no pair of invariable generators x, y of $\mathrm{Sym}(3)$ with $\{x,y\} \cap \mathrm{Alt}(3) = \emptyset$. The only available criterion in order to decide whether an invariable generating set of a quotient group G/N can be lifted to G is given in [5, Proposition 8] and holds only in the case where N is abelian. To formulate this result, we need to recall some notation from [5]. Let H be a finite group acting faithfully and irreducibly on an elementary abelian finite p-group V. For a positive integer u we consider the semidirect product $V^u \rtimes H$: Unless otherwise stated, we assume that the action of H is diagonal on V^u, that is, H acts in the same way on each of the u direct factors.

Proposition 10 *[5, Proposition 8] Suppose that* $h_1, \dots, h_d$ *invariably generate* H *and that* $H^1(H,V) = 0$. *Let* $w_1, \dots, w_d \in V^u$ *with* $w_i = (w_{i,1}, \dots, w_{i,u})$. *For* $j \in \{1, \dots, u\}$, *consider the vectors*

$$r_j = \big(\pi_j(w_1), \dots, \pi_j(w_d)\big) = (w_{1,j}, \dots, w_{d,j}) \in V^d.$$

Then $h_1w_1, h_2w_2, \dots, h_dw_d$ *invariably generate* $V^u \rtimes H$ *if and only if the vectors* $r_1, \dots, r_u$ *are linearly independent modulo*

$$W = \{(u_1, \dots, u_d) \in V^d \mid u_i \in [h_i, V],\ i = 1, \dots, d\}.$$

In particular, there exist $w_1, \dots, w_d \in V^u$ *such that* $h_1w_1, h_2w_2, \dots, h_dw_d$ *invariably generate* $V^u \rtimes H$ *if and only if*

$$u \leqslant \sum_i \dim_{\mathrm{End}_H(V)} C_V(h_i).$$

By Gaschütz's Lemma, if the set $\{g_1, \dots, g_{d(G/N)}\}$ generates G modulo N, then there exist $d(G)$ elements n_i in N such that

$$\langle g_1n_1, \dots, g_{d(G/N)}n_{d(G/N)}, n_{d(G/N)+1}, \dots, n_{d(G)} \rangle = G.$$

So there always exists a generating set with $d(G) - d(G/N)$ elements belonging to N. Also the analogous of this sentence for invariable generation is false, as it is indicated by the following result.

Lemma 11 *There exist a finite group* G *and a normal subgroup* N *of* G *such that there is no invariable generating set of* G *of size* $d_I(G)$ *with* $d_I(G) - d_I(G/N)$ *elements in* N.

Proof — Let $H = \langle a, b\rangle \cong C_2 \times C_2$ and let $V_1 = \langle \gamma \rangle \cong C_3$, $V_2 = \langle \delta \rangle \cong C_3$.

Consider the semidirect product

$$G = (V_1 \times V_2) \rtimes H \cong \mathrm{Sym}(3) \times \mathrm{Sym}(3)$$

with $\gamma^a = \gamma^{-1}$, $\gamma^b = \gamma$, $\delta^a = \delta$, $\delta^b = \delta^{-1}$. Assume that $X = \{x_1, x_2\}$ is a generating set for H. Clearly $x_i \neq 1$ and, since H is abelian, X is also an invariable generating set. By Proposition 10 and Lemma 4, there exist elements $w_1, w_2 \in V_1 \times V_2$ such that $\langle x_1 w_1, x_2 w_2 \rangle$ invariably generates G if and only if

$$1 \leqslant \dim C_{V_1}(x_1) + \dim C_{V_1}(x_2) \text{ and } 1 \leqslant \dim C_{V_2}(x_1) + \dim C_{V_2}(x_2)$$

i.e. if and only if

$$X \cap C_H(V_1) \neq \emptyset \text{ and } X \cap C_H(V_2) \neq \emptyset.$$

Since $C_H(V_1) = \langle b \rangle$ and $C_H(V_2) = \langle a \rangle$ it must be $X = \{a, b\}$. It follows that any pair of invariable generators of G is of the form (aw_1, bw_2), for suitable $w_1, w_2 \in V_1 \times V_2$, and $d_I(G) = 2$.

Now let $N = (V_1 \times V_2) \rtimes \langle ab \rangle$. We have $d_I(G) = 2$ and $d_I(G/N) = 1$, however a pair of invariable generators does not contain elements of N. □

3 Invariable generation of groups of finite rank

Theorem 3.1 in [15] (see Lemma 7) states that if a finite group G has a chief series with a abelian factors and b non-abelian factors then $d_I(G) \leqslant a + 2b$. If G is soluble, Proposition 12 in [7] gives the bound $d_I(G) \leqslant l(d(G) - 1) + 1$, where l is the derived length of G. Whenever we can control the nilpotent factors on a normal series of a, not necessarily soluble, group G, we can also use the following bound.

Proposition 12 *Let* G *be a finite* d*-generated group having a normal series with* l *nilpotent factors,* a *abelian chief factors and* b *non-abelian chief factors. Then* $d_I(G) \leqslant l(d-1) + a + 2b + 1$.

Proof — The proof is by induction on $|G|$, the case $|G| = 1$ being trivial.

Suppose $|G| > 1$ and let $\{N_i\}_{i \geqslant 0}$ be a normal series of G with l nilpotent factors, a abelian chief factors and b non-abelian chief factors.

If $\mathrm{Frat}(G) \neq 1$, then we consider the series $\{N_i \mathrm{Frat}(G)/\mathrm{Frat}(G)\}_{i \geqslant 0}$ of the factor group $G/\mathrm{Frat}(G)$: this series has at most l nilpotent factors, a abelian chief factors and b non-abelian chief factors. By induction and Lemma 7, $d_I(G) = d_I(G/\mathrm{Frat}(G)) \leqslant l(d-1) + a + 2b + 1$.

So we assume $\mathrm{Frat}(G) = 1$.

Let $N = N_1 \trianglelefteq G$ be the last non-trivial term of the normal series $\{N_i\}_{i \geqslant 0}$.

If N is a chief factor, then by Lemma 7 we get that $d_I(G) \leqslant d_I(G/N) + 1$ if N is abelian, or $d_I(G) \leqslant d_I(G/N) + 2$ if N is non-abelian, and then we apply induction to G/N to obtain the desired bound.

Assume now that N is nilpotent. As $\mathrm{Frat}(N) \leqslant \mathrm{Frat}(G) = 1$, N is abelian. Actually, N is a direct product of complemented minimal normal subgroups of G and we can write $N = A \times B$ where

$$A = A_1^{n_1} \times \ldots \times A_r^{n_r}, \quad B = A_{r+1}^{n_{r+1}} \times \ldots \times A_s^{n_s}$$

where each A_i is an elementary abelian p_i-group, for a prime number p_i, A_i is an irreducible $\mathbb{F}_{p_i}$ G-module and A_i is not G-isomorphic to A_j for $i \neq j$; in particular we assume that A_i is a trivial G-module if and only if $i \geqslant r + 1$.

Note that G/N has a normal series (namely $\{N_i/N\}_{i \geqslant 1}$) with $l - 1$ nilpotent factors, a abelian chief factors and b non-abelian chief factors. If $l = 1$, then we apply Theorem 3.1 in [15] (see Lemma 7) to get that $d_I(G/N) \leqslant a + 2b$. By Lemma 8

$$d_G(N) = \max_{i \in \{1,\ldots,s\}} \left(\left\lceil \frac{n_i}{r_G(A_i)} \right\rceil \right). \tag{0.1}$$

On the other hand, by Proposition 6,

$$d \geqslant d(G) \geqslant \max_{V} \left(\theta_G(V) + \left\lceil \frac{\delta_G(V)}{r_G(V)} \right\rceil \right) \tag{0.2}$$

where V ranges over the set of non G-isomorphic complemented chief factors of G. Since $n_i \leqslant \delta_G(A_i)$, by (0.1) and (0.2) we deduce that

$$d \geqslant \max_{i \in \{1,\ldots,s\}} \left(\left\lceil \frac{n_i}{r_G(A_i)} \right\rceil \right) = d_G(N)$$

hence $d_G(N) \leqslant d$. Then by Lemma 7 we obtain

$$d_I(G) \leqslant d_I(G/N) + d_G(N) \leqslant a + 2b + d \tag{0.3}$$

which is the desired bound when $l = 1$.

Assume now that $l > 1$. Since $B \cong_G N/A$ is a product of trivial G-modules and it is complemented since $\mathrm{Frat}(G) = 1$, we have $G/A \cong G/N \times N/A$. Since $l > 1$, the group G/A has again a normal series with $l - 1$

nilpotent factors, a abelian chief factors and b non-abelian chief factors, namely,

$$1 \leqslant \frac{N_2}{N} \leqslant \ldots \leqslant \frac{N_i}{N} \leqslant \frac{N_{i+1}}{N} \times \frac{N}{A} \leqslant \frac{N_{i+2}}{N} \times \frac{N}{A} \leqslant \ldots \leqslant \frac{G}{N} \times \frac{N}{A}$$

where i is the smallest positive integer such that N_{i+1}/N_i is nilpotent. Therefore, by induction,

$$d_I(G/A) \leqslant (l-1)(d-1) + a + 2b + 1. \tag{0.4}$$

By Lemma 8

$$d_G(A) = \max_{i \in \{1,\ldots,r\}} \left(\left\lceil \frac{n_i}{r_G(A_i)} \right\rceil \right). \tag{0.5}$$

Note that by the definition of A, we have $\theta_G(A_i) = 1$ for every $i \leqslant r$. Since $n_i \leqslant \delta_G(A_i)$, by (0.5) and (0.2) we deduce that

$$d \geqslant \max_{i \in \{1,\ldots,r\}} \left(1 + \left\lceil \frac{n_i}{r_G(A_i)} \right\rceil \right) = 1 + d_G(A)$$

hence $d_G(A) \leqslant d - 1$. Then, by Lemma 7 and (0.4), we obtain

$$\begin{aligned} d_I(G) &\leqslant d_I(G/A) + d_G(A) \leqslant (l-1)(d-1) + a + 2b + 1 + (d-1) \\ &= l(d-1) + a + 2b + 1 \end{aligned}$$

which gives the desired bound. □

The next two results will be needed in the proof of Theorem 1.

Theorem 13 *[6, Theorem 1] Let* G *be a subgroup of* Sym(n)*; then either* $G = \mathrm{Sym}(3)$ *and* $d_I(G) = 2$ *or* $d_I(G) \leqslant \lfloor n/2 \rfloor$.

Theorem 14 *[8, Theorem 6.2A] Let* G *be a soluble subgroup of* GL($n, \mathbb{F}$)*. Then the derived length of* G *is at most* $2n$.

Now we are ready to prove Theorem 1.

Proof — [Proof of Theorem 1] Since $d_I(G) = d_I(G/\operatorname{Frat}(G))$, without loss of generality, we can assume $\operatorname{Frat}(G) = 1$. In this case, the Fitting subgroup F of G is a direct product of abelian minimal normal subgroups of G, say

$$F = N_1 \times \ldots \times N_t$$

where each N_i is an elementary abelian p_i-group of rank at most d.

Let $R = R(G)$ be largest soluble normal subgroup of G, and consider its homomorphic images $H_i = R/C_R(N_i)$, for $i = 1, \ldots t$. Every H_i is isomorphic to a soluble linear group acting on N_i, where N_i is a vector space of dimension at most d, and thus, by Theorem 14, the derived length of each H_i is bounded by $2d$. Therefore, $R/\cap_{i=1}^{t} C_R(N_i)$ has derived length at most $2d$. Since $C = \cap_{i=1}^{t} C_R(N_i)$ is a soluble normal subgroup of $C_G(F)$, we have that $C \leqslant F$ (see e.g. [1, 31.9]) hence

$$\mathrm{dl}(R/F) \leqslant 2d,$$

where $\mathrm{dl}(R/F)$ denoted the derived length of R/F.

Let now T be a normal subgroup of G such that T/R is the socle of G/R. Since R is the largest soluble normal subgroup of G, T/R is a direct product of non-abelian minimal normal subgroups of G/R, say

$$T/R = M_1 \times \cdots \times M_r$$

where $M_i \cong S_i^{r_i}$ for some simple non-abelian group S_i and some integer r_i. Since a Sylow 2-subgroup P_i of a non-abelian simple group S_i is not cyclic, the number of generators of $\prod_{i=1}^{r} P_i^{r_i}$ is at least $2(\sum_{i=1}^{r} r_i)$, hence

$$\sum_{i=1}^{r} r_i \leqslant d/2.$$

Now, for each $1 \in \{1, \dots r\}$, $(G/R)/C_{G/R}(M_i)$ is isomorphic to a subgroup of $K_i = \mathrm{Aut}(S_i) \wr \mathrm{Sym}(r_i)$, and $\cap_{i=1}^{r} C_{G/R}(M_i) \leqslant T/R$ (see e.g. [1, 31.13]), hence $G/T \leqslant \prod_{i=1}^{r} K_i/T \leqslant \prod_i \mathrm{Out}(S_i) \wr \mathrm{Sym}(r_i)$. Call $\overline{G} = G/T$ and let L be a subgroup of G containing T and such that

$$L/T = \overline{L} = \overline{G} \cap \prod_{i=1}^{r} \mathrm{Out}(S_i)^{r_i}.$$

As $\mathrm{dl}(\mathrm{Out}(S_i)) \leqslant 3$, we have that $\overline{L}$ is soluble of derived length at most 3.

Finally, $\overline{G}/\overline{L}$ is isomorphic to a subgroup of $\prod_{i=1}^{r} \mathrm{Sym}(r_i)$ and hence it is a permutation group of degree $\sum_{i=1}^{r} r_i \leqslant d/2$. By Theorem 13 a permutation group of degree m can be invariably generated by $\lceil m/2 \rceil$ elements, hence $d_I(G/L) \leqslant d_I(\overline{G}/\overline{L}) \leqslant \lceil d/4 \rceil$.

Summing up, we have found a normal series in G

$$1 \leqslant F \leqslant R \leqslant T \leqslant L \leqslant G$$

such that F is nilpotent, R/F is soluble with $\mathrm{dl}(R/F) \leqslant 2d$, T/R has a series of at most $\lfloor d/2 \rfloor$ non-abelian chief factors, L/T is soluble with $\mathrm{dl}(L/T) \leqslant$

3, and $d_I(G/L) \leqslant d/4$. In particular, L has a normal series with at most $1+(2d+3)$ nilpotent factors and $\lfloor d/2 \rfloor$ non-abelian chief factors. Hence, by Proposition 12 it follows that

$$d_I(L) \leqslant (2d+4)(d-1)+2\lfloor d/2 \rfloor+1 \leqslant 2d^2+3d-3.$$

Since $d_I(G) \leqslant d_I(G/L)+d_I(L)$ (see e.g. [6, Lemma 2]), we conclude that

$$d_I(G) \leqslant \lceil d/4 \rceil+2d^2+3d-3 \leqslant 2d^2+\frac{13}{4}d-2,$$

as required. □

In 1989, R. Guralnick [13] and Lucchini [17] independently proved that if all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements. So a natural question is the following:

Question 1 *If all the Sylow subgroups of a finite group* G *can be generated by* d *elements, is it possible to bound* $d_I(G)$ *as a function of* d*?*

The following result shows that we can bound $d_I(G)$ as a function of d and the number of the distinct prime divisors of $|G|$.

Proposition 15 *Let* G *be a finite group and assume that every Sylow subgroup of* G *can be generated by* d *elements. If* n *is the number of the distinct prime divisor of* $|G|$*, then* $d_I(G) \leqslant (n+1)d$*. In particular, if* G *is soluble, then* $d_I(G) \leqslant nd$.

Proof — Fix a chief series of G and denote by a_p the number of complemented chief factors of order a power of p and by b the number of non-abelian chief factors. By [19, Lemma 4], we have that $a_p \leqslant d$ and $a_2+b \leqslant d$. By Lemma 7 we deduce that

$$d_I(G) \leqslant \sum_{p\neq 2} a_p+a_2+2b \leqslant (n-1)d+2d=(n+1)d.$$

If G is soluble, that is $b=0$, then by Lemma 7 we have that $d_I(G) \leqslant \sum_p a_p \leqslant nd$. □

Question 1 has a positive answer in the particular case of finite supersoluble groups. Indeed if G is supersoluble, then, by [7, Theorem 3], $d_I(G) \leqslant 2d(G)-1$. If every Sylow subgroup of G is d-generated, then by the theorem of Guralnick and Lucchini, $d(G) \leqslant d+1$, so we conclude $d_I(G) \leqslant 2d+1$. However the next result shows that even in the case of supersoluble groups, we cannot have $d_I(G) \leqslant d+1$.

Proposition 16 *For every* $d \in \mathbb{N}$ *there exists a finite supersoluble group* G *such that the rank of* G *is* d *and* $d_I(G) = 2d-1$.

Proof — Let $K = C_2^d$. There are $\alpha = 2^d - 1$ different epimorphisms $\sigma_1, \dots, \sigma_\alpha$ from K to C_2 ($\sigma_i : K \to C_2$ is uniquely determined by $M_i = \ker \sigma_i$, a $(d-1)$-dimensional subspace of K). Assume that $p_1, \dots, p_\alpha$ are different odd prime numbers. For each i, consider the $\mathbb{F}_{p_i}K$-module V_i defined as follows: $V_i \cong C_{p_i}$ and $v_i^k = v_i$ if $k \in M_i$, $v_i^k = v_i^2$ otherwise. Let $W_i = V_i^{d-1}$ and consider $G = \left(\prod_{1 \leqslant i \leqslant \alpha} W_i\right) \rtimes K$. The group G is supersoluble and it is easy to see that every subgroup of G is d-generated. Now assume that $g_1, \dots, g_r$ invariably generate G, where $r = d_I(G)$. We write $g_i = (w_{i1}, \dots, w_{i\alpha})k_i$ with $k_i \in K$ and $w_{ij} \in W_j$. In particular $k_1, \dots, k_r$ generate K and, up to reordering the elements $g_1, \dots, g_r$, we can assume that the first d-elements $k_1, \dots, k_d$ are a basis for K. Let $M = \langle k_1^{-1}k_2, \dots, k_{d-1}^{-1}k_d \rangle$. It can be easily checked that M is a maximal subgroup of K, so $M = M_j$ for some $j \in \{1, \dots, \alpha\}$. Moreover $k_i \notin M_j$ for every $i \in \{1, \dots, d\}$, in particular $C_{V_j}(k_i) = 0$ for every $i \in \{1, \dots, d\}$. On the other hand $w_{1j}k_1, \dots, w_{rj}k_r$ invariably generate G, so, by [7, Corollary 7],

$$d - 1 \leqslant \sum_{1 \leqslant i \leqslant r} \dim_{\mathbb{F}_{p_j}} C_{V_j}(k_i) = \sum_{d+1 \leqslant i \leqslant r} \dim_{\mathbb{F}_{p_j}} C_{V_j}(k_i) \leqslant r - d.$$

Hence $d_I(G) = r \geqslant 2d - 1$. On the other hand, it follows from [7, Theorem 3] that a supersoluble d-generated finite group is invariably generated by $2d-1$ elements. Therefore $d_I(G) = 2d - 1$. □

4 An Example

Families of groups generated by 2 elements but requiring an increasing large number of elements to be invariably generated have been constructed in [15] and in [18], actually as a direct product of alternating groups and as a wreath product of cyclic groups, respectively. In both cases, it is necessary to increase the number of the primes dividing $|G|$ to make $d_I(G)$ bigger. So another natural question arises:

Question 2 *Is it possible to bound* $d_I(G)$ *only as a function of* $d(G)$ *and of the primes, or the number of primes, dividing* $|G|$*?*

In this section we will build a 2 generated group, whose order is divided by only two primes, such that 3 elements are not sufficient to invariably generate G. The only intent of this example is to show how complicated is to control the number of invariable generators with the only aid of Proposition 10.

We start with $H_1 = C_2 \times C_2$, the direct product of two copies of a cyclic group of order 2. This group has precisely 3 homomorphic images which are isomorphic to C_2, hence we can define 3 different actions of H_1 on C_3, the cyclic group of order 3. With respect to these 3 actions, we define the semidirect product

$$G_1 = C_3^3 \rtimes H_1.$$

Actually, G_1 is the group constructed in Proposition 14 of [7] for $d = 2$, so $d(G_1) = 2$ and $d_I(G_1) = 3$.

We can identify G_1 with the subgroup of $\mathrm{Sym}(3) \times \mathrm{Sym}(3) \times \mathrm{Sym}(3) \leqslant \mathrm{Sym}(9)$ consisting of even permutations. Note that G_1 is a subdirect product of $\mathrm{Sym}(3)^3$ and there are three different epimorphisms

$$\pi_i : G_1 \to \mathrm{Sym}(3),$$

for $i = 1, 2, 3$, obtained by factoring out $G_1 \cap (\mathrm{Sym}(3) \times \mathrm{Sym}(3) \times 1)$, $G_1 \cap (1 \times \mathrm{Sym}(3) \times \mathrm{Sym}(3))$ and $G_1 \cap (\mathrm{Sym}(3) \times 1 \times \mathrm{Sym}(3))$ respectively.

Let g_1, g_2, g_3 be invariable generators of G_1 and assume that

$$g_i = (\sigma_{i1}, \sigma_{i2}, \sigma_{i3})$$

for $i \in \{1, 2, 3\}$. Since $\pi_i(g_1), \pi_i(g_2), \pi_i(g_3)$ invariably generate $\mathrm{Sym}(3)$, for every i, each column of the following matrix (whose rows are the components of the g_i's)

$$\begin{pmatrix} \sigma_{11} & \sigma_{12} & \sigma_{13} \\ \sigma_{21} & \sigma_{22} & \sigma_{23} \\ \sigma_{31} & \sigma_{32} & \sigma_{33} \end{pmatrix}$$

must contain at least one element of order 2 (that is, an odd permutation) and one element of order 3 (that is, an even permutation). On the other hand, each row of the matrix corresponds to some g_i, which is an even permutation, so in at least one column we have two odd permutations. We may assume that the first column contains two odd permutations. Moreover, we can replace any invariable generator with one of its conjugates, so we may assume that

$$\pi_1(g_1) = \sigma_{11} = (1, 2), \quad \pi_1(g_2) = \sigma_{21} = (1, 2), \quad \pi_1(g_3) = \sigma_{31} = (1, 2, 3).$$

The group S_3 acts naturally on the module

$$I = \{(a_1, a_2, a_3) \in {\mathbb{F}_2}^3 \mid a_1 + a_2 + a_3 = 0\}$$

by permuting the indices, so that I is an absolutely irreducible Sym(3)-module. For each $i = 1, 2, 3$, the epimorphism $\pi_i : G \to \mathrm{Sym}(3)$ makes I into an absolutely irreducible G-module I_i and the three modules I_1, I_2, I_3 are non-isomorphic to each other, because they have different centralizers. Consider the group

$$H_2 = (I_1^2 \times I_2^2 \times I_3^2) \rtimes G_1$$

where the action on I_i^2 is diagonal. Since $\delta_{H_2}(I_i) = 2$, by Proposition 5 the group H_2 is again 2-generated. We will call

$$\tilde{\pi}_i : H_2 \to I^2 \rtimes \mathrm{Sym}(3)$$

the projection induced by $\pi_i : G_1 \to \mathrm{Sym}(3)$.

Assume that $\tilde{g}_1, \tilde{g}_2, \tilde{g}_3$ are invariable generators of H_2 that projects into g_1, g_2, g_3. Then their images under the first projection $\tilde{\pi}_1$

$$y_i = \tilde{\pi}_1(\tilde{g}_i),$$

invariably generate $I^2 \rtimes \mathrm{Sym}(3)$. Moreover, y_1, y_2, y_3 are lifts of the generators $\sigma_{i1} = \pi_1(g_i)$, $i = 1, 2, 3$, to $\tilde{\pi}_1(H_2) = I^2 \rtimes \mathrm{Sym}(3)$. We now apply Proposition 10 to obtain some information on y_1, y_2, y_3.

Let us fix the vectors $v_1 = (1, 1, 0)$ and $v_2 = (0, 1, 1)$ as a basis of I over $\mathbb{F}_2$. Let $W_i = \mathrm{Im}(\sigma_{i1} - 1)$. Then

$$W_1 = W_2 = \langle v_1 \rangle, \quad W_3 = \langle v_1, v_1 + v_2 \rangle = I.$$

Since each y_i is a lift of σ_{i1} to $I^2 \rtimes \mathrm{Sym}(3)$, we can write

$$\begin{aligned} y_1 &= (12)(a_{11}v_1 + a_{12}v_2, b_{11}v_1 + b_{12}v_2), \\ y_2 &= (12)(a_{21}v_1 + a_{22}v_2, b_{21}v_1 + b_{22}v_2), \\ y_3 &= (123)(a_{31}v_1 + a_{32}v_2, b_{31}v_1 + b_{32}v_2), \end{aligned}$$

for some $a_{i,j}, b_{i,j} \in \mathbb{F}_2$. Consider the matrix whose first rows form a basis of $W = W_1 \oplus W_2 \oplus W_3$ and the last two rows are the vectors r_1, r_2 defined in Proposition 10:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ a_{11} & a_{12} & a_{21} & a_{22} & a_{31} & a_{32} \\ b_{11} & b_{12} & b_{21} & b_{22} & b_{31} & b_{32} \end{pmatrix}.$$

Since y_1, y_2, y_3 invariably generate $I^2 \rtimes \mathrm{Sym}(3)$, by Proposition 10 the matrix A is invertible, that is, the submatrix

$$A' = \begin{pmatrix} a_{12} & a_{22} \\ b_{12} & b_{22} \end{pmatrix}$$

is invertible. Consider the three epimorphisms

$$\varphi_i : I^2 \rtimes \mathrm{Sym}(3) \to I \rtimes \mathrm{Sym}(3)$$

obtained by factoring out the first copy of I, the second copy of I and the diagonal in I^2, respectively. The condition on A' implies that either one of the rows of A' is equal to $(1,1)$ or $a_{12} + b_{12} = a_{22} + b_{22} = 1$. Therefore for at least one $j \in \{1,2,3\}$ we have that

$$\begin{aligned} \varphi_j(y_1) &= (1,2)(\alpha_1 v_1 + v_2) \\ \varphi_j(y_2) &= (1,2)(\alpha_2 v_1 + v_2). \end{aligned} \tag{0.6}$$

Note that

$$J = \mathbb{F}_3^3$$

is an absolutely irreducible $I \rtimes \mathrm{Sym}(3)$-module, with the action defined by:

$$(b_1, b_2, b_3)^{(a_1,a_2,a_3)\sigma} = (b_{\sigma(1)}^{a_{\sigma(1)}}, b_{\sigma(2)}^{a_{\sigma(2)}}, b_{\sigma(3)}^{a_{\sigma(3)}}),$$

where $b_i^{a_i} = -b_i$ if $a_i \neq 1$ and $b_i^{a_i} = b_i$ otherwise.

Combining the three maps φ_i with the three projections π_j of H_2 to $I^2 \rtimes \mathrm{Sym}(3)$, we get 9 epimorphisms $\varphi_{i,j} = \varphi_i \circ \pi_j$ from H_2 onto $I \rtimes \mathrm{Sym}(3)$, having different kernels. These epimorphisms produce 9 non-isomorphic H_2-modules J_i, for $i = 1, \dots, 9$. Now we take each module with multiplicity

3 and we consider the group

$$G_2 = \left(\prod_{1 \leqslant i \leqslant 9} J_i^3 \right) \rtimes H_2.$$

By Proposition 5, as $\delta_{H_2}(J_i) = r_{H_2}(J_i)$, we deduce that G_2 is still 2-generated.

We want to prove that g_1, g_2, g_3 cannot be lifted to three invariable generators of G_2.

We will consider in particular the projection $\pi = \varphi_{1,j}$, where j is defined in such a way that (0.6) holds, hence

$$\pi(g_i) = (1,2)(\alpha_i v_1 + v_2)$$

for both $i = 1, 2$.

Assume by contradiction that g_1, g_2, g_3 can be lifted to invariable generators of G_2. Then in particular the elements $\pi(g_1), \pi(g_2), \pi(g_3)$ can be lifted to invariable generators of $J^3 \rtimes H_2$, so by Proposition 10 the following relation holds:

$$\dim C_J(\pi(g_1)) + \dim C_J(\pi(g_2)) + \dim C_J(\pi(g_3)) \geqslant 3. \tag{0.7}$$

Let $\pi(g_3) = (1,2,3)(\alpha v_1 + \beta v_2) = (1,2,3)(\alpha, \alpha+\beta, \beta)$ and take $(z_1, z_2, z_3) \in J$. Then

$$(z_1, z_2, z_3) = (z_1, z_2, z_3)^{\pi(g_3)} = ((-1)^{\alpha} z_3, (-1)^{\alpha+\beta} z_1, (-1)^{\beta} z_2)$$

if and only if $z_2 = (-1)^{\alpha+\beta} z_1$ e $z_3 = (-1)^{\beta} z_2 = (-1)^{\alpha} z_1$; in particular we always have $\dim C_J(\pi(g_3)) = 1$. Now, $\pi(g_i)$, for $i = 1, 2$, is of the form $(1,2)(\alpha v_1 + v_2) = (1,2)(\alpha, \alpha+1, 1)$. We note that if

$$(z_1, z_2, z_3) = (z_1, z_2, z_3)^{(1,2)(\alpha v_1 + v_2)} = ((-1)^{\alpha} z_2, (-1)^{\alpha+1} z_1, -z_3)$$

then

$$-z_3 = z_3, \quad z_2 = (-1)^{\alpha} z_1, \quad z_1 = (-1)^{\alpha+1} z_2 = (-1)^{\alpha+1}(-1)^{\alpha} z_1 = -z_1,$$

hence $(z_1, z_2, z_3) = (0, 0, 0)$. Therefore $\dim C_J(\pi(g_1)) = \dim C_J(\pi(g_2)) = 0$, so (0.7) cannot be satisfied, giving the desired contradiction. We conclude that $d_I(G_2) \geqslant 4$.

REFERENCES

[1] M. Aschbacher, “Finite group theory”, Second edition, Cambridge Studies in Advanced Mathematics, 10, *Cambridge University Press*, Cambridge, 2000.

[2] F. Dalla Volta – A. Lucchini, “Finite groups that need more generators than any proper quotient”, sl J. Austral. Math. Soc. Ser. A 64 (1998), 82–91.

[3] F. Dalla Volta – A. Lucchini – F. Morini, “On the probability of generating a minimal d-generated group”, *J. Aust. Math. Soc.* 71 (2001), 177–185.

[4] E. Detomi – A. Lucchini, “Crowns and factorization of the probabilistic zeta function of a finite group”, *J. Algebra* 265 (2003), 651–668.

[5] E. Detomi – A. Lucchini, “Invariable generation with elements of coprime prime-power order”, *J. Algebra* 423 (2015), 683–701.

[6] E. Detomi – A. Lucchini, “Invariable generation of permutation groups”, *Arch. Math.* 104 (2015), 301–309.

[7] E. Detomi – A. Lucchini, “Invariable generation of prosoluble groups”, *Israel J. Math.* 211 (2016), 481–491.

[8] J. D. Dixon, “The structure of linear groups”, *Van Nostrand Reinhold Company*, 1971.

[9] J. D. Dixon, “Random sets which invariably generate the symmetric group”, *Discrete Math.* 105 (1992), 25–39.

[10] 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.

[11] W. Gaschütz, “Zu einem von B.H. und H. Neumann gestellten Problem”, *Mathematische Nachrichten* 14 (1955), 249 – 252.

[12] W. Gaschütz, “Die Eulersche Funktion endlicher auflösbarer Gruppen”, *Illinois J. Math.* 3 (1959), 469–476.

[13] R. Guralnick, “On the number of generators of a finite group”, *Arch. Math.* 53 (1989), 521–523.

[14] R. Guralnick – G. Malle, “Simple groups admit Beauville structures”, *J. Lond. Math. Soc.* (2) 85 (2012), 694–721.

[15] W. M. Kantor – A. Lubotzky – A. Shalev, "Invariable generation and the Chebotarev invariant of a finite group", *J. Algebra* 348 (2011), 302–314.

[16] W. M. Kantor – A. Lubotzky – A. Shalev, "Invariable generation of infinite groups", *J. Algebra* 421 (2015), 296–310.

[17] A. Lucchini, "A bound on the number of generators of a finite group", *Arch. Math.* 53 (1989), 313–317.

[18] A. Lucchini, "Invariable generation of iterated wreath products of cyclic groups", *Beitr. Algebra Geom.* 58 (2017), 477–482.

[19] A. Lucchini, "A bound on the expected number of random elements to generate a finite group all of whose Sylow subgroups are d-generated", *Arch. Math.* 107 (2016), 1–8.

[20] A. Lucchini – G. Tracey, "An upper bound on the Chebotarev invariant of a finite group", *Israel J. Math.* 219 (2017), 449–467.

[21] T. Luczak – L. Pyber, "On random generation of the symmetric group", *Combin. Probab. Comput.* 2 (1993), 505–512.

[22] A. Shalev, "A theorem on random matrices and some applications", *J. Algebra* 199 (1998) 124–141.

[23] U. Stammbach, "Cohomological characterisations of finite solvable and nilpotent groups", *J. Pure Appl. Algebra* 11 (1977/78), 293–301.

Eloisa Detomi, Andrea Lucchini
Dipartimento di Matematica "Tullio Levi-Civita"
Università di Padova
Via Trieste, 63
35131 Padova
Italy
e-mail: detomi@math.unipd.it lucchini@math.unipd.it

Marta Morigi
Dipartimento di Matematica
Università di Bologna
Piazza di Porta San Donato, 5
40126 Bologna
Italy
e-mail: marta.morigi@unibo.it