Forum Math. **24** (2012), 875–887
DOI 10.1515/FORM.2011.092
Forum Mathematicum

Boundedly generated subgroups of finite groups

Andrea Lucchini, Marta Morigi and Pavel Shumyatsky

Communicated by Dan Segal

Abstract. The starting point for this work was the question whether every finite group G contains a two-generated subgroup H such that $\pi(H) = \pi(G)$, where $\pi(G)$ denotes the set of primes dividing the order of G. We answer the question in the affirmative and address the following more general problem. Let G be a finite group and let $i(G)$ be a property of G. What is the minimum number t such that G contains a t-generated subgroup H satisfying the condition that $i(H) = i(G)$? In particular, we consider the situation where $i(G)$ is the set of composition factors (up to isomorphism), the exponent, the prime graph, or the spectrum of the group G. We give a complete answer in the cases where $i(G)$ is the prime graph or the spectrum (obtaining that $t = 3$ in the former case and t can be arbitrarily large in the latter case). We also prove that if $i(G)$ is the exponent of G, then t is at most four.

Keywords. Generators, exponent, prime graph, spectrum.

2010 Mathematics Subject Classification. 20F05, 20D60.

1 Introduction

Certain properties of a finite group G can be detected from its 2-generated subgroups. For example, the well-known theorem of Zorn says that G is nilpotent if and only if it is Engel. It follows that G is nilpotent if and only if every 2-generated subgroup of G is nilpotent. A deep theorem of Thompson says that G is soluble if and only if every 2-generated subgroup of G is soluble [14] (see also Flavell [6]). Thus, we observe here a very interesting phenomenon that in a sense the structure of some 2-generated subgroup of a finite group should be as complex as that of the whole group. A further illustration for this is the theorem obtained in [13] that in particular implies that a finite group G is soluble and has Fitting height h if and only if every 2-generated subgroup of G is soluble and has Fitting height h. It is natural to ask what other properties of G can be detected by looking at subgroups with small number of generators. In the present paper we address the problem for

The first and second authors were partially supported by MIUR (Project “Teoria dei Gruppi e applicazioni”). The third author was supported by CNPq.

such important characteristics of a group G as the set of all prime divisors of the order of G (denoted by $\pi(G)$), the set of composition factors (up to isomorphism), the exponent, the prime graph, or the spectrum of the group G.

We started with the question whether every finite group G contains a 2-generated subgroup H with the property that $\pi(H) = \pi(G)$ (cf. Kourovka Notebook [9, Problem 17.125]). We were able to confirm this. Actually, we proved a stronger result.

Theorem A. *Let $\mathcal{C}(G)$ be the set of isomorphism classes of composition factors of G. Then there exists a 2-generated subgroup H of G such that $\mathcal{C}(H) = \mathcal{C}(G)$.*

We also note that Theorem A has a natural generalization to profinite groups. If G is a profinite group, then a composition factor of G is defined as a composition factor of G/N for some open subgroup N of G.

Theorem B. *Let G be a profinite group and let $\mathcal{C}(G)$ be the set of isomorphism classes of composition factors of G. Then there exists a (topologically) 2-generated closed subgroup H of G such that $\mathcal{C}(H) = \mathcal{C}(G)$.*

Denote by $\Gamma(G)$ the prime graph of a finite group G. This is the graph whose set of vertices is $\pi(G)$ and $p, q \in \pi(G)$, with $p \neq q$, are connected by an edge if and only if G has an element of order pq.

Theorem C. *Let G be a finite group. Then there exists a 3-generated subgroup H of G such that $\Gamma(H) = \Gamma(G)$.*

It can be shown that this bound is sharp. In Section 3 we construct a soluble 3-generated group G such that no 2-generated subgroup of G has the same prime graph as G.

Recall that the spectrum of a finite group G is the set of orders of elements of G. In Section 3 we show that for every positive integer $d \geq 2$ there exists a d-generated group G with no proper subgroup having the same spectrum. This shows that Theorem C is no longer true if we replace $\Gamma(G)$ by the spectrum of G. In particular, the spectrum of G cannot be determined by a single boundedly generated subgroup.

Next, we ask the same question for the exponent of G. This is the minimum natural number n such that $g^n = 1$ for every $g \in G$. Our result with respect to the question is as follows.

Theorem D. *Let G be a finite group. Then there exists a 4-generated subgroup H of G such that H has the same exponent of G.*

We were unable to prove that this bound is sharp. Actually, we believe that it is possible to bring it down to 3, but there are not even examples which show that this bound is bigger than 2. On the other hand, for soluble groups the complete answer is given in the following theorem.

Theorem E. *Let G be a finite soluble group. Then there exists a 2-generated subgroup H of G such that H has the same exponent as G.*

As it often happens when studying the minimum number of generators of a group G, a fundamental role is played by the so called "crown-based power" of a primitive monolithic group L. Most of the results and terminology we will need can be found in [4], but we are going to review some of them for the reader's convenience.

2 Background material

In what follows $\mathrm{d}(G)$ denotes the the minimal number of generators of the group G and $\exp(G)$ stands for the exponent of G. If p is a prime, $|G|_p$ denotes the order of a Sylow p-subgroup of G and an element of G of p-power order will be often called a p-element, for shortness. Also, if V is a G-module, then $\mathrm{H}^1(G, V)$ denotes the first cohomology group of G on V. We recall that the socle $\mathrm{Soc}(G)$ is the subgroup generated by all minimal normal subgroups of G.

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

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

Clearly, $\mathrm{Soc}(L_k) = A^k$ and $L_k/\mathrm{Soc}(L_k) \cong L/\mathrm{Soc}(L)$. Note also that if A has a complement in L, then $\mathrm{Soc}(L_k)$ has a complement in L_k.

Crown-based powers arise naturally when studying finite groups that need more generators than any proper quotient. A proof of the following theorem can be found in [4].

Theorem 2.1. *Let m be a natural number and let G be a finite group such that $\mathrm{d}(G/N) \leq m$ for every non-trivial normal subgroup N, but $\mathrm{d}(G) > m$. Then there exists a group L with a unique minimal normal subgroup A such that $G \cong L_k$ for some k and A is either non-abelian or complemented.*

Proposition 6 of [5] gives the following result, which provides a bound on the number of generators of a crown-based power L_k in terms of k in the case when the socle of L is abelian.

Theorem 2.2. *Let L be a group with a unique minimal normal subgroup A such that A is abelian and complemented in L. Suppose $q = |\mathrm{End}_{L/A}(A)|$, $q^r = |A|$, $q^s = |\mathrm{H}^1(L/A, A)|$, $\theta = 0$ or 1 according to whether A is a trivial L/A-module or not. Then*

$$\mathrm{d}(L_k) = \max(\mathrm{d}(L/A), \theta + \lceil (k+s)/r \rceil),$$

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

We remark that in the above theorem we always have $s < r$. This is because of the following result of Aschbacher and Guralnick [1].

Theorem 2.3. *Let p be prime. If G is a finite group and V is a faithful irreducible G-module over the field with p elements, then $|\mathrm{H}^1(G, V)| < |V|$.*

In the case where the socle A of the monolithic group L is non-abelian a bound on $\mathrm{d}(L_k)$ can be obtained using the next lemma. It is a straightforward consequence of [11, Lemma 1 (ii)].

Lemma 2.4. *Let L be a group with a unique minimal normal subgroup A such that A is non-abelian, and let $t \geq \max\{4, \mathrm{d}(L)\}$. Then for every k such that $k \leq |A|^{t-3}$ we have $\mathrm{d}(L_k) \leq t$.*

Proof. The sequence $\mathrm{d}(L_1), \dots, \mathrm{d}(L_s), \dots$ is unbounded and non-decreasing and, by a theorem proved in [10], $\mathrm{d}(L_{s+1}) \leq \mathrm{d}(L_s) + 1$, so for each $t \geq \mathrm{d}(L)$ there is a unique s such that $\mathrm{d}(L_s) = t < \mathrm{d}(L_{s+1})$. Define $f(L, t) = s + 1$. If $A \cong S^n$, where S is a non-abelian simple group, then [11, Lemma 1 (ii)] says that $f(L, t) \geq 1 + \frac{|A|^{t-2}}{n}$. So if $k \leq \frac{|A|^{t-2}}{n}$, then $\mathrm{d}(L_k) \leq t$. As $n < |A|$, the result follows. □

To prove Theorem B we also need the following lemma about normal subgroups of crown-based powers.

Lemma 2.5. *Let L be a monolithic group and let $G = L_k$ be the crown-based power of L of size k. If N is a normal subgroup of G, then either $\mathrm{Soc}(G) \leq N$ or $N \leq \mathrm{Soc}(G)$.*

Proof. The proof is by induction on k. If $k = 1$, then the result is true because $\mathrm{Soc}(G)$ is the unique non-trivial minimal normal subgroup of G. So assume that $k > 1$ and that $N \neq 1$ and let M be a non-trivial minimal normal subgroup of G such that $M \leq N$. Then $M \cong \mathrm{Soc}(L)$, $G/M \cong L_{k-1}$ and $\mathrm{Soc}(G/M) = \mathrm{Soc}(G)/M$. By induction, it follows that either $\mathrm{Soc}(G/M) \leq N/M$ or $N/M \leq \mathrm{Soc}(G/M)$ and then the result follows. □

3 Proofs of Theorems A, B and C

Theorem A is a special case of the following proposition, whose formulation is more appropriate in the context of profinite groups.

Proposition 3.1. *Let G be a finite group and $G_0 = 1 < \cdots < G_i < \cdots < G_n = G$ be a chief series of G. Then there exists a 2-generated subgroup H of G such that $\mathcal{C}(HG_i/G_i) = \mathcal{C}(G/G_i)$ for every $i = 0, \dots, n-1$.*

Proof. We will prove that if G is a group with no proper subgroups H such that $\mathcal{C}(HG_i/M) = \mathcal{C}(G/G_i)$ for every $i = 0, \dots, n-1$, then $\mathrm{d}(G) \leq 2$. Of course, we may assume that G is not cyclic, otherwise the result is obviously true. Let N be a normal subgroup of G such that $\mathrm{d}(G/N) = d = \mathrm{d}(G)$ but every proper quotient of G/N can be generated with $d-1$ elements. Then, by Theorem 2.1, $G/N \cong L_t$ for some integer t and some monolithic group L whose socle is either non-abelian or complemented. Note also that $\mathrm{d}(L/\operatorname{Soc}(L)) \leq d-1$ because this group is a proper quotient of G/N.

We first prove that $t = 1$. Assume by contradiction that $t \geq 2$. If we delete repetitions in the series $N \leq \cdots \leq G_iN/N \leq \cdots \leq G_n/N = G/N$, we obtain a chief series of G/N. It follows from Lemma 2.5 that there exist j and k with $0 \leq j < k \leq n$ such that $G_kN/N = \operatorname{Soc}(G/N)$, $G_kN/G_jN \cong \operatorname{Soc}(L)$ and $G/G_jN \cong L$. Note also that if $G_iN \leq G_jN$, then $G/G_iN \cong L_s$ for some positive integer $s \leq t$, so $\mathcal{C}(G/G_iN) = \mathcal{C}(L)$. Define X in the following way.

- If $\operatorname{Soc}(L)$ is abelian, then $\operatorname{Soc}(L)$ has a complement in L and thus $\operatorname{Soc}(G/N)$ has a complement Y/N in G/N. Then there exists a Y/N-invariant complement M/N of G_jN/N in $\operatorname{Soc}(G/N)$ and let $X/N = MY/N$.
- Otherwise let X/N be the subgroup of G/N corresponding to the diagonal $\{(l, \dots, l) \mid l \in L\}$ of L_t.

Note that in both cases X is a proper subgroup of G such that $XNG_j = G$. We want to prove that XG_i/G_i has the same set of isomorphism classes of composition factors as G/G_i for each $i = 1, \dots, n-1$. Since $N \leq X$, it suffices to prove that $\mathcal{C}(XG_i/NG_i) = \mathcal{C}(G/NG_i)$. If $NG_i > NG_j$, then $XG_i = XNG_i = G$ and our claim is trivial. If $NG_i \leq NG_j$, then $L \cong G/NG_j \cong XNG_j/NG_j \cong X/X \cap NG_j$ is an epimorphic image of $X/X \cap NG_i \cong XG_i/NG_i$ and this implies that $\mathcal{C}(G/NG_i) = \mathcal{C}(L) = \mathcal{C}(XG_i/NG_i)$.

Now X is a proper subgroup of G such that $\mathcal{C}(XG_i/G_i) = \mathcal{C}(G/G_i)$ for each $i = 1, \dots, n-1$, and this contradicts our choice of G.

So $t = 1$ and we can apply the Main Theorem in [12]. It follows that $d = \mathrm{d}(G/N) = \mathrm{d}(L) = \max\{2, \mathrm{d}(L/A)\} \leq \max\{2, d-1\}$, so $d = 2$, as required. □

We mention here that the proof of Proposition 3.1 is almost trivial when G is a finite soluble group because it follows easily by induction on $|G|$ using the Schur–Zassenhaus theorem.

We are now ready to prove Theorem B. We recall that a profinite group is a topological group which is an inverse limit of finite groups (which are endowed with the discrete topology) or, equivalently, it is a compact totally disconnected topological group. For a general reference on profinite groups see Wilson's book [15].

If G is a profinite group and H is a closed subgroup of G, we say that H is (topologically) generated by $x_1, \dots, x_n$ if HN/N is generated by $x_1N, \dots, x_nN$ for every open normal subgroup N of G.

Proof of Theorem B. We note that the cardinality of $\mathcal{C}(G)$ is at most countable because there is only a countable number of isomorphism classes of finite groups. For every $S \in \mathcal{C}(G)$ let N_S be an open normal subgroup of G such that S is a composition factor of G/N_S. If $N = \bigcap_{S \in \mathcal{C}(G)} N_S$, then $G/N = \bar{G}$ is a profinite group. For every $x \in G$ we will denote with $\bar{x}$ the image xN of x in G/N, and similarly if $\bar{M}$ is a subgroup of $\bar{G}$, then M will denote its preimage in G. We note that $\{\bar{N}_S\}_{S \in \mathcal{C}(G)}$ is a countable basis of open subgroups of $\bar{G}$; moreover, by taking appropriate intersections, we can choose a basis $\mathcal{B}$ of open subgroups of $\bar{G}$ such that the elements of $\mathcal{B}$ are totally ordered with respect to inclusion, that is for each $\bar{M}_i, \bar{M}_j \in \mathcal{B}$, either $\bar{M}_i \le \bar{M}_j$ or $\bar{M}_j \le \bar{M}_i$.

For every open normal subgroup $\bar{M} \in \mathcal{B}$ we define

$$\Omega_{\bar{M}} = \Big\{(x_1, x_2) \in G \times G \mid \mathcal{C}(\langle x_1, x_2 \rangle M/M) = \mathcal{C}(G/M)\Big\}.$$

Note that if $(x_1, x_2) \in \Omega_{\bar{M}}$, then $x_1M \times x_2M \subseteq \Omega_{\bar{M}}$, and actually $\Omega_{\bar{M}}$ is the (finite) union of all subsets of that type. As M is closed in G, it follows that $x_1M \times x_2M$ is closed in $G \times G$ and thus $\Omega_{\bar{M}}$ is also closed in $G \times G$, being the union of finitely many closed sets. Moreover, if we choose $\bar{M}_1, \dots, \bar{M}_r \in \mathcal{B}$, we may assume that $\bar{M}_1 \le \dots \le \bar{M}_r$ and we can refine the series $M_1 \le M_2/M_1 \le \dots \le M_r/M_1 \le G/M_1$ to a composition series of G/M_1. By Proposition 3.1, there is a 2-generated subgroup T/M_1 of G/M_1 such that $\mathcal{C}(G/M_i) = \mathcal{C}(TM_i/M_i)$ for every $i = 1, \dots, r$. Let $T/M_1 = \langle y_1, y_2 \rangle M_1/M_1$; then $(y_1, y_2) \in \bigcap_{i=1}^{r} \Omega_{\bar{M}_i}$. So the family $\{\Omega_{\bar{M}}\}_{\bar{M} \in \mathcal{B}}$ has the property that every finite subfamily has non-empty intersection. As G is compact, the whole family has non-empty intersection, that is there exists $(x_1, x_2) \in G \times G$ such that $\mathcal{C}(\langle x_1, x_2 \rangle M/M) = \mathcal{C}(G/M)$ for any $\bar{M} \in \mathcal{B}$. Let H be the topological closure of $\langle x_1, x_2 \rangle$ in G. We prove that H has the same set of isomorphism classes of composition factors as G. If $S \in \mathcal{C}(G)$, then N_S/N is open in G/N, so there exists an open subgroup M of G such that $\bar{M} \in \mathcal{B}$ and $M \le N_S$. We have that $S \in \mathcal{C}(G/M) = \mathcal{C}(\langle x_1, x_2 \rangle M/M) =$

$\mathcal{C}(HM/M) = \mathcal{C}(H/(H \cap M)) \subseteq \mathcal{C}(H)$. Similarly, $\mathcal{C}(H) \subseteq \mathcal{C}(G)$. This concludes the proof. □

For the proof of Theorem C we will need the following two results:

Proposition 3.2. *Let P be a p-group acting on a p'-group Q in such a way that $C_Q(a) = 1$ for every $a \in P \setminus \{1\}$. Then either P is cyclic or $p = 2$ and P is generalized quaternion.*

Proof. See [7, 10.3.1 (iv)]. □

Lemma 3.3. *Let L be an almost simple group. If $k \leq 2$, then the crown-based power L_k is at most 3-generated.*

Proof. If $k = 1$, then $L_1 = L$ and the statement is true by the main result in [3]. Let $k = 2$ and let $A = \mathrm{Soc}(L)$. Then, of course, A is a non-abelian finite simple group. Again by the main result in [3], it is possible to choose $g_1, g_2, g_3 \in L$ such that $A \leq \langle g_2, g_3 \rangle$ and $L = \langle g_1, g_2, g_3 \rangle$. Let $x \in A$ be such that $|g_1 x| \neq |g_1|$ (note that such an x exists by the Main Lemma in [12]). Then $L_2 = \langle (g_1, g_1 x), (g_2, g_2), (g_3, g_3) \rangle$. □

Proof of Theorem C. The idea of the proof is to argue as in the proof of Theorem A, showing that if G is a group with no proper subgroups having the same prime graph, then $\mathrm{d}(G) \leq 3$. Let N be a normal subgroup of G such that $\mathrm{d}(G/N) = d = \mathrm{d}(G)$ but every proper quotient of G/N can be generated with $d - 1$ elements. Then, by Theorem 2.1, G/N is isomorphic to the group

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

and let $\varphi : L_k \to G/N$ be an isomorphism between them. For each $i \leq k$ define

$$T_i = \{(l_1, \ldots, l_k) \in L_k \mid l_j = l_i \text{ for every } j > i\} \leq L_k.$$

Note that $T_i \cong L_i$. Recall that A is the product of isomorphic simple groups. We will work with the subgroup X of G that can be defined as follows:

(1) if $k = 1$ or if A is not simple, let $X/N = \varphi(T_1)$,

(2) if $k = 2$ or A is simple of order greater than 2, let $X/N = \varphi(T_2)$,

(3) otherwise $|A| = 2$, $k \geq 3$ and we let $X/N = \varphi(T_3)$.

We wish to prove that $X = G$. This is obviously true if $k = 1$ or if $k = 2$ and A is simple. So from now on we will assume that

$$k \geq 2 \text{ and if } k = 2, \text{ then } A \text{ is not simple.} \tag{$*$}$$

Of course, the set of primes dividing the order of X is the same as the set of primes dividing the order of G, so $\Gamma(X)$ and $\Gamma(G)$ have the same vertices. It remains to prove that they also have the same edges because then we would have the equality $\Gamma(X) = \Gamma(G)$ and thus $X = G$ by the minimality of G.

Obviously, if $p, q \in \Gamma(X)$ with $p \neq q$ and there is an edge connecting p and q in $\Gamma(X)$, then there is also an edge connecting p and q in $\Gamma(G)$.

Now let $p, q \in \Gamma(G)$ with $p \neq q$, and assume that there is an edge connecting p and q, that is there is an element u of order pq in G.

If $u \in N \leq X$, then there is an edge in $\Gamma(X)$ connecting p and q.

If $u \in G \setminus N$, then we distinguish two cases: when uN has order pq and when uN has prime order.

In the first case pq divides the order of L. If there exists $l \in L$ of order pq, let $vN = \varphi(l, l, \ldots, l)$. Then $v \in X$ has order divisible by pq, so there is an edge in $\Gamma(X)$ connecting p and q. If L has no element of order pq, then $k > 1$. Let $\varphi^{-1}(uN) = (l_1, \ldots, l_k) \in L^k$. As uN has order pq, there are two components of $\varphi^{-1}(uN)$, say l_r, l_s, such that $|l_r| = p$, $|l_s| = q$. As $|l_r A| = |l_s A|$, it follows that $l_r, l_s \in A$, so the order of A is divisible by two different primes. Moreover, as A has no element of order pq, it follows that A is simple. Therefore, X is defined by condition (2) and if we take $vN = \varphi(l_r, l_s, l_s, \ldots, l_s) \in X/N$, then $v \in X$ has order divisible by pq. Hence, there is an edge in $\Gamma(X)$ connecting p and q.

If uN has prime order, say p, then q divides the order of N.

First assume that $p \nmid |A|$. Then, by the definition of X, it follows that every Sylow p-subgroup of X/N is also a Sylow p-subgroup of G/N. As uN has order p, there exists $y \in G$ such that $(uN)^y \in X/N$, so $u^y \in X$ is an element of X of order pq and there is an edge in $\Gamma(X)$ connecting p and q.

Now assume that p divides $|A|$. Let Q be a Sylow q-subgroup of N and let $T = N_X(Q)$. By the Frattini argument, $X = TN$. Let P be a Sylow p-subgroup of T. In the natural way, P acts on Q by conjugation. Also, PN/N is a Sylow p-subgroup of X/N.

The hypothesis $(*)$ shows that a Sylow p-subgroup of X/N is non-cyclic. Thus, P is non-cyclic. Moreover, if $p = 2$, then $\mathrm{Soc}(X/N)$ contains a subgroup isomorphic to an elementary abelian 2-group Y of rank 3, hence P has a section isomorphic to Y and cannot be a generalized quaternion group. By Proposition 3.2, we conclude that there is a non-trivial element in Q centralized by some non-trivial element from P. Hence, there is an element of order pq in X, as required. This concludes the proof of the fact that $X = G$.

Now we will bound $\mathrm{d}(G) = \mathrm{d}(G/N)$ by examining $G/N = X/N \cong L_k$.

(i) If $k = 1$ or if A is not simple, then $G/N = \varphi(T_1) \cong L$, so the Main Theorem in [12] yields $\mathrm{d}(G/N) = \mathrm{d}(L) \leq \max\{2, \mathrm{d}(L/A)\} \leq \max\{2, d-1\}$, which implies that $d = 2$.

(ii) If A is abelian of order greater than 2, then $k \leq 2$. Let q, r, s, θ be as in Theorem 2.2. Since $\mathrm{d}(L/A) \leq d-1$, it follows that $d = \mathrm{d}(G/N) = \theta + \lceil (k+s)/r \rceil \leq 1 + \lceil (2+s)/r \rceil$. We have already observed that $s < r$ whence $d \leq 3$.

(iii) If A has order 2, then $k \leq 3$, so the same argument as before shows that $d = \mathrm{d}(G/N) = \lceil (k+s)/r \rceil \leq 3$ (note that $\theta = 0$ in this case).

(iv) If none of the above occurs, then it follows from the definition of X that A is a simple non-abelian group and $k = 2$. Now Lemma 3.3 implies that $G/N \cong L_2$ is at most 3-generated, so again $d \leq 3$.

This completes the proof. □

The following example shows that there exists a 3-generated group H such that no 2-generated subgroup T of H satisfies $\Gamma(H) = \Gamma(T)$. Thus, the bound in Theorem C is sharp.

Consider the group $S_3 = \langle a, b \mid a^2 = b^3 = 1, b^a = b^{-1} \rangle$. Let V_1 be an elementary abelian 5-group of rank 2, and let V_2 be an elementary abelian 7-group of rank 2.

The assignment $a \mapsto \alpha_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$, $b \mapsto \alpha_2 = \left(\begin{smallmatrix} 1 & 1 \\ 2 & 3 \end{smallmatrix}\right)$ makes V_1 into an irreducible S_3-module, and b acts on it without fixed points, so the semidirect product $V_1 \rtimes S_3$ has no element of order 15.

The assignment $a \mapsto \gamma_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $b \mapsto \gamma_2 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ makes V_2 into an irreducible S_3-module, and b acts on it without fixed points, so the semidirect product $V_2 \rtimes S_3$ has no element of order 21.

Now consider $G = (\langle b_1 \rangle \times \langle b_2 \rangle) \rtimes \langle a \rangle$, where $|b_1| = |b_2| = 3$ and $|a| = 2$ and $b_i^a = b_i^{-1}$. Note that $G \cong L_2$, where $L = S_3$, so Theorem 2.2 shows $\mathrm{d}(G) = 3$.

The assignment $a \mapsto (\alpha_1, \gamma_1)$, $b_1 \mapsto (\alpha_2, 1)$, $b_2 \mapsto (1, \gamma_2)$ gives an action of G on $V_1 \times V_2$, and we can consider the semidirect product $H = (V_1 \times V_2) \rtimes G$. As G is a quotient of H, it follows that $\mathrm{d}(H) \geq 3$ (actually using Theorem 2.2 it is easy to see that $\mathrm{d}(H) = 3$).

Now let T be a subgroup of H which has the same prime graph as H and let $T^* = (V_1 \times V_2)T$. We claim that $T^* = H$. Assume by contradiction that T is a proper subgroup of H. As $\pi(T^*) = \pi(H)$, it follows that T^* has index 3 in H. Moreover, a Sylow 3-subgroup P of T^* is cyclic, and as T^* must contain elements of order 15 and 21, the centralizer in T^* of P has order divisible by 35. But it is easy to see that in H there is no element of order 3 whose centralizer has order divisible by 35, so $T^* = H$. Now for each $i = 1, 2$ we have $T \cap V_i \neq 1$. Moreover, the normal closure of $T \cap V_i$ in T is equal to the normal closure V_i of $T \cap V_i$ in H, so $V_i \leq T$ for each $i = 1, 2$ and $T = H$. This shows that H has the desired property.

Recall that the spectrum of a group G is the set of orders of the elements of G. Let us fix an arbitrary positive integer d and construct a group G such that $\mathrm{d}(G) = d$ and no $(d-1)$-generated subgroup of G has the same spectrum. Let $X = \{p_1, \dots, p_d\}$ be a set consisting of d different odd prime numbers, and let $D_i = \langle b_i, a_i \mid b_i^{p_i} = a_i^2 = 1, b_i^{a_i} = b_i^{-1}\rangle$ be the dihedral group of order $2p_i$, for each $i = 1, \dots, d$. Put

$$G = \prod_{i=1}^{d} D_i.$$

Let also $B = \prod_{i=1}^{d} \langle b_i \rangle \le G$, and let $\rho : G \to G/B$ be the natural projection. It is easy to see that $\mathrm{d}(G) \le d$ because $\rho(G)$ is an elementary abelian 2-group of rank d, and as $G = \langle a_1 b_2, a_2 b_3, \dots, a_d b_1 \rangle$, it follows that $\mathrm{d}(G) = d$. Moreover, the spectrum of G is the set of all proper divisors of the number $m = 2p_1 \cdots p_d$. Note that the elements $g \in G$ of order m/p_i are precisely those of the form $(b_1^{r_1}, \dots, b_{i-1}^{r_{i-1}}, a_i, b_{i+1}^{r_{i+1}}, \dots, b_d^{r_d})$, where $r_j \not\equiv 0 \bmod p_j$, for all $j \in \{1, \dots, d\}$, $j \ne i$. Hence, if a subgroup H of G contains an element of order m/p_i, then $\rho(H) = \rho(D_i)$. Thus, if a subgroup H of G has the same spectrum as G, then $\rho(H)$ is an elementary abelian group of rank d and thus H is at least d-generated (actually $H = G$).

4 Proofs of Theorems D and E

The strategy of the proofs of Theorems D and E is similar to that of the previous ones but involves different arguments. We will isolate one of them in the following

Lemma 4.1. *Let G be a finite group in which all proper subgroups have smaller exponent than G. Let N be a normal subgroup of G such that $G/N \cong L_k$ for some monolithic group L whose socle A is abelian and complemented. If we have $|\mathrm{End}_{L/A}(A)| = q$, $|A| = q^r$, then $k \le r$.*

Proof. Let p be the prime such that q is a p-power, $\mathbb{F}_p$ be the field with p elements and $\varphi : L_k \to G/N$ be an isomorphism between L_k and G/N. Further, let $I/N = \varphi(\mathrm{Soc}(L_k))$. We note that φ makes $\mathrm{Soc}(L_k) \cong A^k$ into an $\mathbb{F}_p G$-module and $\mathrm{End}_{L/A}(A) = \mathrm{End}_{\mathbb{F}_p G}(A)$. Let us show that I/N is a cyclic $\mathbb{F}_p G$-module.

Note that if T is a complement for A in the monolithic group L, then the subgroup $\{(t, \dots, t) \mid t \in T\} \le L_k$ is a complement for A^k in L_k and $K/N = \varphi(T)$ is a complement of I/N in G/N. Remark that I/N is a p-group. Hence, if $s \ne p$ is a prime, then every Sylow s-subgroup of K is also a Sylow s-subgroup of G. Now for every prime $s \ne p$ let y_s be an s-element of K of maximum order and let $y_p \in K$ be a p-element of G of maximum order. Write $y_p = yz$, where $y \in I$

and $z \in K$. Let $M = \langle y \rangle^G$. Of course, we have $\exp(G) = \exp(\langle y_s \mid s$ is a prime dividing $|G|\rangle) = \exp(\langle K, y_p \rangle) = \exp(MK)$, so $G = MK$. This implies that $I/N = M/N$.

So I/N is a cyclic $\mathbb{F}_p G$-module. Let J be the Jacobson radical of $\mathbb{F}_p G$, so that $\mathbb{F}_p G/J$ is a semisimple algebra. Of course, $I/N \cong A^k$ is also a cyclic $\mathbb{F}_p G/J$-module (because the Jacobson radical annihilates any simple G-module) and we can apply [2, Lemma 1]. If A occurs n times in $\mathbb{F}_p G/J$, it follows that $\lceil k/n \rceil = 1$, so that $k \leq n$.

But $\mathbb{F}_p G/J$ is a semisimple algebra (and, of course, it is also Artinian, being finite), so we can apply the Wedderburn–Artin theorem (see [8, Lemma 1.11, Theorems 1.14 and 3.3]), and we conclude that n is precisely $\dim_{\mathrm{End}_G(A)}(A) = \dim_{\mathrm{End}_{L/A}(A)}(A) = r$. So we conclude that $k \leq r$, as required. □

Proof of Theorem E. Let G be a soluble group with no proper subgroup having the same exponent and N be a normal subgroup of G such that $\mathrm{d}(G/N) = d = \mathrm{d}(G)$ but every proper quotient of G/N can be generated with $d - 1$ elements. Then, by Theorem 2.1, G/N is isomorphic to L_k for some monolithic group L whose socle A is abelian and complemented. Let q, r, s, θ be as in Theorem 2.2. Since G is soluble, all complements of A in L are conjugate, so that $s = 0$. Moreover, Lemma 4.1 tells us that $k \leq r$, so $\lceil k/r \rceil = 1$. As $\mathrm{d}(L/A) \leq d - 1$, it follows from Theorem 2.2 that $d = \mathrm{d}(G/N) = \theta + \lceil k/r \rceil \leq 2$. This concludes the proof. □

Before embarking on the study of the general case, we need a preliminary lemma concerning monolithic groups whose socle is non-abelian.

Lemma 4.2. *Let p be a prime, let L be a finite monolithic group whose socle A is non-abelian and choose a p-element $l \in L$. If a_l is the number of A-conjugacy classes of L which are contained in lA and whose elements have p-power orders, then $a_l \leq |A|_p$.*

Proof. Let $\Omega = \{x \in lA \mid x$ has p-power order$\}$ and $H = \langle l \rangle A$. Choose a Sylow p-subgroup P of H containing l and let $Q = A \cap P$. It is clear that $P = \langle l \rangle A \cap P = \langle l \rangle (A \cap P)$. Since $H = \langle l \rangle A$ and $l \in P$, every Sylow p-subgroup of H is A-conjugate to P.

Now let $x \in \Omega$. We have $x = la$ for some $a \in A$ and there exists $y \in A$ such that $x^y \in P$. But $(la)^y = l[l, y]a^y$, and as $l \in P$, it follows that $[l, y]a^y \in P \cap A = Q$. This proves that every element of Ω is A-conjugate to an element of lQ. Thus, $a_l = |\Omega| \leq |Q| \leq |A|_p$, as required. □

Proof of Theorem D. Let G be a group with no proper subgroups having the same exponent and let N be a normal subgroup of G such that $\mathrm{d}(G/N) = d = \mathrm{d}(G)$

but every proper quotient of G/N is $(d-1)$-generated. Then, by Theorem 2.1, we have that G/N is isomorphic to L_k for some monolithic group L, and let $\varphi : L_k \to G/N$ be an isomorphism between them.

First assume that the socle A of L is abelian and complemented. Let q, r, s, θ be as in Theorem 2.2. We observe that $s < r$ by Theorem 2.3 and $k \le r$ by Lemma 4.1. Thus, $\lceil (k+s)/r \rceil \le 2$. As $\mathrm{d}(L/A) \le d-1$, it follows from Theorem 2.2 that $d = \mathrm{d}(G/N) = \theta + \lceil (k+s/r \rceil \le 3$.

So we can assume that A is non-abelian. We want to prove that in this case $k \le |A|$. Let $D = \{(l,\dots,l) \mid l \in L\}$ be the diagonal of L_k and $K/N = \varphi(D)$. Note that for every prime q such that $q \nmid |A|$ the subgroup K contains a Sylow q-subgroup of G.

Let $\pi(A)$ be the set of primes dividing $|A|$. For every prime $q \notin \pi(A)$ we choose a q-element x_q of K of maximum order and for every prime $p \in \pi(A)$ we choose a p-element $x_p \in G$ of maximum order.

If $p \in \pi(A)$, we see that the element $\bar{x}_p = \varphi^{-1}(x_p N) \in L_k$ is of the form $\bar{x}_p = (x_{p,1},\dots,x_{p,k})$, where $x_{p,i} \in l_p A$ for every $i = 1,\dots,k$ and $l_p \in L$ is an element of p-power order. If there exist $x_{p,i}$ and $x_{p,j}$ such that $x_{p,j} = x_{p,i}^a$ for some $a \in A$, by replacing $\bar{x}_p$ by a suitable conjugate, we can assume that $x_{p,j} = x_{p,i}$ (more precisely, we take the conjugate of $\bar{x}_p$ by the element $y = (1,\dots,a,\dots,1) \in L_k$, where a is in the i-th position). We accordingly replace x_p with x_p^z, where $zN = \phi(y)$. Note that the resulting element is still a p-element of G of maximal order. Let $T = \langle K, x_p \mid r \text{ is a prime dividing } |A| \rangle$. Then $\exp(G) = \exp(\langle x_r \mid r \text{ is a prime dividing } |G| \rangle) = \exp(T)$, so $T = G$ by minimality of G.

Let $a = \prod_{p\in\pi(G)} a_{l_p}$, where a_{l_p} is defined as in Lemma 4.2. If $k > a$, then there exists $i, j \in \{1,\dots,k\}$ with $i \ne j$ such that $x_{p,i} = x_{p,j}$ for any $p \in \pi(A)$. Let $H = \{(l_1,\dots,l_k) \in L_k \mid l_i = l_j\}$. We see that H is a proper subgroup of L_k such that that $D \le H$ and $\bar{x}_p \in H$ for every $p \in \pi(A)$. So $\varphi(T) \le H$, but this is a contradiction because $\varphi(T) = \varphi(G) = L_k$. Thus, $k \le a$. Now Lemma 4.2 shows that $a = \prod_{p\in\pi(G)} a_{l_p} \le \prod_{p\in\pi(G)} |A|_p \le |A|$ so $k \le |A|$, as we wanted.

Finally, we can bound $\mathrm{d}(G)$. Assume by contradiction $\mathrm{d}(G) = d > 4$. Then on the one side we have that $\mathrm{d}(L_k) = \mathrm{d}(G/N) = d$, on the other side Lemma 2.4 with $t = d-1$ shows that $\mathrm{d}(L_k) \le d-1$ because $k \le |A| \le |A|^{t-3}$. This contradiction concludes the proof. □

Bibliography

[1] M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, *J. Algebra* **90** (1984), 446–460.

[2] J. Cossey, K. W. Gruenberg and L. G. Kovacs, The presentation rank of a direct product of finite groups, *J. Algebra* **28** (1974), 597–603.

[3] F. Dalla Volta and A. Lucchini, Generation of almost simple groups, *J. Algebra* **178** (1995), 194–223.

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

[5] F. Dalla Volta, A. Lucchini and F. Morini, On the probability of generating a minimally d-generated group, *J. Austral. Math. Soc.* **71** (2001), 177–185.

[6] P. J. Flavell, Finite groups in which every two elements generate a soluble subgroup, *Invent. Math.* **121** (1995), 279–285.

[7] D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.

[8] T. W. Hungerford, *Algebra*, Reprint of the 1974 original, Graduate Texts in Mathematics 73, Springer-Verlag, New York, Berlin, 1980.

[9] E. I. Khukhro and V. D. Mazurov (editors), *Unsolved Problems in Group Theory. The Kourovka Notebook*, no. 17, Russian Academy of Sciences, Institute of Mathematics, Novosibirsk, 2010.

[10] A. Lucchini, Generators and minimal normal subgroups, *Arch. Math* **64** (1995), 273–276.

[11] A. Lucchini, On groups with d-generator subgroups of coprime index, *Comm. Algebra* **28** (2000), 1875–1880.

[12] A. Lucchini and F. Menegazzo, Generators for finite groups with a unique minimal normal subgroup, *Rend. Sem. Mat. Univ. Padova* **98** (1997), 173–191.

[13] P. Shumyatsky, On the Fitting height of a finite group, *J. Group Theory* **13** (2010), 139–142.

[14] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, *Bull. Amer. Math. Soc.* **74** (1968), 383–437.

[15] J. S. Wilson, *Profinite Groups*, London Mathematical Society Monographs N. S. 19, Clarendon Press, Oxford University Press, New York, 1998.

Received September 27, 2010; revised September 30, 2010.

Author information

Andrea Lucchini, Dipartimento di Matematica Pura e Applicata, Università di Padova,
Via Trieste 63, 35121 Padova, Italy.
E-mail: `lucchini@math.unipd.it`

Marta Morigi, Dipartimento di Matematica, Università di Bologna,
Piazza di Porta San Donato 5, 40126 Bologna, Italy.
E-mail: `mmorigi@dm.unibo.it`

Pavel Shumyatsky, Department of Mathematics, University of Brasilia,
Brasilia-DF, 70910-900, Brazil.
E-mail: `pavel@mat.unb.br`