Not every p-group can be generated by elements of the same order

E.A. O'Brien, Carlo M. Scoppola and M.R. Vaughan-Lee

Abstract

For every prime p, we exhibit a finite p-group which cannot be generated by a set of elements, all having the same order. This answers a long-standing question from the Kourovka Notebook.

1 Introduction

In 1990, Czesław Bagiński posed the following problem in the Kourovka Notebook [5, Problem 11.6]:

> Let p be an odd prime. Is it true that every finite p-group possesses a set of generators of equal orders?

Since the semidihedral group of order 16 cannot be generated by elements of the same order, the problem is of interest only for odd primes. Clearly a necessary and sufficient condition for a 2-generator p-group P to fail to be generated by a set of elements, all having the same order, is that the orders of *non-Frattini* elements (those outside of the Frattini subgroup $\Phi(P)$) in each maximal subgroup of P differ from those in the other maximal subgroups. The semidihedral group satisfies this condition, having three maximal subgroups: namely, the cyclic, dihedral, and quaternion groups of order 8. It is the smallest group which does not possess such a generating set.

In 2003, E.F. Robertson and James Wiegold asked the question once more, this time in Group Pub Forum [3], and labelled as *GSO* those (arbitrary finite) groups which can be generated by elements of the same order. Such groups are common: for example, all perfect groups are GSO. They asked for an example of a non-GSO 3-group.

The first author was supported by GNSAGA-INdAM and by EPSRC grant GR/S86259/01 while this paper was written. The second author is a member of GNSAGA-INdAM. 2000 *Mathematics Subject Classification.* Primary 20D15.

The resulting discussion, with contributions by Isaacs, Mann and others, established various properties of GSO groups.

Perhaps the most relevant is the following. Lubotzky & Mann [6] prove that if P is a powerful finite p-group for odd prime p, then the set of all of its elements of order less than the exponent of P generates a proper subgroup, and so P is GSO.

What can we say about p-groups which are not GSO? One easy but critical observation, originally made by Bagiński [1], is that, for an odd prime p, a non-GSO p-group P has exponent at least p^{p+1}.

This can be readily established by induction on order. Since P is not cyclic, it has at least $p+1$ maximal subgroups which satisfy the inductive hypothesis. If the exponent of P is at most p^p, then at least two different maximal subgroups of P are generated by elements of the same order, and so P is generated by these elements.

In this paper we answer the central problem in the negative, by proving the following.

Theorem 1 *Let p be a prime and let G be the finitely-presented group:*

$$\langle a, b \mid a^p,\, b^{p^2},\, [b^p, a],\, (ab^r)^{p^{r+2}}\ (r = 1, 2, \ldots, p-1)\rangle.$$

Let P be the largest p-quotient of G which is both metabelian and of nilpotency class $p^2 - p + 1$. Then P cannot be generated by a set of elements, all having the same order.

In Section 3 we exhibit a group of matrices which satisfies all of the required relations, and show that the specified p-quotient is non-GSO.

Our result is optimal in the sense that P has exponent exactly p^{p+1}, and our proof implies that metabelian p-quotients of G having smaller class have exponent at most p^p.

Theorem 1 also applies to the prime 2. We conjecture that the order of P is $p^{(p^3+p^2-8p+14)/2}$. For $p \leq 11$, we constructed explicitly a power-commutator presentation [9] for the p-quotient P using our implementation of the p-quotient algorithm [7], and so verified our conjecture for these primes.

If we factor P by a maximal subgroup of its centre, which does not contain the last term of the lower central series of P, then we obtain a quotient Q with the same class as P, and Q may also be non-GSO. For example, the 2-group of order 32 has as a central quotient the semidihedral group of order 16.

Applying (recursively) this strategy to the 3-group P of order 3^{13}, we obtained as a quotient a non-GSO group of order 3^{10} and class 7. We have established that all 2-generator 3-groups of order dividing 3^9 are GSO; to do this, we constructed them explicitly using our implementation of the p-group generation algorithm [8] and then constructed appropriate generating sets. We have also constructed non-metabelian 3-groups of order 3^{10} which are non-GSO. (We remark that the

largest non-metabelian class 7 3-quotient of the finitely-presented group G from Theorem 1 has order 3^{23} and is a GSO group.)

Lemma 2 *If we add relations* $[b,a,a,a,a] = [b,a,a,a,b]b^3$ *and* $[b,a,a,a,a,a,a] = b^{-3}$ *to the finite presentation of Theorem* 1*, then the largest metabelian class* 7 3*-quotient of the resulting finitely-presented group has order* 3^{10} *and is non-GSO. No smaller* 2*-generator* 3*-group is non-GSO.*

The statement and proof of Theorem 1 can be readily modified to exhibit infinitely many examples for each prime p: we can choose a sequence (s_i) of integers $3 \le s_1 < s_2 < \ldots < s_{p-1}$ and modify the presentation for G by replacing p^{r+2} by p^{s_r}.

2 Some results on metabelian groups

We first determine explicitly the powers of the basic commutators which arise in evaluating p-th powers of products of elements of a metabelian group. A related result by Hall [4, Theorem 12.3.1] is not sufficiently detailed for our purposes.

Lemma 3 *Let* $a, b \in K$*, a metabelian group, and let* p *be a prime. Denote by* $[b,_r a,_s b]$ *the commutator* $[b, \underbrace{a, a, \ldots, a}_{r}, \underbrace{b, b, \ldots, b}_{s}]$*, where* $r, s \ge 0$*. Then*

$$(ab)^p = a^p b^p \prod_{1 \le r \le p-1, 0 \le s \le p-1} [b,_r a,_s b]^{c_{r,s}}$$

where $c_{r,s} = 0 \bmod p$ *for* $r+s < p-1$*, and if* $r+s = p-1$ *then* $c_{r,s} = (-1)^r \bmod p$*.*

Proof: We apply the Hall collection process [4, Chapter 11] to $(ab)^p$ to obtain the following expansion:

$$(ab)^p = a^p b^p \prod_{1 \le r \le p-1, 0 \le s \le p-1} [b,_r a,_s b]^{c_{r,s}}$$

where

$$c_{r,s} = \sum_{i=\max\{r,s\}}^{p-1} \binom{i}{r}\binom{i}{s}.$$

We obtain the coefficients $c_{r,s}$ as follows. First we write $(ab)^p$ as $abab\ldots ab$. Then for each b in this expression we count the number of as to the right of it. If there are k as to the right of a particular b, then collecting the as past that b will create $\binom{k}{r}$ copies of the commutator $[b,_r a]$. When all the as have been collected, each of these instances of $[b,_r a]$ will have k bs to the right of it. When we collect the bs past one of these instances, $\binom{k}{s}$ copies of the commutator $[b,_r a,_s b]$ will

be created. Hence the original b in the expression $abab\dots ab$ gives rise to $\binom{k}{r}\binom{k}{s}$ copies of $[b,_r a,_s b]$. The value given for $c_{r,s}$ is obtained by adding the contributions from each b in $abab\dots ab$.

Now consider the polynomial

$$\sum_{i=0}^{p-1}(1+x)^i(1+y)^i,$$

where x and y are commuting indeterminates. Expanding, we obtain

$$\sum_{r,s=0}^{p-1} c_{r,s}x^r y^s,$$

which gives

$$(1+x)^p(1+y)^p - 1 = (x+y+xy)\sum_{r,s=0}^{p-1} c_{r,s}x^r y^s.$$

Working modulo p we obtain

$$x^p + y^p + x^p y^p = (x+y+xy)\sum_{r,s=0}^{p-1} c_{r,s}x^r y^s \text{ modulo } p,$$

and hence

$$(x+y+xy)^{p-1} = \sum_{r,s=0}^{p-1} c_{r,s}x^r y^s \text{ modulo } p.$$

The claim now follows. □

While the following lemma is well-known (for example, it can be obtained as a corollary to [2, Theorem 3.2]), we include a direct proof for completeness.

Lemma 4 *Let G be a 2-generator finite metabelian p-group, and let $a \in G\backslash\Phi(G)$. Then a and ag have the same order for all $g \in G'$.*

Proof: Since G is a finite 2-generator p-group, we can find $b \in G$ so that G is generated by a and b. If $g \in G'$ then g can be expressed in the form

$$g = g_1^{\alpha_1} g_2^{\alpha_2} \dots g_k^{\alpha_k}$$

where $g_1, g_2, \dots, g_k$ are commutators of the form $[a, b_1, b_2, \dots, b_m]$ with $m \geq 1$ and $b_1, b_2, \dots, b_m \in \{a, b\}$. Let a have order n. Since G is metabelian, we see that

$$\begin{aligned}(ag)^n &= g^n[g,a]^{\binom{n}{2}}[g,a,a]^{\binom{n}{3}}\dots[g,_{n-1} a] \\ &= \prod_{i=1}^{k}\left(g_i^n[g_i,a]^{\binom{n}{2}}[g_i,a,a]^{\binom{n}{3}}\dots[g_i,_{n-1} a]\right)^{\alpha_i}.\end{aligned}$$

But if $g_i = [a, b_1, b_2, \ldots, b_m]$ then

$$\begin{aligned} & g_i^n [g_i, a]^{\binom{n}{2}} [g_i, a, a]^{\binom{n}{3}} \ldots [g_{i,n-1}\, a] \\ = \;& [[a, b_1]^n [a, b_1, a]^{\binom{n}{2}} [a, b_1, a, a]^{\binom{n}{3}} \ldots [a, b_{1,n-1}\, a], b_2, \ldots, b_m] \\ = \;& [[a^n, b_1], b_2, \ldots, b_m] \\ = \;& 1. \end{aligned}$$

Hence the order of ag divides the order of a. But the same argument shows that the order of $a = (ag)g^{-1}$ divides the order of ag. We conclude that a and ag have the same order. □

We now obtain an upper bound for the nilpotency class of a specific metabelian p-group.

Theorem 5 *Let $m \geq 2$. Let G be the finitely-presented group*

$$\langle a, b \,|\, a^p, b^{p^2}, [b^p, a], (ab^r)^{p^m} \; (r = 1, 2, \ldots, p-1) \rangle.$$

If K is a metabelian p-quotient of G, then K is nilpotent of class at most $m(p-1)$.

PROOF: Observe that the relation $a^p = 1$ implies that $(K')^p \leq \gamma_{p+1}(K)$. Applying Lemma 3, we obtain

$$(ab)^p = a^p b^p [b_{,p-1}\, a][b_{,p-2}\, a, b]^{-1} [b_{,p-3}\, a, b, b] \ldots [b, a_{,p-2}\, b]^{-1} \text{ modulo } \gamma_{p+1}(K).$$

Since a has order p and b^p is central and of order p, the relation $(ab)^{p^m} = 1$ implies

$$([b_{,p-1}\, a][b_{,p-2}\, a, b]^{-1} [b_{,p-3}\, a, b, b] \ldots [b, a_{,p-2}\, b]^{-1})^{p^{m-1}} \leq (\gamma_{p+1}(K))^{p^{m-1}}.$$

Similarly, the relation $(ab^r)^{p^m} = 1$ implies

$$([b^r{}_{,p-1}\, a][b^r{}_{,p-2}\, a, b^r]^{-1} [b^r{}_{,p-3}\, a, b^r, b^r] \ldots [b^r, a_{,p-2}\, b^r]^{-1})^{p^{m-1}} \leq (\gamma_{p+1}(K))^{p^{m-1}},$$

and we conclude that

$$([b_{,p-1}\, a]^r [b_{,p-2}\, a, b]^{-r^2} [b_{,p-3}\, a, b, b]^{r^3} \ldots [b, a_{,p-2}\, b]^{-r^{p-1}})^{p^{m-1}} \leq (\gamma_{p+1}(K))^{p^{m-1}}.$$

These relations for $r = 1, 2, \ldots, p-1$ give

$$[b_{,p-1}\, a]^{p^{m-1}}, [b_{,p-2}\, a, b]^{p^{m-1}}, [b_{,p-3}\, a, b, b]^{p^{m-1}}, \ldots, [b, a_{,p-2}\, b]^{p^{m-1}} \in (\gamma_{p+1}(K))^{p^{m-1}},$$

which implies

$$(\gamma_p(K))^{p^{m-1}} \leq (\gamma_{p+1}(K))^{p^{m-1}},$$

and hence we deduce that

$$(\gamma_p(K))^{p^{m-1}} = \{1\}.$$

Since $a^p = 1$,

$$1 = [b, a^p] = [b, a]^p [b,_2 a]^{\binom{p}{2}} [b,_3 a]^{\binom{p}{3}} \dots [b,_p a],$$

and since b^p is central we have

$$1 = [b^p, a] = [b, a]^p [b, a, b]^{\binom{p}{2}} [b, a,_2 b]^{\binom{p}{3}} \dots [b, a,_{p-1} b].$$

Thus $[b,_p a]$, $[b, a,_{p-1} b] \in (K')^p$. If $k \geq p$ then $\gamma_{k+p-1}(K)$ is the normal closure of elements

$$[b,_p a, a_1, a_2, \dots, a_{k-2}],\ [b, a,_{p-1} b, a_1, a_2, \dots, a_{k-2}]$$

with $a_1, a_2, \dots, a_{k-2} \in \{a, b\}$, and these lie in

$$[(K')^p, \underbrace{K, K, \dots, K}_{k-2}] \leq (\gamma_k(K))^p.$$

It follows that if $k \geq p$ then $\gamma_{k+p-1}(K) \leq (\gamma_k(K))^p$, and so $(\gamma_p(K))^{p^{m-1}} = \{1\}$ implies that $(\gamma_{2p-1}(K))^{p^{m-2}} = \{1\}$, $(\gamma_{3p-2}(K))^{p^{m-3}} = \{1\}$, …, $\gamma_{1+m(p-1)}(K) = \{1\}$, as claimed. □

3 Proof of Theorem 1

We now prove Theorem 1 by exhibiting a group of matrices which satisfies all of the required relations, and showing that the specified p-quotient is non-GSO.

Let $H = \langle c, d \mid c^p,\ d^{p^2},\ [d, c] \rangle$ and let $R = \mathbb{Z}_{p^{p+1}} H$ be the group ring of H over $\mathbb{Z}_{p^{p+1}}$. Let I be the ideal of R generated by $d^p - 1$. Observe that R/I is the group ring over $\mathbb{Z}_{p^{p+1}}$ of an elementary abelian group of order p^2.

Define a group M of matrices

$$\begin{pmatrix} x & r + I \\ 0 & 1 \end{pmatrix}\ x \in H,\ r \in R,$$

with multiplication

$$\begin{pmatrix} x & r + I \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & s + I \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} xy & xs + r + I \\ 0 & 1 \end{pmatrix}.$$

Clearly, M is a finite metabelian p-group.

Let S be the subgroup of M generated by

$$A = \begin{pmatrix} c & (c-1) + I \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} d & I \\ 0 & 1 \end{pmatrix}.$$

We now investigate whether S satisfies the relations of the finite presentation of Theorem 1. It is easy to see that

$$A^r = \begin{pmatrix} c^r & (1 + c + c^2 + \dots + c^{r-1})(c-1) + I \\ 0 & 1 \end{pmatrix}$$

for $r = 1, 2, \ldots$, and hence that

$$\begin{aligned} A^p &= \begin{pmatrix} c^p & (1 + c + c^2 + \ldots + c^{p-1})(c-1) + I \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (c^p - 1) + I \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & I \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

It is also easy to see that $B^p = \begin{pmatrix} d^p & I \\ 0 & 1 \end{pmatrix}$ is central in S and of order p.

We now evaluate $(AB^r)^p$ for $1 \leq r < p$.

$$\begin{aligned} (AB^r)^p &= \begin{pmatrix} cd^r & (c-1) + I \\ 0 & 1 \end{pmatrix}^p \\ &= \begin{pmatrix} d^{pr} & (1 + cd^r + c^2d^{2r} + \ldots + c^{p-1}d^{(p-1)r})(c-1) + I \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

It follows that $(AB^r)^{p^{r+2}} = \begin{pmatrix} 1 & e_r + I \\ 0 & 1 \end{pmatrix}$, where

$$e_r = p^{r+1}(1 + cd^r + c^2d^{2r} + \ldots + c^{p-1}d^{(p-1)r})(c-1).$$

These observations lead to the following theorem.

Theorem 6 *Let J be the ideal of R generated by $d^p - 1, e_1, e_2, \ldots, e_{p-1}$. Let S be the group generated by*

$$A = \begin{pmatrix} c & (c-1) + J \\ 0 & 1 \end{pmatrix}, \; B = \begin{pmatrix} d & J \\ 0 & 1 \end{pmatrix}.$$

Then S satisfies the relations of the finite presentation of Theorem 1.

Remark 7 We can deduce a stronger result which we use below: namely AB^r for $1 \leq r < p$ has order exactly p^{r+2}. Equivalently we show that

$$p^r(1 + cd^r + c^2d^{2r} + \ldots + c^{p-1}d^{(p-1)r})(c-1) \notin J.$$

We find a homomorphism from $\langle d \rangle \to \langle c \rangle$ mapping d^r to c^{-1}, and extend it to a homomorphism from R onto $\mathbb{Z}_{p^{p+1}}\langle c \rangle$ (mapping $c \in R$ to $c \in \mathbb{Z}_{p^{p+1}}\langle c \rangle$). Then

$$p^r(1 + cd^r + c^2d^{2r} + \ldots + c^{p-1}d^{(p-1)r})(c-1) \mapsto p^{r+1}(c-1),$$

and $e_r \mapsto p^{r+2}(c-1)$. If $1 \leq t < p$ and $t \neq r$ then

$$1 + cd^t + c^2d^{2t} + \ldots + c^{p-1}d^{(p-1)t} \mapsto 1 + c + c^2 + \ldots + c^{p-1}$$

and so $e_t \mapsto 0$. It follows that the image of J is the ideal of $\mathbb{Z}_{p^{p+1}}\langle c \rangle$ generated by $p^{r+2}(c-1)$, and clearly this ideal does not contain $p^{r+1}(c-1)$.

We are now in a position to establish Theorem 1. Let

$$G = \langle a, b \,|\, a^p, b^{p^2}, [b^p, a], (ab^r)^{p^{r+2}} \, (r = 1, 2, \ldots, p-1)\rangle,$$

and let P be the largest metabelian p-quotient of G of class $p^2 - p + 1$, as in the statement of Theorem 1. We claim that P is a non-GSO group.

First note that Theorem 5 implies that any metabelian p-quotient of G has class at most $p^2 - 1$. Hence there exists a largest metabelian p-quotient of G, which we call Q. Theorem 6 and Remark 7 imply that the images in Q of a, b, ab, ab^2, …, ab^{p-1} have orders exactly p, p^2, p^3, …, p^{p+1}. Now $a^p = 1$ implies that $G^p \leq \langle b^p, \gamma_p(G)\rangle$, and since b^p is central and of order p, $G^{p^2} \leq \gamma_{2p-1}(G)$. Then $G^{p^3} \leq \gamma_{3p-2}(G)$, …, $G^{p^p} \leq \gamma_{p^2-p+1}(G)$, and hence $Q^{p^p} \leq \gamma_{p^2-p+1}(Q)$. The image of ab^{p-1} in Q has order p^{p+1} and so $Q^{p^p} \neq \{1\}$. It follows that $\gamma_{p^2-p+1}(Q) \neq \{1\}$, and so Q has class at least $p^2 - p + 1$. Hence P is a homomorphic image of Q, and P has class exactly $p^2 - p + 1$.

Let $\overline{a}, \overline{b}$ denote the images of a, b in P. We show that $\overline{a}$, $\overline{b}$, $\overline{a}\overline{b}$, $\overline{a}\overline{b}^2$, …, $\overline{a}\overline{b}^{p-1}$ have orders exactly p, p^2, p^3, …, p^{p+1}.

First consider $\overline{a}\overline{b}^{p-1}$. If it had order dividing p^p then Theorem 5 would imply that P had class at most $p^2 - p$, whereas in fact P has class $p^2 - p + 1$. So $\overline{a}\overline{b}^{p-1}$ has order p^{p+1}.

Now consider $\overline{a}\overline{b}^r$, where $0 < r < p - 1$. Our argument in Remark 7 to show that AB^r has order exactly p^{r+2} can readily be modified to show that $\overline{a}\overline{b}^r$ also has order p^{r+2}. Recall that J is the ideal of R generated by $d^p - 1$, e_1, $e_2, \ldots, e_{p-1}$. If we replace J by the ideal J_1 generated by

$$d^p - 1, e_1, e_2, \ldots, e_{p-2}, \frac{1}{p}e_{p-1},$$

and if we let

$$A_1 = \begin{pmatrix} c & (c-1) + J_1 \\ 0 & 1 \end{pmatrix}, \; B_1 = \begin{pmatrix} d & J_1 \\ 0 & 1 \end{pmatrix}$$

then A_1, B_1 generate a finite metabelian p-group K satisfying the relations

$$A_1^p, B_1^{p^2}, [B_1^p, A_1], (A_1B_1)^{p^3}, \ldots, (A_1B_1^{p-2})^{p^p}, (A_1B_1^{p-1})^{p^p}.$$

The argument given in Remark 7 shows that $A_1B_1^r$ has order exactly p^{r+2}. But, by Theorem 5, K has class at most $p^2 - p$. Thus K is a homomorphic image of P, and $\overline{a}\overline{b}^r$ also has order exactly p^{r+2}.

Clearly $\overline{a}$ and $\overline{b}$ have orders p and p^2. Hence we have shown that the elements $\overline{a}$, $\overline{b}$, $\overline{a}\overline{b}$, $\overline{a}\overline{b}^2$, …, $\overline{a}\overline{b}^{p-1}$ all have different orders. Further, if c is one of these $p+1$ elements, then any non-Frattini element of the maximal subgroup containing c has the form $c^r\overline{b}^{ps}x$ for some $x \in P'$. Lemma 4, together with the fact that $\overline{b}^p$ is central and of order p, implies that $c^r\overline{b}^{ps}x$ has the same order as c. Hence P cannot be generated by a set of elements, all having the same order.

Acknowledgements

We thank M.F. Newman for useful comments on a draft of the paper.

References

[1] C. Bagiński, Some remarks on finite p-groups, Demonstratio Math. **14**, (1981), 279-285.

[2] A. Caranti and C.M. Scoppola, Endomorphisms of two-generated metabelian groups that induce the identity modulo the derived subgroup. *Arch. Math.* **56** (1991), 218-227.

[3] Group Pub Forum. `(http://www.bath.ac.uk/~masgcs/gpf.html)`, 2003.

[4] Marshall Hall, Jr., The theory of groups. The Macmillan Co., New York, 1959.

[5] The Kourovka Notebook. Unsolved problems in group theory. Fifteenth augmented edition, 2002. Edited by V.D. Mazurov and E.I. Khukhro.

[6] Alexander Lubotzky and Avinoam Mann, Powerful p-groups. I. Finite groups. *J. Algebra* **105** (1987), 484-505.

[7] M.F. Newman and E.A. O'Brien. Application of computers to questions like those of Burnside, II. *Internat. J. Algebra Comput.*, **6** (1996), 593–605.

[8] E.A. O'Brien. The p-group generation algorithm. *J. Symbolic Comput.*, **9** (1990), 677–698.

[9] Charles C. Sims. *Computation with finitely presented groups.* Cambridge University Press, 1994.

E.A. O'Brien
Department of Mathematics
University of Auckland
Auckland
New Zealand
obrien@math.auckland.ac.nz

Carlo M. Scoppola
Dipartimento di Matematica Pura ed Applicata
Universita di L'Aquila
Coppito 67010, L'Aquila
Italy
scoppola@univaq.it

M.R. Vaughan-Lee
Christ Church
University of Oxford
OX1 1DP
United Kingdom
michael.vaughan-lee@christ-church.oxford.ac.uk