Bull. Aust. Math. Soc. **82** (2010), 84–98
doi:10.1017/S0004972710000055

ON FINITE p-GROUPS WITH SUBGROUPS OF BREADTH 1

GIOVANNI CUTOLO[✉], HOWARD SMITH and JAMES WIEGOLD[†]

(Received 2 October 2009)

Abstract

We consider finite p-groups G in which every cyclic subgroup has at most p conjugates. We show that the derived subgroup of such a group has order at most p^2. Further, if the stronger condition holds that all subgroups have at most p conjugates then the central factor group has order p^4 at most.

2000 *Mathematics subject classification*: primary 20D15, 20E45; secondary 20D25.
Keywords and phrases: finite p-groups, conjugacy classes, breadth.

Introduction

As is well known, sizes of conjugacy classes provide critical information on the structure of finite groups. One classical research topic in this context is the investigation of the relations between the maximum size of a conjugacy class (of elements, or of subgroups) and the size of the central factor group, the size of the commutator subgroup or, in the case of p-groups, the nilpotency class—[1] contains references to publications in this area. (Throughout this paper p will always denote a prime.)

In agreement with standard terminology, if G is a finite p-group, $x \in G$ and $H \leq G$, we define the breadth of x in H as that number b, denoted by $\mathrm{br}_H(x)$, such that $p^b = |H : C_H(x)|$. The maximum value of $\mathrm{br}_G(x)$, where x runs over G, is the breadth $\mathrm{br}(G)$ of G. Similarly, the subgroup breadth (or s-breadth for short) of H in G is the integer $b = \mathrm{sbr}_G(H)$ such that $p^b = |G : N_G(H)|$. The maximum value of $\mathrm{sbr}_G(H)$, where H runs over the set of all subgroups of G, is called the subgroup breadth $\mathrm{sbr}(G)$ of G, while the cyclic breadth (or c-breadth) $\mathrm{cbr}(G)$ of G is the maximum value of of $\mathrm{sbr}_G(H)$, where H runs over the set of cyclic subgroups only. We shall use $\circ(g)$ to denote the order of a group-element g.

We know from [1, Proposition 1.4], that (finite) p-groups with c-breadth 1 have nilpotency class 3 at most, hence they are metabelian. The primary aim of this note is

The first and second authors express here their deep sense of loss of a first-rate colleague and friend, Jim Wiegold, who passed away at the time that this paper was in the final stages of preparation.
[†]Deceased: 4 August 2009.

to record the fact that the derived subgroup of such a group is extremely constrained in size. Indeed, our main result is the following.

THEOREM A. *Let p be a prime and G be a finite p-group of c-breadth* 1. *Then $|G'| \leq p^2$. Moreover, if $p > 2$ then $\exp G' = \exp(G/Z(G)) = p$.*

By contrast with this result, it is obviously impossible to bound the size of the central factor group of a finite p-group in terms of the cyclic breadth only, for extraspecial p-groups have c-breadth 1 but arbitrarily big central factor group. On the other hand, it is possible to bound $|G/Z(G)|$ in terms of the (usually bigger) subgroup breadth of G, as was first recognized by Macdonald [4]. Macdonald's bounds were not meant to be sharp.

One of the problems discussed in the PhD thesis of Kraus [3] is that of determining the structure of finite 2-groups G satisfying $\mathrm{sbr}(G) = 1$. She showed that such groups satisfy $|G/Z(G)| \leq 16$ and this is the best possible bound (in the process of proving this she also showed that $|G'| \leq 4$). Kraus's argument uses some machine-aided computation that allows her to exclude a number of critical cases; we present here a proof of Kraus's result that avoids such computation. We will also show that the corresponding bound is slightly better for odd primes: if G is a finite p-group, where p is an odd prime, and $\mathrm{sbr}(G) = 1$ then $|G/Z(G)| \leq p^3$. Thus, we shall prove the following theorem.

THEOREM B. *Let p be a prime and G be a finite p-group of s-breadth* 1.

(i) *If $p = 2$ then $|G/Z(G)| \leq 16$.*
(ii) *If $p > 2$ then $|G/Z(G)| \leq p^3$.*

For every prime p there exists exactly one p-group of s-breadth 1, order p^4 and class 3; these groups are listed in [1]. For every such group G we have $|G/Z(G)| = p^3$ and $|G'| = p^2$. As already mentioned, it is also easy to find examples of 2-groups with s-breadth 1 whose central factor group has order 16, one such group being the direct product $D_8 \times Q_8$ of the dihedral and the quaternion groups of order eight. Thus the bounds in Theorems A and B are the best possible. As a matter of fact, granted that if $|G'| = p$ then G has class 2, all structures for G' which are not excluded by Theorem A occur in groups with c-breadth 1 and prescribed class 2 or 3. By contrast, if $\mathrm{sbr}(G) = 1$, we shall see that G' can be cyclic of order four only if G has class 3 (Corollary 1.6).

1. Proof of Theorem A

We start by establishing the bound on the exponents in Theorem A, in the case where p is odd.

LEMMA 1.1. *Let G be a finite p-group of c-breadth* 1.

(i) *If $p > 2$ then $\exp G' = \exp(G/Z(G)) = p$.*
(ii) *If $p = 2$ then $\exp G'$ and $\exp(G/Z(G))$ are at most* 4, *and G^2 is abelian.*

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

PROOF. As observed in the introduction, G has class 3 at most, and so G' is abelian. Our proof splits into three cases according to the value of p. If $p > 3$ then G is regular, hence the result follows immediately from [1, Lemma 1.6]. If $p = 3$ we still have that G^3 is in the kern of G, by the same lemma, hence $(\gamma_3(G))^3 = [G', G^3] = 1$ and for every $x, y \in G$,

$$[x, y^3] = [x, y]^3[x, y, y]^3 = [x, y]^3 \in \langle x \rangle. \qquad (*)$$

We may assume that $(G')^9 = 1$. Suppose that $[a, b]^3 \neq 1$ for some $a, b \in G$ such that $\circ(a) \geq \circ(b)$, and also assume that b has been chosen of minimal order with respect to satisfying this condition. By $(*)$ we have $[a, b]^3 \in \langle a \rangle \cap \langle b \rangle$. Let q be the least power of 3 such that $b^q \in \langle a \rangle$; then $a^{nq} = b^q$ for some $n \in \mathbb{N}$. As $[a, b] = [a, a^{-n}b]$ the minimality of $\circ(b)$ and the fact that $\langle a \rangle \cap \langle b \rangle \neq 1$ yield $(a^{-n}b)^q \neq 1$. Now (see, for instance, [5, p. 49])

$$(a^{-n}b)^3 = a^{-3n}b^3[b, a^{-n}]^3[b, a, a]^{n^2}[b, a, b]^{-5n},$$

and so $(a^{-n}b)^9 = a^{-9n}b^9$ since G^3 is abelian as a subgroup of the kern of G. If 9 divides q then $(a^{-n}b)^q = a^{-nq}b^q = 1$ and we have a contradiction. It follows that $q = 3$. But then $b^3 \in \langle a \rangle$ and $(*)$ yields $[a, b]^3 = [a, b^3] = 1$, a contradiction. Therefore $\exp G' = 3$. By $(*)$ we also have that $G^3 \leq Z(G)$. Thus (i) is proved.

Now consider the case when $p = 2$. Since G^2 is contained in the kern of G we know that $G^2 \leq Z_2(G)$ and $G' \leq Z(G^2)$. Then $[G, G^4] = [G, G^2]^2 = [G^2, G^2]$. Moreover, G^2 is a Dedekind group; if it were hamiltonian then again $(G')^2 \leq (Z(G^2))^2 = 1$, hence the commutator equalities just found would yield the contradiction $(G^2)' = 1$. Therefore G^2 is abelian; the same equalities now show that $G^4 \leq Z(G)$. Finally, for all $a, b \in G$ we have $1 = [a, b^2]^2 = ([a, b]^2[a, b, b])^2 = [a, b]^4$. Thus the proof is complete. □

Note that the exponent of G' and $G/Z(G)$ can actually be 4 in a 2-group with c-breadth 1, the easiest example being provided by the generalized quaternion group of order 16, whose subgroup breadth is 1. This group has class 3; we shall discuss below, in some detail, 2-groups of c-breadth 1 and class 2 (see Example 1.4 and Proposition 1.5).

Next we bound the rank of the derived subgroups of the groups that we are dealing with. The next lemma (together with the previous one and the fact that our groups are metabelian) proves Theorem A in the case when p is odd; as so often happens with problems on conjugacy classes in finite p-groups, the case when $p = 2$ requires separate arguments.

LEMMA 1.2. *Let G be a finite p-group of c-breadth 1. Then G' has rank two at most.*

PROOF. We know that G' is abelian, thus, even if $p = 2$, we may factor out $(G')^p$ and assume that G' has exponent p. This implies that, for every $g \in G$, if $N = N_G(\langle g \rangle)$ and $C = C_G(g)$ then $|[\langle g \rangle, N]| \leq p$, hence $|N/C| \leq p$; therefore $|G : C| \leq p^2$. This means that $\mathrm{br}(G) \leq 2$; also note that $\mathrm{br}_G(g) = 2$ is possible, but in this

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

case necessarily $[g, G] \cap \langle g \rangle = [g, N] \neq 1$. Now, it is known that if $\mathrm{br}(G) = 2$ then either $|G'| = p^2$ or $|G/Z(G)| = |G'| = p^3$ (see [1, Lemma 1.1(v)] for the relevant references), so we assume that the latter equalities hold. If G has class 3 then $G = \langle a, b \rangle Z(G)$, for some $a, b \in G$. Let $g = [a, b]$. Then $G' = \langle g \rangle [g, G]$. But $\mathrm{br}_G(g) = \mathrm{sbr}_G(\langle g \rangle)$, because $g^p = 1$, hence $|G'| \leq p^2$, a contradiction.

Thus G has class 2, and it follows that $G/Z(G)$ is elementary abelian, because an abelian group of order p^3 and exponent p^2 cannot be isomorphic to the central factor group of any group. Let $Z = Z(G)$. If x, y, g are generators of G modulo Z then $G' = \langle [x, y] \rangle \times \langle [y, g] \rangle \times \langle [g, x] \rangle$, in particular $\mathrm{br}_G(g) = 2$ for all $g \in G \setminus Z$; for such g we also have $g^p \neq 1$, as $\mathrm{br}_G(g) > \mathrm{sbr}_G(\langle g \rangle)$.

Consider first the special case when $\exp G = 4$. For every $x \in G \setminus Z$ we have that x has order four and there exists $y \in G$ such that $[x, y] = x^2$. Again, $y \notin Z$, so $[y, t] = y^2$ for some $t \in G$. If $x^2 \neq y^2$ then $t \notin \langle x, y \rangle Z$ and $G = \langle x, y, t \rangle Z$. In this case $[x, G] = \langle x^2, [x, t] \rangle$, hence $[x, t] \notin \langle x^2 \rangle$, and

$$[xy, G] = \langle [xy, y], [xy, t] \rangle = \langle x^2, [x, t] y^2 \rangle.$$

But $y^2 = (xy)^2 \in [xy, G]$ and it follows easily that $y^2 = x^2$. This proves that $Q := \langle x, y \rangle \simeq Q_8$. Let $g \in G \setminus QZ$. The same argument used for x and y shows that $\langle g, h \rangle \simeq Q_8$ for some element h that can certainly be chosen in Q. But then $[h, G] = \langle [h, Q], [g, h] \rangle = \langle h^2 \rangle$ and $\mathrm{br}_G(h) = 1$, a contradiction. Thus $\exp G \neq 4$.

Let $q = (\exp G)/p$. Then $g^q \in [g, G]$ for every $g \in G \setminus Z$ and, even if $p = 2$, now we can say that the mapping given by $g \mapsto g^q$ is an endomorphism of G, two facts that we will use repeatedly. Suppose that $\exp Z = \exp G$, let z be an element of Z of maximal order pq and let $S = \langle z^q \rangle$. Then $|(G/S)'| = p^2$ and there exists $g \in G \setminus Z$ such that $z^q \notin [g, G]$, because otherwise $\mathrm{br}(G/S) = 1$ and hence $|(G/S)'| = p$ by a result in [2]. As $g^q \in [g, G]$ then $\langle zg \rangle \cap [zg, G] = \langle zg \rangle \cap [g, G] = 1$, which is a contradiction. Hence $\exp Z \leq q$. Let a be an element of G of order pq. There exists $b \in G$ such that $[a, b] = a^q$. We claim that b can be chosen such that $b^q = 1$. Indeed, if $b^q \in \langle a \rangle$ then $b^q = a^{nq}$ for some integer n, as $\circ(a) \geq \circ(b)$; in this case $(a^{-n}b)^q = 1$ and we can substitute $a^{-n}b$ for b. Otherwise $b^q \notin \langle a \rangle$; in this case there exists $g \in G$ such that $[b, g] = b^q \neq 1$; as $[a, b] \in \langle a \rangle$ then $g \notin \langle a, b \rangle Z$ and so $G' = \langle [a, b] \rangle \times \langle [b, g] \rangle \times \langle [a, g] \rangle$. Now $[ab, G] = \langle [a, b], [a, g][b, g] \rangle$, hence $b^q = [b, g] \notin [ab, G]$. On the other hand, both $a^q = [a, b]$ and $a^q b^q = (ab)^q$ are in $[ab, G]$, hence $b^q \in [ab, G]$; this contradiction establishes our claim. A similar argument applies for every $c \in G \setminus \langle a, b \rangle Z$: we have $G = \langle a, b, c \rangle Z$ and $[ac, G] = \langle [a, c], [a, b][c, b] \rangle$, so that $[a, b] \notin [ac, G]$. If $\circ(c) < \circ(a)$ then $(ac)^q = a^q = [a, b]$, which is impossible as $(ac)^q \in [ac, G]$; therefore $\circ(c) = \circ(a) = pq$. It follows that $\langle b \rangle Z$ is the set of all elements of G of order at most q. Hence, by arguing for c as we did for a, we obtain that $1 \neq [c, b_1] = c^q$ for some $b_1 \in \langle b \rangle Z$, thus $[c, b] = c^{tq}$ for some $t \in \{1, 2, \ldots, p-1\}$. Now $[ac, G]$ contains $a^q c^q = (ac)^q$ as well as $a^q c^{tq} = [ac, b]$; if $t \neq 1$ then $[a, b] = a^q \in [ac, G]$, a contradiction again. Therefore $t = 1$. What we have proved amounts to saying that b induces on G the (nontrivial, universal) power automorphism given by $g \mapsto g^{1+q}$. We may assume that b has been

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

chosen of minimal order in the coset bZ. Now $1 \neq [g, b] \in \langle b\rangle \cap \langle g\rangle$ for some $g \in G$, but then, since $\langle g^p, b\rangle$ is abelian and $\circ(g^p) \geq \circ(b)$ it is easy to find an integer n such that bg^{np} has order less than $\circ(b)$. This is in contradiction with our choice of b, thus the proof is complete. □

Now that Theorem A has been proved for odd primes we may concentrate on 2-groups.

LEMMA 1.3. *Let G be a finite 2-group such that* $\mathrm{cbr}(G) = 1$. *Then* $|G'| \leq 4$.

PROOF. In view of the previous lemmas we may assume that the abelian group G' has exponent 4 and order eight. Let $Z = Z(G)$. Suppose first that $\mathrm{br}(G) = 2$. Then $|G/Z| = 8$, by a result already mentioned on p-groups of breadth 2 [1, Lemma 1.1(v)], so G/Z is either elementary abelian or dihedral, because no other group of order eight can be isomorphic to the central factor group of any group. In the former case $\exp(G') = \exp(G/Z) = 2$ and we have a contradiction. In the latter case $G = \langle a, b\rangle Z$, where $a^2,\ b^2 \in Z$. Let $c = [a, b]$; then $G' = \langle c\rangle^G$. Now $1 = [a^2, b] = c^a c$ and $1 = [a, b^2] = cc^b$, hence $c^a = c^b = c^{-1}$, so $\langle c\rangle \lhd G$ and $G' = \langle c\rangle$ has order four. Thus the lemma is proved in this case and we may assume that $\mathrm{br}(G) = 3$. Then there exists $a \in G$ such that $G' = [a, G]$. Since $|G : N_G(\langle a\rangle)| \leq 2$ we therefore have $|N_G(\langle a\rangle) : C_G(a)| \geq 4$; it follows that $a^4 \neq 1$ and there exists $b \in N_G(\langle a\rangle)$ such that $[a, b]$ has order four. As a^2 lies in the kern of G it normalizes $\langle b\rangle$, hence $1 \neq [a, b]^2 = [a^2, b] \in \langle a\rangle \cap \langle b\rangle$. Note that $[a, b]^2$ has order two, so we have $[a, b]^2 = a^{2^\alpha} = b^{2^\beta}$ for some $\alpha, \beta \in \mathbb{N}$, and $\alpha > 1$. We may assume that b has been chosen of minimal order subject to the stated conditions. Suppose first that $\langle a, b\rangle$ has class 2, that is, $[a, b, b] = 1$. Then $[a, b] \in \langle a^4\rangle$, as $[a, b]$ has order four, hence $\alpha > 2$. If $\alpha \geq \beta$ let $b_1 = ba^{2^{\alpha-\beta}}$. Then

$$b_1^{2^\beta} = b^{2^\beta} a^{2^\alpha} [a^{2^{\alpha-\beta}}, b]^{2^{\beta-1}(2^\beta-1)} = [a, b]^{2^{\alpha-1}} = 1.$$

This contradicts the minimality of the order of b. Hence we may assume that $\alpha < \beta$. Let 2^u and 2^v be the indices of $\langle a\rangle \cap \langle b\rangle$ in $\langle a\rangle$ and $\langle b\rangle$ respectively; then $u < v$ and $a^{2^u} = b^{-\lambda 2^v}$ for some odd integer λ. Moreover, $u > 1$, because $[a^2, b] \neq 1$, hence $v > 2$. Let $a_1 = ab^{\lambda 2^{v-u}}$; then

$$a_1^{2^u} = a^{2^u} b^{\lambda 2^v} [b^{\lambda 2^{v-u}}, a]^{2^{u-1}(2^u-1)} = [b, a]^{\lambda 2^{v-1}(2^u-1)} = 1.$$

It follows that $\langle a_1\rangle \cap \langle b\rangle = 1$, hence $\langle a_1\rangle \cap \langle a\rangle = 1$, then $[a_1, b^2] = [a, b^2] \notin \langle a_1\rangle$. This is a contradiction, because b^2 is in the kern of G. Therefore $[a, b, b] \neq 1$; this means that a has order eight and $a^2 \in [a, G]$, hence a is inverted (that is, mapped via conjugation to its own inverse) by an element of G. Let x be such an inverter. Then $\mathrm{br}_{\langle a\rangle}(x) = 2$, hence $\mathrm{br}_G(x)$ is either 2 or 3. If $\mathrm{br}_G(x) = 2$ then $G = \langle a\rangle C_G(x)$, hence $\mathrm{br}_{C_G(x)}(xa) = \mathrm{br}_{C_G(x)}(a) = \mathrm{br}_G(a) = 3$, so that xa is an inverter of a of breadth 3. Therefore a must have an inverter of breadth 3, which we again call x. By repeating the above argument for x in place of a, we see that x has order eight and $x^2 \in G'$.

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

Also, $x^2 \notin \langle a^2 \rangle$, as a^2 is inverted by x, hence $G' = \langle a^2, x^2 \rangle$ centralizes a. Thus far we have proved that every element of breadth 3 in G has an inverter of breadth 3 and centralizes G'. But this leads to a contradiction, since x does not centralize a^2 and yet $a^2 \in G'$. This contradiction proves the lemma. □

With this final lemma we have completed the proof of Theorem A.

Before closing the discussion on 2-groups with c-breadth 1 we take a closer look at groups G such that G' is cyclic of order four. We already know that there are such groups G having s-breadth 1 and class 3, the generalized quaternion group of order 16 providing an example. Also the case occurs where $\mathrm{cbr}(G) = 1$ and G has class 2. An example is the following, but we shall see that it is, in a sense, essentially unique; a consequence will be that such groups cannot have s-breadth 1.

EXAMPLE 1.4. Let G be the group in the variety of nilpotent groups of class at most 2 generated by a, b and subject to the extra relations $a^4 = b^4 = c^2$, where $c = [a, b]$, thus $|G| = 64$. Then $G' = \langle c \rangle$ has order four, hence $\mathrm{br}(G) = 2$, and $\mathrm{cbr}(G) = 1$. Indeed, $G^2 = \langle a^2, b^2, c \rangle$ is abelian; if $x \in G^2$ then $x = g^2 c^i$ for some $g \in G$ and integer i, hence x is centralized by the maximal subgroup $G^2\langle g \rangle$ and $\mathrm{br}_G(x) \leq 1$; if $x \in G \setminus G^2$ then $x = a^i b^j c^k$ for some $i, j, k \in \mathbb{N}$ such that i and j are not both even. Then $x^4 = a^{4i} b^{4j} c^{2ij} = c^{2i} c^{2j} c^{2ij} = c^2$, and it follows that $\mathrm{sbr}_G(\langle x \rangle) = 1$. Therefore $\mathrm{cbr}(G) = 1$. On the other hand $\mathrm{sbr}(G) = 2$. Indeed, it is clear that no subgroup of G can have subgroup breadth greater than 2, for such a subgroup would have to be at least 3-generator, hence its normalizer would have at least order 2^4, but $V := \langle a^2 b^2, a^2 c \rangle$ has (subgroup) breadth 2. In fact, $V \simeq V_4$ and we have $V^a = \langle a^2 b^2 c^2, a^2 c \rangle$ and $V^b = \langle a^2 b^2 c^2, a^2 c^{-1} \rangle$; since $c^2 \notin V$ (and hence $c^2 \notin V^a \cup V^b$) it follows that V, V^a and V^b are pairwise distinct. It can be shown that the conjugacy class of V is the only one in G having size 4.

PROPOSITION 1.5. *Let G be a finite 2-group of class 2 such that $\mathrm{cbr}(G) = 1$. If G' is cyclic of order four then G has a central factor isomorphic to the group in Example 1.4.*

PROOF. There exist $a, b \in G$ such that $c := [a, b]$ generates G'. We assume that the pair (a, b) has been chosen such that b has minimal order. Thus $\circ(a) \geq \circ(b)$; actually $\circ(ab^n) \geq \circ(b)$ for all $n \in \mathbb{N}$. Since G^2 is contained in the kern of G we have $c^2 = [a^2, b] = [a, b^2] \in \langle a \rangle \cap \langle b \rangle$. Therefore $c^2 = b^{2^\lambda} = a^{2^{\lambda+\mu}}$ for some $\lambda, \mu \in \mathbb{N}$. By minimality of $\circ(b)$,

$$1 \neq (a^{2^\mu} b)^{2^\lambda} = a^{2^{\lambda+\mu}} b^{2^\lambda} [b, a^{2^\mu}]^{2^{\lambda-1}(2^\lambda - 1)} = c^{2^{\lambda+\mu-1}},$$

hence $\lambda + \mu - 1 \leq 1$. On the other hand, $1 \neq c^2 = [a, b^2]$, so that $b^2 \notin \langle a, c \rangle$; thus $\lambda > 1$. Hence $\lambda = 2$ and $\mu = 0$, that is, $c^2 = a^4 = b^4$, and it follows that $H := \langle a, b \rangle$ is isomorphic to the group of Example 1.4. It is also clear that H is a central factor of G. □

COROLLARY 1.6 (see [3, Theorem 3.5.1]). *If G is a 2-group of class 2 and subgroup breadth 1 then G' has exponent 2.*

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

PROOF. This follows from the previous proposition, since the group of Example 1.4 has s-breadth 2. □

Going back to groups of class 3, it is worth remarking that there exist 2-groups G of class 3 such that G' is cyclic of order four and $\mathrm{cbr}(G) = 1$ which are essentially different from the quaternion group of order 16. For instance, the group G (of class 3 and size 2^8) generated by a, b, c, x, y subject to the relations

$$a^8 = x^2 = y^2 = 1, \quad c = [a, b], \quad a^4 = b^4 = c^2 = [c, a] = [x, y],$$

$$[a, x] = [a, y] = [b, x] = [b, y] = [b, c] = 1$$

is such that $\mathrm{cbr}(G) = 1$, $G' = \langle c \rangle$ has order four and $|G/Z(G)| = 32$.

2. Proof of Theorem B

As anticipated in the introduction, the principal aim of this section will be that of finding a sharp bound for the size of the central factor group of a finite p-group with subgroup breadth 1. We observed that no such (upper) bound exists for groups with cyclic breadth 1.

We begin with two simple and useful lemmas.

LEMMA 2.1. *Let C be a nonabelian 2-group such that $C^2 \leq Z(C)$. Assume that there exist two nontrivial subgroups U, V of C such that every noncentral cyclic subgroup of C contains either U or V. Then every noncentral element of C has order four.*

PROOF. Let x be an element of minimal order in $C \setminus Z(C)$. Let $y \in C \setminus Z(C)$ and suppose that $\circ(y) > \circ(x)$. Then $A := \langle x, y^2 \rangle$ is abelian of exponent $\circ(y^2)$, hence $A = \langle y^2 \rangle \times \langle x_1 \rangle$ for some x_1 which necessarily lies outside $Z(C)$. Minimality of $\circ(x)$ implies that x_1 has the same order as x, hence $A = \langle y^2 \rangle \times \langle x \rangle$. Now let y' be a power of y such that $\circ(y') = \circ(x)$. Then the three cyclic noncentral subgroups $\langle y \rangle$, $\langle y'x \rangle$ and $\langle x \rangle$ have pairwise different socles. This is excluded by the hypothesis, hence we see that all elements of $C \setminus Z(C)$ have the same order, say $2^{\lambda+1}$. Clearly $\exp Z(C) \leq 2^{\lambda+1}$, hence $\exp C = 2^{\lambda+1}$ and $\lambda > 0$. If $\lambda > 1$ the mapping $\theta \colon a \in C \mapsto a^{2^\lambda} \in C$ is an endomorphism, since $C^2 \leq Z(C)$. Let a and b be any two elements of C which are independent modulo $Z(C)$. Then the socles of $\langle a \rangle$, $\langle b \rangle$ and $\langle ab \rangle$ are $\langle a^\theta \rangle$, $\langle b^\theta \rangle$ and $\langle (ab)^\theta \rangle$ respectively, and they are pairwise different. As before, this is a contradiction. Therefore $\lambda = 1$ and the lemma is proved. □

LEMMA 2.2. *Let G be a finite p-group of s-breadth 1 and assume that G has a noncentral element a of order p. Let $b \in G \setminus C_G(a)$ and $C = C_G(H)$, where $H = \langle a, b \rangle$. Then every subgroup of C which is not normal in G contains $[a, b]$. Moreover, if there are such subgroups in C then $|G'| = p^2$ and $H' = \langle [a, b] \rangle$ has order p.*

PROOF. Let $c \in C$; then $\langle c \rangle$ is maximal in $U := \langle a, c \rangle = \langle a \rangle \times \langle c \rangle$. If $U \neq U^b$ then $U_G = \bigcap_{i=0}^{p-1} U^{b^i}$, because U has breadth 1 in G, and hence $U_G = \langle c \rangle$, since $[c, b] = 1$.

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

Thus $\langle c\rangle \lhd G$ in this case. So, if we assume that $\langle c\rangle$ is not normal in G, then $U = U^b$. In this case $U/\langle c\rangle$ is a chief factor of $U\langle b\rangle$, so $[a, b] \in \langle c\rangle$. Since $\langle c\rangle \not\lhd G$ it also follows that $G' > \langle [a, b]\rangle$, hence $|G'| = p^2$ by Theorem A. The lemma follows, since now $[a, b] \in C \cap H = Z(H)$ and $[a, b]^p = [a^p, b] = 1$.

In the situation of Lemma 2.2 we can often draw the conclusion that C is in fact a Dedekind group, as the next lemma shows. However we shall see that this is not always the case.

LEMMA 2.3. *Let C be a finite p-group, and assume that C has an element u of order p such that, for all nonnormal cyclic subgroups $\langle c\rangle$ of C,*

(i) $u \in \langle c\rangle$, *if* $p > 2$, *and*
(ii) $u \in \langle c^4\rangle$, *if* $p = 2$.

Then C is a Dedekind group.

PROOF. Let C be a counterexample of the least possible order. There exist $g, h \in C$ such that h does not normalize $\langle g\rangle$. Hence $u \in \langle g\rangle$ (and $u \in \langle g^4\rangle$, if $p = 2$), and $\langle g, h\rangle$ is a counterexample, hence $C = \langle g, h\rangle$ by minimality. Every subgroup of order p in C which is different from $\langle u\rangle$ is normal and hence central; it follows that $\langle u\rangle$ too is central. Therefore, if $Z(C)$ is cyclic then C has only one subgroup of order p. Since C is not Dedekind, this means that C is a generalized quaternion group of order greater than eight (see, for example, [6, 5.3.6]). But in this case C has a nonnormal cyclic subgroup of order four, which is excluded by the hypothesis. Hence $Z(C)$ is not cyclic, so C has two (distinct) central subgroups A and B, each of order p, such that $A \neq \langle u\rangle \neq B$. Since C/A and C/B inherit the hypothesis from C, they are both Dedekind, by minimality of $|C|$. As C is not abelian, it follows that $p = 2$, C has class 2 and C' has exponent 2. Since C is 2-generator, $|C'| = 2$. There are only two possibilities for the socle of a noncentral cyclic subgroup X of C: it is either C' (if $X \lhd C$) or $\langle u\rangle$ (if $X \not\lhd C$). By Lemma 2.1 this implies that all noncentral elements of C have order four. But C has a nonnormal cyclic subgroup, which must have order greater than four, by hypothesis. This is a contradiction, and the proof is complete. □

Easy examples of non-Dedekind 2-groups in which all nonnormal subgroups contain the same element of order two are the generalized quaternion groups of order greater than eight and the nonabelian semidirect product of two cyclic groups of order four. This explains the necessity of treating the cases $p = 2$ and $p > 2$ separately in the previous lemma.

We can use Lemma 2.3 to refine Lemma 2.2.

COROLLARY 2.4. *Let G be a finite p-group of s-breadth 1 and assume that G has a noncentral element a of order p. Let $b \in G \setminus C_G(a)$ and $H = \langle a, b\rangle$. If $C := C_G(H)$ is not a Dedekind group then $p = 2$ and $[a, b]$ is not a square in H.*

PROOF. Suppose that C is not Dedekind, and let $u = [a, b]$. Then $p = 2$ and we may choose $c \in C$ such that $\langle c\rangle \not\lhd C$ and $c^2 = u$, as follows from Lemmas 2.2 and 2.3.

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

Now suppose that $u = h^2$ for some $h \in H$. Then hc has order two, so $|[hc, G]| \leq 2$, because G has s-breadth 1. We have $[hc, C] = [c, C] \neq 1$, hence $[hc, G] = [c, C]$, and $|[c, C]| = 2$. Lemma 2.2 yields $|H'| = 2$ and $H' \leq \langle c \rangle$. If $h \notin Z(H)$, then $H' = [h, H] = [hc, H] = [c, C]$, so $[c, C] \leq \langle c \rangle$. This is impossible, as $\langle c \rangle \not\lhd C$. Thus $h \in Z(H)$, hence $hc \in C$. Lemma 2.2 shows that all elements of order two in C are central, hence $hc \in Z(C)$, but then $c \in Z(C)$, a contradiction. □

COROLLARY 2.5. *Let G be a finite 2-group of s-breadth 1 and assume that G has a subgroup $H \simeq D_8$. Then $G = HC$, where $C = C_G(H)$ is a Dedekind group, and $|G/Z(G)| \leq 16$.*

PROOF. H is generated by two involutions, each of which has breadth 1 in G. Therefore C has index 4 in G and $G = HC$. Since the generator of H' is a square in H, Corollary 2.4 shows that C is a Dedekind group. The result follows. □

We are now in a position to address the proof of Theorem B. The odd-prime case is settled by the following result.

THEOREM 2.6. *Let p be an odd prime and let G be a finite p-group such that $\mathrm{sbr}(G) = 1$. Then $|G/Z(G)| \leq p^3$.*

PROOF. Let $Z = Z(G)$ and suppose that G has the minimum possible size for a counterexample. If $N \lhd G$ and $N \cap G' = 1$ then $N \leq Z$ and $Z(G/N) = Z/N$, hence G/N still is a counterexample and $N = 1$ by minimality of $|G|$. We know from Theorem A that G' is elementary abelian and $|G'| \leq p^2$.

Assume first that $|G'| = p$. Then there exists a 2-generator subgroup $H \leq G$ such that $H' = G'$ and so $G = HC$, where $C = C_G(H)$. Also, there exists $a \in H$ such that $\langle a \rangle \not\lhd H$, hence $\langle a \rangle \cap G' = 1$. But $a^p \in Z$, therefore $a^p = 1$. Now Corollary 2.4 shows that C is abelian. Therefore $C = Z$, hence $|G/Z| = p^2$ in this case.

Now suppose that $|G'| = p^2$. Then $G' = \langle a \rangle \times \langle b \rangle$ for some a and b of order p. If G has class 2, both $\langle a \rangle$ and $\langle b \rangle$ are normal. If we let $A/\langle a \rangle = Z(G/\langle a \rangle)$ and $B/\langle b \rangle = Z(G/\langle b \rangle)$ then $|G/A| = |G/B| = p^2$ by the previous paragraph. Moreover, $Z = A \cap B$, thus, in order to prove that $|G/Z| \leq p^3$ we only need to exclude the possibility that $G = AB$. If this is the case then every $g \in G$ has the form $g = uv$ for some $u \in A$ and $v \in B$ and $[g, G] = [u, A][v, B]$ is one of 1, $\langle a \rangle$, $\langle b \rangle$ and G', so $[g, G] \neq \langle ab \rangle$. It follows that $Z(G/\langle ab \rangle) = Z/\langle ab \rangle$. However, this is impossible, since the first part of this proof shows that $Z(G/\langle ab \rangle)$ has index p^2. This contradiction shows that $G \neq AB$, hence $|G/Z| = p^3$ if G has class 2. If G has class 3, then let $x \in G' \setminus \gamma_3(G)$. Then $C := C_G(G') = C_G(x)$, hence $|G/C| = p$. Let $x \in H \leq C$ and suppose that $H \not\lhd C$. Then $G = CN_G(H)$, because $\mathrm{sbr}_G(H) = 1 = \mathrm{sbr}_C(H)$. So $G' = \langle x \rangle^G \leq H$ and $H \lhd G$. Therefore $C/\langle x \rangle$ is a Dedekind group, hence abelian. Thus $C' \leq \langle x \rangle$. Since x was arbitrarily chosen in $G' \setminus \gamma_3(G)$ and G' is elementary abelian, it follows that C is abelian. Let $g \in G \setminus C$. Then $Z = C_C(g)$. Since $\mathrm{br}_G(g) \leq 2$ we have proved that $|G/Z| \leq p^3$ in this case as well. □

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

It is perhaps worth noting that the proof also shows that $|G/Z(G)| = p^2$ if (and only if) $|G'| = p$. This is, however, a property shared by all p-groups whose central factor group has size at most p^3.

For any prime p, there are p-groups G of s-breadth 1 and class 3, hence such that $|G'| = p^2$ and $|G/Z(G)| = p^3$; examples of this type are given in [1]. Also the case where G has class 2, $\mathrm{sbr}(G) = 1$, $|G'| = p^2$ and so $|G/Z(G)| = p^3$ occurs for any odd prime p: an example is given by $G = ((\langle a\rangle \rtimes \langle b\rangle) \times \langle c\rangle) \rtimes \langle d\rangle$, where a has order p^2 while b, c, d have order p, $a^p = [a, b]$, $c = [a, d]$ and $\langle a^p, b, c, d\rangle$ is abelian.

The rest of this paper will be concerned with 2-groups. A special case that we have already settled is that of 2-groups with a dihedral subgroup of order eight, in Corollary 2.5. It is important to remark that groups with s-breadth 1 having a central factorization like that in Corollary 2.5 actually occur. Indeed, it is not hard to see that the nondirect central product W of D_8 and Q_8 has s-breadth 1 (the same holds for the corresponding direct product). This group has the property that $W' = Z(W)$ has order two, hence $|W/Z(W)| = 16$. Thus in the case of 2-groups the bound for the size of the central factor group is not as good as that for p-groups of odd order, even in the special case when the derived subgroup has order two—whereas Theorem 2.6 gives the smallest conceivable bound, namely p^2, in the corresponding case when p is odd. However, the presence of a quotient isomorphic to W is the only obstruction to having such a small central factor group also when $p = 2$.

PROPOSITION 2.7. *Let G be a 2-group such that $\mathrm{sbr}(G) = 1$ and $|G'| = 2$. Then either $|G/Z(G)| = 4$ or G has a central subgroup N such that G/N is isomorphic to the central (nondirect) product of D_8 and Q_8. In the latter case $|G/Z(G)| = 16$.*

PROOF. Let N be a normal subgroup of G which is maximal with respect to satisfying $N \cap G' = 1$. Let $F = G/N$. Since $Z(F) = Z(G)/N$ it will be enough to show that either $|F/Z(F)| \leq 4$ or F is isomorphic to the central product $D_8 Q_8$. Clearly F' is contained in all nontrivial normal subgroups of F; thus $Z(F)$ is cyclic. Assume that $|F/Z(F)| > 4$; then F has elements a, b such that $\langle a\rangle^b \neq \langle a\rangle$. Let $H = \langle a, b\rangle$; then $F = HC$ where $C = C_F(H)$, because $|F'| = 2$. If $a^2 \neq 1$ then $F' \leq \langle a^2\rangle$ because $F^2 \leq Z(F)$, and we have the contradiction $\langle a\rangle \lhd F$. Therefore $a^2 = 1$, hence C is a Dedekind group by Lemma 2.2. Since $Z(F)$ is cyclic and $|F/Z(F)| > 4 = |F/C|$ it follows that $C \simeq Q_8$. Next, $H^2 \leq Z(F) = Z(C)$. Hence $|H| \leq 8$ and so $H \simeq D_8$. The proof is complete. □

Corollary 2.5 shows that if G is a 2-group of s-breadth 1 such that $|G/Z(G)| > 16$ then G has no dihedral subgroup of order eight. In this case the involutions in G, together with 1, must form an abelian subgroup of exponent 2: otherwise G would have a dihedral subgroup of order greater than eight, but such dihedral 2-groups have s-breadth greater than 1. We will find strong constraints on the structure of G under the hypothesis that this subgroup is not central.

LEMMA 2.8. *Let G be a finite 2-group of s-breadth 1, and assume that G has no dihedral subgroup of order eight. Let a be a noncentral involution in G and let*

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

$b \in G \setminus C_G(a)$. If $H = \langle a, b\rangle$ and $C = C_G(H)$ then $H = V \rtimes \langle b\rangle$, where $V = \langle a, a^b\rangle$ is noncyclic of order four, and $|C/Z(C)| \le 4$. Moreover, $\langle b^2\rangle \lhd G$ and b^2 is not a square in C, and:

(i) *if C is not abelian, all elements of $C \setminus Z(C)$ have order four;*
(ii) *if C is hamiltonian then b has order four and $C' = H' = \langle aa^b\rangle$;*
(iii) *if C is not a Dedekind group then b has order eight and $C' = \langle aa^b b^4\rangle$.*

PROOF. Let $V = \langle a, a^b\rangle$. If $[a, a^b] \ne 1$ then V is dihedral. Since $\mathrm{br}_G(a) = 1$ then $V \simeq D_8$, and this is excluded by hypothesis. Thus $[a, a^b] = 1$ and V is noncyclic of order four. Also, $H = V\langle b\rangle$. It is easy to check that $H \cap C = Z(H) = \langle aa^b, b^2\rangle$ and $H' = \langle aa^b\rangle$. If $b^2 = x^2$ for some $x \in C$ then $x^{-1}b$ has order two and $\langle a, x^{-1}b\rangle \simeq D_8$, a contradiction. Hence b^2 is not a square in C; as a special case, $b^2 \ne 1$. More precisely, $b^2 \notin V$, otherwise $|H| = 8$ and, again, $H \simeq D_8$. Also note that $\langle b^2\rangle = \langle b\rangle \cap \langle b\rangle^a = \langle b\rangle_G$, because G has s-breadth 1, hence $\langle b^2\rangle \lhd G$. Now assume that C is hamiltonian. Then $Z(C)$ has exponent 2 and so b has order four, as $b^2 \in Z(C)$; it follows that $H = V \rtimes \langle b\rangle$. Let z be the nontrivial element of C'. Then $z \ne b^2$, because z is a square in C. Arguing as above but with ab in place of b, we also have that $z \ne (ab)^2 = aa^b b^2$. Let $c \in C \setminus Z(C)$; what we have just noticed shows that $(bc)^2 = b^2 z \notin \langle aa^b, z\rangle \le [bc, G]$. If $z \ne aa^b$ this implies the contradiction $\mathrm{sbr}_G(\langle bc\rangle) > 1$. Therefore $z = aa^b$, hence $C' = H'$. Thus (ii) is proved.

Part (i) of the statement is obvious when C is a Dedekind group, hence from now on we may assume that C is not Dedekind and prove (i) and (iii) and that $V \cap \langle b\rangle = 1$ in this case. By Lemma 2.2, all subgroups of C not containing $u := aa^b$ are normal in G; moreover, it follows from Lemma 2.3 that there exists $c \in C$ such that $u = c^2$ and $\langle c\rangle \not\lhd C$, and u is not a square in H, by Corollary 2.4. This latter fact shows that $u \notin \langle b\rangle$. Since $V \cap \langle b\rangle \le V \cap Z(H) = \langle u\rangle$ it follows that $V \cap \langle b\rangle = 1$. Next we show that $|C'| = 2$. Assume that this is false, so $C' = G'$ has order four. Suppose that X is either $\langle b^2\rangle$ or a subgroup of order two in $C' \cap Z(G)$ different from $\langle u\rangle$. Then $X \lhd G$. Denote by bars images modulo X. Then $\bar a$ is an involution in $\bar G$, not centralized by $\bar b$, and either $\bar H \simeq D_8$ or $|\bar G'| = 2$. Lemma 2.2 and Corollary 2.5 show that $C^* := C_{\bar G}(\bar H)$ is a Dedekind group. Actually, both C^* and $\bar C$ are hamiltonian, since $\bar C' \ne 1$, as $|C'| = 4$, and $\bar C \le C^*$. Assume first that $b^4 \ne 1$, and let b_1 be a power of b of order four. Then $b_1 \in Z(C)$ and $d := b_1 c$ is an element of order four in C, because $b_1^2 \ne u = c^2$. Since $d^2 \ne u$ we also have $\langle d\rangle \lhd G$, so $d^2 \in Z(G)$, and $d \notin Z(C)$, so $\langle d^2\rangle = [d, C] \le C'$. Thus we may set $X = \langle d^2\rangle$ and argue modulo X as shown above. We obtain $\bar b^2 \in Z(C^*)$ and so $\bar b^4 = 1$, that is, $b^4 = d^2 = ub_1^2$. As $u \notin \langle b\rangle$ this is a contradiction, hence $b^4 = 1$. Now set $X = \langle b^2\rangle$ and follow the argument again. Let $\bar Z = Z(\bar C)$. As b^2 is not a square in C, if $g \in Z$ and so $\bar g^2 = 1$ then $g^2 = 1$ and hence $g \in Z(C)$—recall from Lemma 2.2 that all elements of order two in C are central. It also follows that $C^4 = 1$, because $\bar C^2 \le \bar Z$. By [2], since $|C'| = 4$ there exists $x \in C$ such that $\mathrm{br}_C(x) = 2$, and hence $\mathrm{br}_C(xb) = 2$ also. From $\mathrm{cbr}(G) = 1$ it follows easily that $\langle x\rangle \cap G' \ne 1 \ne \langle xb\rangle \cap G'$, hence $x^2, x^2b^2 \in C'$. So we have $b^2 \in C'$, and hence $b^2 = [x, y]$ for some $y \in C$. Thus $x, y \notin Z$, hence $\bar x$ and $\bar y$ both

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

have order four. But they commute; it follows that $y \in \langle x\rangle Z \leq C_G(x)$, a contradiction. This shows that $|C'| = 2$. Then all noncentral cyclic subgroups of C contain either C' (if normal) or $\langle u\rangle$ (if not normal), hence all elements of $C \setminus Z(C)$ have order four, by Lemma 2.1.

Let $d \in C_G(c) \setminus \langle c\rangle Z(C)$. Then $\circ(d) = 4$; moreover, $d^2 \neq u$, otherwise $(cd)^2 = 1$, hence $cd \in Z(C)$ and $d \in \langle c\rangle Z(C)$. Thus $\langle d\rangle \lhd G$, so $C' = \langle d^2\rangle$. The same argument can be repeated for cd in place of d, thus showing that $\langle (cd)^2\rangle = C' = \langle d^2\rangle$ and $(cd)^2 = d^2$. This is false, so we deduce that $C_G(c) = \langle c\rangle Z(C)$. But $|C : C_G(c)| = 2$, as $|C'| = 2$, hence $|C/Z(C)| = 4$. Finally, we establish (iii). Firstly $b^8 = 1$, because $C^4 = 1$. $[bc, G]$ contains both $u = [bc, a]$ and $C' = [bc, C]$, hence $[bc, G] = G'$. As $\mathrm{sbr}(G) = 1$, this implies that $\langle bc\rangle \cap G' \neq 1$. Now, C has a noncentral normal subgroup $\langle y\rangle$, otherwise u would be the square of all noncentral elements of C and C would be hamiltonian. Then $C' = \langle y^2\rangle$ and $G' = \langle u, y^2\rangle$. If $b^4 = 1$ then $ub^2 = (bc)^2 \in G'$, hence $b^2 \in G'$. But, as we know, $b^2 \neq u$, moreover $b^2 \neq y^2$, because b^2 is not a square in C. Then $b^2 = uy^2$, but this implies that $(ab)^2 = ub^2 = y^2$, which is another contradiction: by arguing for ab as we did for b we see that $(ab)^2$ cannot be a square in C. This contradiction proves that b has order eight. It follows that $C' = \langle ub^4\rangle$ and the proof is complete. □

It is worth remarking that case (iii) above actually occurs, and in this case the structure of G is prescribed. Indeed, let $H = V \rtimes \langle b\rangle$ as in Lemma 2.8, with $\circ(b) = 8$, and $K = \langle d\rangle \rtimes \langle c\rangle$, where, d and c have order four and $d^c = d^{-1}$. Then form the central product HK, by letting $b^4 = c^2d^2$ and $c^2 = aa^b$, the generator of H'. Finally, let $G_0 = HK \times E$, where E is an elementary abelian 2-group. It can be checked that $\mathrm{sbr}(G_0) = 1$. Of course, H has a noncentral involution, a, and $C_{G_0}(H) = \langle b^2\rangle KE$ is not a Dedekind group (and G_0 has no subgroups isomorphic to D_8). Conversely, by using Lemma 2.8 and its proof, a relatively short extra argument proves that in case (iii) the subgroup HC has exactly the structure just described for G_0. Having completed the proof of Theorem B, one can use the information that $|G/Z(G)| \leq 16$ to deduce that $G = HC$. Thus G is isomorphic to the group G_0 just defined.

LEMMA 2.9. *Let G be a 2-group with s-breadth 1 and suppose that G has a noncentral element of order two. Then $|G/Z(G)| \leq 16$.*

PROOF. Let a be noncentral involution in G, hence $C_a := C_G(a)$ has index 2 in G. Suppose, for a contradiction, that $|G/Z(G)| > 16$. Then G has no dihedral subgroup of order eight, by Corollary 2.5, hence we may adopt the notation and conclusions of Lemma 2.8. We will often use this lemma throughout this proof, without further notice. Note that $C = C_a \cap C_b$, where $C_b := C_G(b)$ has index at most 4 in G, since $|G'| = 4$ by Theorem A and Proposition 2.7. Therefore $|G : C| \leq 8$. We know from Lemma 2.8 that $|C/Z(C)| \leq 4$. If $|G : C| \leq 4$ then $G = HC$ and $Z(C) \leq Z(G)$, hence $|G/Z(G)| \leq 16$, a contradiction. Thus we may assume that $|G : C| = 8$. Then $G = C_aC_b$. Moreover, $a \notin N_G(\langle b\rangle)$, so there exists $x \in N_{C_a}(\langle b\rangle) \setminus C_b$; note that $G = C\langle a, b, x\rangle$. Also note that since $[b, x] \in \langle b\rangle$ while $u = aa^b \notin \langle b\rangle$ and $|G'| = 4$

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

we must have $[b, x] = b_0$ and $G' = \langle u \rangle \times \langle b_0 \rangle$, where b_0 generates the socle of $\langle b \rangle$. Suppose first that C is abelian. Then $C_C(x) \leq Z(G)$; since $|G/Z(G)| > 16$ it follows that $G = CC_x$, where $C_x = C_G(x)$, because $|G : C_x| \leq |G'| = 4$. In this latter case $b = cb_1$ for some $c \in C$ and $b_1 \in C_x$. If $H_1 = \langle a, b_1 \rangle$ then it is easily checked that $[a, b_1] \neq 1 \neq [x, c]$ and $x, c \in C_G(H_1)$. Therefore, at the expense of substituting b_1 for b if needed, we may assume that C is not abelian. Denoting by bars images modulo $\langle b^2 \rangle$ (we know that $\langle b^2 \rangle \lhd G$), we have $\bar{H} \simeq D_8$, hence $\bar{C}_1 := C_{\bar{G}}(\bar{H})$ is a Dedekind group, and $|G : C_1| = 4$ by Corollary 2.5. Then C is a maximal subgroup of C_1; as x centralizes a and normalizes $\langle b \rangle$ it follows that $C_1 = C\langle x \rangle$. Moreover $C' \not\leq \langle b^2 \rangle$ (see Lemma 2.8), so $\bar{C}$ is hamiltonian and $\bar{C}_1 = \bar{C} \times \bar{X}$, where $|\bar{X}| = 2$. Since x was defined up to multiplication by elements of C there is no loss in assuming $x \in X$, hence $x^2 \in \langle b^2 \rangle$. Two cases are possible: either b has order four and C is hamiltonian, or b has order eight and C is not a Dedekind group. In the latter case we may further assume $x^2 = 1$, for $[b, x] = b^4$ in this case; if $x^2 = b^4$ we may substitute xb^2 for x, while if $x^2 = b^2$ we have $(xb)^2 = x^2b^2b^4 = 1$ and so $\langle a, xb \rangle \simeq D_8$, a contradiction. In the case when C is hamiltonian we cannot have $x^2 = 1$, otherwise $\langle x, b \rangle \simeq D_8$, hence $x^2 = b^2$.

In either case let $A = \langle a, x \rangle = \langle a \rangle \times \langle x \rangle$. Then $A \cap V = \langle a \rangle$, hence $a^b \notin A$ and $A^b \neq A$. For all $c \in C$ we have $A^c \cap V = \langle a \rangle$; since A has just two conjugates, $A^c = A$. It follows that $[C, x] \leq A \cap G' \leq \langle x^2 \rangle$, hence C normalizes $\langle x \rangle$. As a matter of fact $[C, x] = 1$: this is obvious when C is not hamiltonian (as $x^2 = 1$). In the other case it is enough to check that $[c, x] = 1$ if $c \in C$ is such that $c^2 \neq 1$, that is, $c^2 = u$. If $[c, x] \neq 1$, then $[c, x] = x^2$, hence $(cx)^2 = u$, and we have $(abcx)^2 = (ab)^2(cx)^2[ab, cx] = ub^2ub^2 = 1$, so $\langle a, abcx \rangle \simeq D_8$, a contradiction once again. Therefore $[C, x] = 1$ in either case.

If C is hamiltonian, now consider $S := \langle a, cx \rangle$, where c is an element of order four in C, so $(cx)^2 = ub^2 \neq 1$. Clearly S is abelian; since $u = aa^b$ and $\langle a, u, b^2 \rangle$ has rank three we have $u, a^b \notin S$. Then $S^b \neq S$. Let d be an element of C not centralizing c, so $[cx, d] = [c, d] = u$. Then $S^d \neq S$. On the other hand $a \notin S^b$, hence $S^d \neq S^b$. We have found three different conjugates of S, and this is a contradiction.

If C is not hamiltonian, let $U = \langle c, x \rangle$, where $c \in C$ is such that $\langle c \rangle \not\lhd C$; hence $c^2 = u$. Also U is abelian, and $b^4 \notin U$ because $\langle u, x, b^4 \rangle$ has rank three. As $x^b = xb^4$ it follows that $U \neq U^b$. On the other hand, if d is an element of C not normalizing $\langle c \rangle$, then $U \cap HC = U^b \cap HC = \langle c \rangle \neq \langle c \rangle^d = U^d \cap HC$, hence U^d is different from both U and U^b, thus providing a contradiction. Now the proof is complete. □

THEOREM 2.10. *Let G be a 2-group with s-breadth 1. Then $|G/Z(G)| \leq 16$.*

PROOF. We may assume that G has the least possible order for a counterexample, so that all nontrivial normal subgroups of G have nontrivial intersection with G'. An immediate consequence is that the socle S of $Z(G)$ is contained in G'. Assume first that $Z(G)$ is cyclic. By Lemma 2.9 it follows that G has only one element of

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press

order two, hence G is a generalized quaternion group (see, for instance, [6, 5.3.6]). From $\mathrm{sbr}(G) = 1$ it easily follows that $|G| \leq 16$, a contradiction. Therefore $Z(G)$ is not cyclic, so $S = G'$. In other words, G has class 2 and $G' \simeq V_4$. Let A_1, A_2, A_3 be the subgroups of order two in G'. For each i let $C_i/A_i = Z(G/A_i)$ and let N_i be a normal subgroup of G which is maximal with respect to the condition $N_i \cap G' = A_i$. If $|G/C_i|, |G/C_j| \leq 4$ for some i, j such that $i \neq j$, then $C_i \cap C_j$ is a central subgroup of index at most 16 in G and we have a contradiction. Therefore, up to relabelling the A_i, we may assume that G/N_1 and G/N_2 are both isomorphic to the central product of D_8 and Q_8 (see Proposition 2.7). Now, $N_1 \cap N_2 \cap G' = A_1 \cap A_2 = 1$, hence $N_1 \cap N_2 = 1$; it follows that $G' = Z(G) = G^2$ and $\exp G = 4$. Let X be the set of all $x \in G$ such that xN_1 is a noncentral involution in G/N_1. For all $x \in X$, Lemma 2.9 shows that $x^2 \neq 1$; on the other hand $N_1 \cap G^2 = A_1$, hence x^2 is the generator of A_1. If $a \in N_1$ the same holds for $ax \in X$, so $x^2 = (xa)^2 = x^2 a^x a$ and $a^x = a^{-1}$. Thus, every element of X induces by conjugation the inverting map on N_1, therefore N_1 is abelian. By Lemma 2.9 the socle of N_1 is $N_1 \cap Z(G) = A_1$ hence N_1 is cyclic, and $|N_1| \leq 4$ since $\exp G = 4$. Then $|G/C_G(N_1)| \leq 2$. Now, the structure of G/N_1 shows that every subgroup of index 2 in G must contain some element of X. Hence there exists $x \in X \cap C_G(N_1)$. We have shown that x acts like inversion on N_1, therefore $|N_1| = 2$. But then $|G| = |N_1|\,|G/N_1| = 2^6$ and so $|G/Z(G)| = 16$, because $|Z(G)| = 4$. This is a contradiction, and the proof is complete. □

With this last result, the proof of Theorem B is also complete.

Acknowledgements

The first author is sincerely grateful to the Department of Mathematics of Bucknell University for its warm hospitality. The authors wish to thank Debbie Kraus for her valuable assistance.

References

[1] G. Cutolo, H. Smith and J. Wiegold, 'The nilpotency class of p-groups in which subgroups have few conjugates', *J. Algebra* **300**(1) (2006), 160–170.
[2] H.-G. Knoche, 'Über den Frobenius'schen Klassenbegriff in nilpotenten Gruppen', *Math. Z.* **55** (1951), 71–83.
[3] D. Kraus, 'Bounds concerning conjugacy in finite p-groups', PhD Thesis, University of Wales College of Cardiff, 1995.
[4] I. D. Macdonald, 'Some explicit bounds in groups with finite derived groups', *Proc. London Math. Soc.* (3) **11** (1961), 23–56.
[5] S. McKay, *Finite p-groups*, Queen Mary Maths Notes, 18 (University of London, Queen Mary, School of Mathematical Sciences, London, 2000).
[6] D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd edn, Graduate Texts in Mathematics, 80 (Springer, New York, 1996).

GIOVANNI CUTOLO, Università degli Studi di Napoli 'Federico II', Dipartimento di Matematica e Applicazioni 'R. Caccioppoli', Via Cintia—Monte S. Angelo, I-80126 Napoli, Italy
e-mail: cutolo@unina.it

HOWARD SMITH, Department of Mathematics, Bucknell University, Lewisburg, PA 17837, USA
e-mail: howsmith@bucknell.edu

JAMES WIEGOLD, School of Mathematics, Cardiff University, Cardiff CF24 4Y, UK

https://doi.org/10.1017/S0004972710000055 Published online by Cambridge University Press