

On core-2 groups

GIOVANNI CUTOLO, HOWARD SMITH AND JAMES WIEGOLD

ABSTRACT: A group G is *core-2* if and only if $|H/H_G| \leq 2$ for every $H \leq G$. We prove that every core-2 nilpotent 2-group of class 2 has an abelian subgroup of index at most 4. This bound is the best possible. As a consequence, every 2-group satisfying the property core-2 has an abelian subgroup of index at most 16.

KEYWORDS: Finite 2-groups, normal subgroups, normal core, breadth.

MATH. SUBJ. CLASSIFICATION (2000): 20D15.

1. Introduction

The present paper continues a series of investigations on the structure of *core-finite* groups, that is, groups G in which the factor H/H_G is finite for every subgroup $H \leq G$, where H_G denotes the normal core of H in G . If, moreover, the sizes of the factors H/H_G are bounded by an integer n then we say that G is *core- n* . Every core-finite locally finite group is core- n for some integer n and has an abelian subgroup of finite index, as was proved in [1] (see also [7]). Here some hypothesis on G is certainly necessary, in order to avoid counterexamples given by groups like Tarski monsters. Also, the minimal possible index of an abelian subgroup in a locally finite core- n group can be bounded in terms of n only (see [2]). By an argument in [6] (and by the Mal'cev Local Theorem), the problem of finding such a bound reduces to the case when G is a finite p -group for some prime p , in which case n may be taken to be a power of p . The question of determining a sharp bound for core- p (finite) p -groups has been addressed in [6] and [3]. It turned out that the exact bound is p^2 if $p \neq 2$. Thus, if p is an odd prime then every core- p locally finite p -group has an abelian subgroup of index less than or equal to p^2 , and, for every prime p , there exist finite p -groups without abelian subgroups of index p . Not surprisingly, the case of 2-groups with the property core-2 seems to be rather more difficult to deal with. For instance, the nilpotency class of a core- p finite p -group can be at most 3 if p is odd, while the example of dihedral groups shows that it can be arbitrarily high if $p = 2$. Still, we know of no example to disprove the conjecture that the exact bound is 4 (that is, p^2) also in the case $p = 2$. Computer calculation done with the package GAP (see [4]) confirms this conjecture for all 2-groups of order at most 2^8 .

The aim of this paper is to solve the problem for groups of class 2. We prove that the conjecture holds true in this case.

Theorem. *Every core-2 nilpotent 2-group of class 2 has an abelian subgroup of index 4.*

The central product of a dihedral and a quaternion group of order 8 is a core-2 group of class 2 in which no maximal subgroup is abelian (see [3], Example 2.5). Thus the lower bound for the index of an abelian subgroup given by the theorem cannot be improved in this case.

By an easy argument (see for instance the proof for Corollary 2.9 in [3]), this implies that every core-2 nilpotent 2-group of class 3 has a normal abelian subgroup of index 16 at most. Also, results in [3] (Lemma 2.10, Lemma 2.12 and Corollary 2.14) ensure that every 2-group G with property

core-2 has a subgroup of index 2 which has nilpotency class 2 unless G itself has class 3. Thus the above theorem yields the following corollary:

Corollary. *Let G be 2-group with the property core-2. If G is nilpotent of class 3 then it has a normal abelian subgroup of index 16, otherwise it has a normal abelian subgroup of index 8 at most.*

That the abelian subgroup may be taken normal follows from the fact that all core-2 groups are metabelian ([3], Lemma 2.1) and a theorem by Gillam [5].

As noted above, the result given by the Corollary might well be not the best possible. We hope to investigate the problem of determining the exact bound for arbitrary core-2 groups in future.

Both the theorem and the corollary improve on analogous results from [3] by lowering the bounds given there. A further improvement is that the proofs presented here are self-contained, whereas the proofs in [3] depended, at a critical stage, on (part of) the computation done with GAP that we have mentioned above. Indeed, the main object of the next section will be a new proof of a key lemma from [3], where this computation was used. However, we do not mean to underestimate the usefulness to our research of a package like GAP. We are happy to acknowledge the enormous help that the availability of this package has given to us, thanks to the possibility of testing several conjectures and building useful examples.

As regards notation, we use V_4 , D_8 and Q_8 to denote the Klein 4-group, the dihedral and the quaternion group of order 8 respectively. Also, $H < G$ means that H is a maximal subgroup of G . Finally, $\text{br}_G(x)$ denotes the *breadth* of the element x in the finite 2-group G , defined by the equality $2^{\text{br}_G(x)} = |G : C_G(x)|$, while $\circ(x)$ is the order of x .

2. Centralizers in core-2 groups

We make silent use of the following properties established in [3].

Lemma 2.1 (see [3], Lemma 2.2). *Let G be a core-2 nilpotent 2-group of class 2. Then the Frattini subgroup G^2 of G is contained in $Z(G)$, so that $\exp G' \leq 2$.*

The key property of core-2 groups is the following (which actually characterizes them among 2-groups). Let G be a 2-group satisfying core-2, and let u, v be nontrivial elements of G . Let $H = \langle u, v \rangle$. Then $H^2 \triangleleft G$ and $|H/H_G| \leq 2$. Even if $H_G = H$ this implies that one of the subgroups of index 2 in H , that is, one of $H^2\langle u \rangle$, $H^2\langle v \rangle$ and $H^2\langle u, v \rangle$, is normal in G . So, for some $h \in \{u, v, uv\}$ we have $H^2\langle h \rangle \triangleleft G$ and hence $[G, h] \leq H^2$, as $|H^2\langle h \rangle/H^2| \leq 2$. If we further assume that G has nilpotency class 2, then $[G, h] \leq \text{Soc } H^2$, since $\exp[G, h] \leq 2$ by Lemma 2.1. In particular, $\text{br}_G(h)$ cannot exceed the rank of $\text{Soc } H^2$, which is at most 3 (and is at most 2 if H is abelian). Without further explicit reference we will almost always apply the core-2 property in this form.

Core-2 groups without elements of breadth 1 will play an important role throughout the paper. There are several limitations on their subgroups.

Lemma 2.2. *Let G be a core-2 nilpotent 2-group of class 2. Assume that G has no elements of breadth 1. Let $H \leq G$ and let $Z = Z(G)$. Then:*

- (i) *if H is cyclic and normal in G then $H \leq Z$;*
- (ii) *if $|H| = 8$ then H is abelian;*
- (iii) *the elements of order at most 2 form a subgroup $G_{[2]}$ in G , and $|G_{[2]} : G_{[2]} \cap Z| \leq 2$;*
- (iv) *if $a \in G_{[2]} \setminus Z$ then $G_{[2]} \leq C_G(a) = \langle a \rangle Z$;*
- (v) *if H is maximal in G then $Z(H) \leq Z$.*

Proof. (i) Let $H = \langle x \rangle \triangleleft G$. Then $[G, x] \triangleleft \langle x \rangle$. But $\exp[G, x] \leq 2$ by Lemma 2.1, and hence $|[G, x]| \leq 2$; i.e., $\text{br}_G(x) \leq 1$. Since G has no element of breadth 1 this gives $x \in Z$, as required.

(ii) Assume that H is a non-abelian subgroup of G of order 8. Then H is 2-generator. By the core-2 property $[G, h] \leq H^2$ for some $h \in H \setminus Z(H)$. But $|H^2| = 2$; hence $[G, h] = H^2$ and so $\text{br}_G(h) = 1$, a contradiction.

(iii) Let V be a subgroup of G generated by two different involutions. Then V is dihedral of order at most 8, because G has class 2. It follows from (ii) that V is isomorphic to V_4 . Then the core-2 property yields $V \cap Z \neq 1$. Part (iii) follows easily from this.

(iv) As $G_{[2]}$ is abelian $G_{[2]} \leq C_G(a)$. Let $b \in C_G(a) \setminus \langle a \rangle$ and set $A = \langle a, b \rangle$. By the core-2 property $[G, x] \leq \text{Soc } A^2$ for some $x \in \{a, b, ab\}$. But $\text{Soc } A^2 = \text{Soc} \langle b^2 \rangle$ has order at most 2; hence $\text{br}_G(x) \leq 1$. By hypothesis $\text{br}_G(x) \neq 1$ and so $x \in Z$. Thus $x \in \{b, ab\}$ and $b \in \langle a \rangle Z$, whence (iv) holds.

(v) If $x \in Z(H)$ then $\text{br}_G(x) \leq 1$; hence $x \in Z$. \square

The next result is basic in our approach to core-2 groups. It was first proved in [3], with the help of computer calculation. Indeed the proof in [3] consists in showing that if the result were false then there would be a counterexample of order 2^8 , a possibility that could be ruled out by computation done with GAP. We provide here a proof (really a proof of that final step) that eliminates the need for using computers.

Lemma 2.3 (see [3], Lemma 2.8). *Let G be a core-2 nilpotent 2-group of nilpotency class 2 and let $x \in G \setminus Z(G)$. Then $C = C_G(x)$ has an abelian subgroup of index 2.*

Proof. By the Mal'cev Local Theorem we may assume that G is finite. Let G be a counterexample of the minimal possible order. The argument in [3], Lemma 2.8, steps (i)–(v), ensures the following:

$$|G| = 2^8, \quad C \triangleleft G, \quad C' = G' = Z(G) = G^2 \text{ has order 8}, \quad Z(C) = C' \langle x \rangle.$$

Hence $\exp G = 4$. Also, $|C/Z(C)| = 8$. Since C has no abelian subgroup of index 2 it follows that $C_C(a) = \langle a \rangle Z(C)$ and so $\text{br}_C(a) = 2$ for all $a \in C \setminus Z(C)$. If b is another element of C then $[a, C] = [b, C]$ if and only if $aZ(C) = bZ(C)$. For, if $[a, C] = [b, C]$ and $aZ(C) \neq bZ(C)$ then $U := \langle a, b \rangle Z(C)$ would be maximal in C ; hence $C' = [U, C] \leq [a, C]$, whereas $|C'| = 8$. Therefore the seven maximal subgroups of C' are precisely the subgroups $[C, a]$ where a ranges over a transversal of $Z(C)$ in C deprived of the central element. Let us call c the nontrivial element of $[G, x]$ (i.e., $c = [x, y]$ for all $y \in G \setminus C$; note that x has breadth 1 in C). There are exactly four maximal subgroups of $G' = C'$ not containing c , say N_1, \dots, N_4 . Let $i \in \{1, 2, 3, 4\}$. Let $\bar{G} = G/N_i$ and $\bar{x} = xN_i$. Then $\bar{x} \notin Z(\bar{G})$. Assume that \bar{G} has an abelian subgroup $\bar{A} = A/N_i$ of index 2. If $x \in A$ then $\bar{A} = C_{\bar{G}}(\bar{x})$; hence $C = A$, so $C' \leq N_i$, a contradiction. If $x \notin A$ then $C = (A \cap C) \langle x \rangle$ and again $C' \leq N_i$. This proves that G/N_i has no abelian subgroups of index 2. Since $|G'/N_i| = 2$, by Lemma 2.6 (i) of [3] there exists a normal subgroup K_i of G such that $K_i \cap G' = N_i$ and G/K_i is isomorphic to the central product of D_8 and Q_8 . Since $[K_i, G] \leq N_i$ it follows that $c \notin [K_i, G]$; hence $[K_i, x] = 1$ and $K_i \leq C$. Also, $|G/K_i| = 32$. As $|G| = 2^8$ and $|N_i| = 4$ we get $|K_i/N_i| = 2$. Let $a_i \in K_i \setminus N_i$, so $K_i = N_i \langle a_i \rangle$. Now let j be any subscript from $\{1, 2, 3, 4\}$ and different from i . Then $N_i \neq N_j$ yields $a_i Z(C) \neq a_j Z(C)$; hence $[a_i, a_j] \neq 1$ by an above remark. Also $\langle [a_i, a_j] \rangle = N_i \cap N_j$, as the latter intersection has order 2. Since $[a_i, a_j]$ is contained in exactly three maximal subgroups of G' these are N_i, N_j and $\langle [a_i, a_j], c \rangle$, which makes sure that $[a_i, a_j]$ does not belong to N_k for any third subscript k different from both i and j ; hence $[a_i, a_j] \neq [a_i, a_k]$. A further consequence is that a_i, a_j and a_k must be independent modulo $Z(C)$. Note that this last remark implies that $a_4 \in a_1 a_2 a_3 Z(C)$.

Now we claim $x^2 = c$. For every $i \in \{1, 2, 3, 4\}$ there exists $y \in C_G(a_i) \setminus C$, because $\text{br}_G(a_i) = \text{br}_C(a_i) = 2$. Then $c = [x, y] = [a_i x, y] \in [G, x] \cap [G, a_i x]$. Suppose that $x^2 = 1$. Apply the property core-2 to $\langle a_i, x \rangle$. We have $[G, a_i] = N_i \not\leq \langle a_i, x \rangle^2 = \langle a_i^2 \rangle$; hence this latter subgroup contains either $[G, x]$ or $[G, a_i x]$. Thus $c \in \langle a_i^2 \rangle$ and we get the contradiction $c = a_i^2 = N_i$. Therefore $x^2 \neq 1$. The intersection among any three of the four subgroups N_1, \dots, N_4 is trivial. Thus x^2 does not belong to at least two of them, say N_i and N_j . Then $\langle a_i, x \rangle^2$ is not $[G, a_i]$. By property core-2 again it is either

$[G, x]$ or $[G, a_i x]$; hence $c \in \langle a_i, x \rangle^2$. Similarly $c \in \langle a_j, x \rangle^2$. Since $a_i^2 \neq c \neq a_j^2$, if $c \neq x^2$ it follows that $c = a_i^2 x^2 = a_j^2 x^2$, and so $1 \neq a_i^2 = a_j^2 \in N_i \cap N_j = \langle [a_i, a_j] \rangle$. Thus $\langle a_i, a_j \rangle \simeq Q_8$, contradicting Lemma 2.2 (ii). Therefore $c = x^2$.

The elements of order 2 in C commute pairwise, by Lemma 2.2 (iii); hence at most one of a_1, \dots, a_4 can have order 2. We may assume that a_1 has order 4. By what we saw earlier the three commutators $[a_1, a_2]$, $[a_1, a_3]$ and $[a_1, a_4]$ are pairwise different, so they are the nontrivial elements of N_1 . Since $1 \neq a_1^2 \in N_1$ one of these three commutators is a_1^2 . We may assume that $a_1^2 = [a_1, a_2]$. Then $a_2^2 \notin N_1$, otherwise $a_2^2 \in N_1 \cap N_2 = \langle a_1^2 \rangle$ and $\langle a_1, a_2 \rangle$ would be nonabelian of order 8, against Lemma 2.2 (ii). Thus a_2 has order 4. By repeating for a_2 the argument used for a_1 we get $a_2^2 = [a_2, a_i]$ for some $i \in \{3, 4\}$, say $i = 3$. Once again, $a_3^2 \notin N_2$ and $[a_3, a_i]$ for some $i \in \{1, 4\}$. So we have $N_2 = \langle a_1^2 \rangle \times \langle a_2^2 \rangle$ and $N_3 = \langle a_2^2 \rangle \times \langle a_3^2 \rangle$. Now $c \in C' \setminus (N_2 \cup N_3) = \{a_1^2 a_3^2, a_1^2 a_2^2 a_3^2\}$. Let us work out $[a_1, a_3]$. This commutator does not belong to N_2 , by the above. Since $c \notin N_2$ and so $C' \setminus N_2 = cN_2$ we have $[a_1, a_3] = cg$ for some $g \in N_2$. From $[a_1, a_3] \in N_1 \cap N_3$ and $c \notin N_1 \cup N_3$ it follows that $g \in N_2 \setminus (N_1 \cup N_3) = \{a_1^2 a_2^2\}$. Thus $[a_1, a_3] = a_1^2 a_2^2 c$. Finally, let $b = a_1 a_2 a_3$. Again as we learned previously $a_4 \in bZ(C) = bC' \cup bxC'$. Also $b^2 = a_1^2 a_2^2 a_3^2 [a_1, a_2][a_2, a_3][a_1, a_3] = a_1^2 a_2^2 a_3^2 c$.

The proof will be completed by splitting it into two cases, according to the possible values of c .

Case 1 — $c = a_1^2 a_2^2 a_3^2$.

In this case $b^2 = 1$. If $a_4 \in bxC'$ then $a_4^2 = x^2 = c$ and so $c \in N_4$, a contradiction. Hence $a_4 \in bC'$ and $a_4^2 = 1$. As already remarked, there exists $y \in C_G(a_4) \setminus C$, and both $[G, y]$ and $[G, a_4 y]$ contain c . Now $\langle a_4, y \rangle^2 = \langle y^2 \rangle$ cannot equal $[G, a_4] = N_4$. By property core-2 it follows that $\langle y^2 \rangle = \langle c \rangle = [G, u]$ where u is either y or $a_4 y$. But then $c = x^2 = u^2 = [x, u]$ and $\langle x, u \rangle \simeq Q_8$. This is impossible by Lemma 2.2 (ii).

Case 2 — $c = a_1^2 a_3^2$.

In this case $b^2 = a_1^2 a_2^2 a_3^2 c = a_2^2$ belongs to $N_2 \cap N_3$, hence not to N_4 . Then $a_4 \notin bC'$ and so $a_4 \in bxC'$. Hence $a_4^2 = b^2 x^2 = a_2^2 c$ and $c = a_2^2 a_4^2$. Recall that $\bar{G} = G/K_1$ is isomorphic to the central product of D_8 and Q_8 , and $K_1 = N_1 \langle a_1 \rangle$. We have $[a_3, a_4] = [a_3, a_1 a_2] = (a_1^2 a_2^2 c) a_2^2 = a_3^2$. In particular $a_3^2 \notin N_1$. Also, $[a_2, a_3] = a_2^2 \notin N_1$. Since $N_1 = G^2 \cap K_1$ it follows that $a_2 K_1$ and $a_3 K_1$ are noncommuting elements of order 4 in \bar{G} . Hence $Q = \langle a_2 K_1, a_3 K_1 \rangle \simeq Q_8$. Therefore $D := C_{\bar{G}}(Q) \simeq D_8$. Since $\bar{G} = DQ$ and $Q \leq C/K_1$ there exists $y \in G \setminus C$ such that yK_1 is an element of order 2 in D . In particular $[y, a_2] \in K_1 \cap N_2 = \langle a_1^2 \rangle$. If $[y, a_2] \neq 1$ replace y with ya_1 , another representative of yK_1 . Then the following hold:

$$y^2 \in K_1 \cap G^2 = N_1, \quad [y, a_2] = 1, \quad [y, a_3] \in K_1 \cap N_3 = \langle [a_1, a_3] \rangle, \quad [y, x] = c. \quad (\ddagger)$$

Let $H := \langle y, a_2 \rangle$. Then $H^2 = \langle y^2, a_2^2 \rangle$ contains one of $[G, a_2] = N_2$, $[G, y]$ and $[G, a_2 y]$. Assume that one of the latter two cases occur. Whichever of $[G, y] \leq H^2$ or $[G, a_2 y] \leq H^2$ holds, then $c \in H^2$, as $c = [x, y] = [x, a_2 y]$, and also $[a_3, y] \in H^2$, because $[a_3, a_2 y] = a_2^2 [a_3, y]$ and $a_2^2 \in H^2$. The former relation gives $H^2 = \langle c, a_2^2 \rangle \simeq V_4$, which in turn implies $y^2 \neq 1$ and $[a_1, a_3] = a_1^2 a_2^2 c \notin H^2$. Thus $[a_3, y] \in H^2$ and (\ddagger) yield $[a_3, y] = 1$. Moreover $y^2 \in H^2 \cap N_1 = \langle ca_2^2 \rangle = \langle a_4^2 \rangle$; hence $y^2 = a_4^2$. Now consider the abelian subgroup $A := \langle y, a_3 \rangle$. We have $A^2 = \langle a_4^2, a_3^2 \rangle = N_4$. This is impossible by property core-2, since then A^2 contains neither $[G, a_3] = N_3$ nor any of $[G, y]$ and $[G, a_2 y]$, given that these two latter subgroups both contain c . This contradiction proves that $H^2 = \langle y^2, a_2^2 \rangle = N_2$. Then $y^2 \in H^2 \cap N_1 = \langle a_1^2 \rangle$ and $y^2 = a_1^2$. This also means $y^2 = (a_1 a_4)^2$, which suggests to apply property core-2 to $U := \langle y, a_1 a_4 \rangle$. As above, commuting with x gives $c \in [G, y] \cap [G, a_1 a_4 y]$. Furthermore, for all $i \in \{1, 2, 3, 4\}$ we have $a_1 a_4 \notin a_i Z(C)$ and so $[C, a_1 a_4] \neq N_i$, because of one of the observations made at the beginning of this proof. Thus $c \in [G, a_1 a_4]$ as well. So $c \in U^2$ by core-2. On the other hand from $[y, a_1 a_4] = [y, a_1 b x] = [y, a_3 x] = [y, a_3] c$ we get $U^2 = \langle a_1^2, [y, a_3] c \rangle$. As $c \neq a_1^2 [y, a_3] c$ because $a_1^2 \notin N_3$, we must have $c = [y, a_3] c$. Thus $[y, a_3] = 1$ again, and $A = \langle y, a_3 \rangle$ is abelian. Now $A^2 = \langle a_1^2, a_3^2 \rangle$, so $[a_2, a_3] = [a_2, y a_3] = a_2^2 \notin A^2$. Hence property core-2 yields $[G, y] \leq A^2$. Therefore $[a_1, y] \in A^2 \cap N_1 = \langle a_1^2 \rangle$. Finally consider $V := \langle y, a_1 \rangle$. The above yields $V^2 = \langle a_1^2 \rangle$. From $c \in [G, y] \cap [G, a_1 y]$ it follows that V^2 does not contain any of $[G, a_1]$, $[G, y]$ and $[G, a_1 y]$. By core-2

this is a contradiction, which proves the lemma. \square

3. Core-2 groups with noncentral involutions

In this section we shall examine those core-2 nilpotent 2-groups of class 2 that have some element of order 2 not contained in the centre. It turns out that such groups must either have elements of breadth 1 or central factor group of order 8. By Lemma 2.3 this implies that the theorem in the introduction holds for such groups.

Throughout this section, if x is a nontrivial element of the 2-group G we shall write x^* for the element of order 2 in $\langle x \rangle$; that is, $\langle x^* \rangle = \text{Soc}\langle x \rangle$.

Lemma 3.1. *Let G be a core-2 nilpotent 2-group of class 2. Assume that G has a noncentral involution a and no elements of breadth 1. Assume that $|G/Z(G)| > 8$. Then, for every $b \in G \setminus \langle a \rangle Z$,*

- (i) *at least one element h among b and ab has breadth 2 in G and is such that $[G, h] = \langle h^* \rangle \times \langle [a, h] \rangle$;*
- (ii) *if $|G/Z(G)| > 16$ only one of b and ab has breadth 2 in G .*

Proof. Apply the core-2 property to the subgroup $H = \langle a, b \rangle$. For some $h \in \{a, b, ab\}$ we have $[G, h] \leq \text{Soc } H^2$. Now, $H^2 = \langle b^2, [a, b] \rangle = \langle (ab)^2, [a, b] \rangle$, so $\text{br}_G(h) \leq 2$. As $b \notin \langle a \rangle Z(G)$ we have $h \notin Z(G)$. Then $\text{br}_G(h) = 2$ since G has no elements of breadth 1. Lemma 2.2 (iv) gives $\text{br}_G(a) > 2$; hence $h \neq a$. It also follows that H^2 is not cyclic, so that $H^2 = \langle h^2 \rangle \times \langle [a, h] \rangle$ and $[G, h] = \text{Soc } H^2 = \langle h^* \rangle \times \langle [a, h] \rangle$. Part (i) is proved. To prove (ii) note first that Lemma 2.2 (iv) yields $C_G(b) \cap C_G(ab) \leq C_G(a) = \langle a \rangle Z(G)$. Since $a \notin C_G(b)$ it follows that $C_G(b) \cap C_G(ab) = Z(G)$. If both b and ab have breadth 2 this implies $|G/Z(G)| \leq 16$. Thus also (ii) is proved. \square

For the sake of later reference we state the next obvious remark as a lemma. The following one also is doubtless well-known.

Lemma 3.2. *Let b and c be elements of the group G such that $[G, b] \cap [G, c] = 1$. Then $[b, c] = 1$ and $C_G(bc) = C_G(b) \cap C_G(c)$.*

Proof. Let $g \in C_G(bc)$. Then $[bc, g] = 1$ and so $[b, g]^c = [c, g]^{-1} \in [G, b] \cap [G, c] = 1$. Thus $g \in C_G(b) \cap C_G(c)$. The statement follows. \square

Lemma 3.3. *For a prime p , let A be an elementary abelian p -group of rank greater than 3. Let \mathcal{S} be a set of subgroups of A such that the following conditions are satisfied:*

- (i) *every element of \mathcal{S} has order p^2 ;*
- (ii) *every two different elements of \mathcal{S} have nontrivial intersection;*
- (iii) *A is generated by the elements of \mathcal{S} .*

Then $\bigcap \mathcal{S}$ has order p .

Proof. Let H and K be two distinct elements of \mathcal{S} . We shall show that every element of \mathcal{S} contains the (nontrivial) subgroup $H \cap K$. Consider elements of \mathcal{S} not contained in HK first. Let $X \in \mathcal{S}$ be such that $X \not\leq HK$. Then $|X \cap HK| \leq p$. Both $X \cap H$ and $X \cap K$ are nontrivial and contained in $X \cap HK$; hence $X \cap H = X \cap HK = X \cap K$. As $|H \cap K| = p$ this gives $H \cap K \leq X$. Now let Y be an element of \mathcal{S} contained in HK . Since HK has rank 3, by condition (iii) there exists $X \in \mathcal{S}$ such that $X \not\leq HK$. Then $1 \neq X \cap Y \leq X \cap HK$, and the latter intersection is $H \cap K$ by the above. So $H \cap K = X \cap Y \leq Y$. This proves that $\bigcap \mathcal{S} = H \cap K$. \square

Lemma 3.4. *Let G be a core-2 nilpotent 2-group of class 2. Assume that G has a noncentral involution a and no elements of breadth 1. Let $\mathcal{B} = \{b \in G \mid \text{br}_G(b) = 2\}$ and further assume that $|G/Z(G)| > 16$. Then:*

- (i) *for every $b, c \in \mathcal{B}$ we have $[b, G] \cap [c, G] \neq 1$;*
- (ii) *$G' = \langle [b, G] \mid b \in \mathcal{B} \rangle$;*
- (iii) *if $|G'| > 8$ then $\bigcap_{b \in \mathcal{B}} [b, G]$ has order 2.*

Proof. Let $b, c \in \mathcal{B}$ and assume that $[b, G] \cap [c, G] = 1$. Then $A := \langle b, c \rangle$ is abelian by Lemma 3.2. Further, $b^* \in [b, G]$ and $c^* \in [c, G]$ by Lemma 3.1; hence $b^* \neq c^*$, so $A = \langle b \rangle \times \langle c \rangle$. By the core-2 property $\text{Soc } A^2 = \langle b^*, c^* \rangle = [x, G]$ for some $x \in \{b, c, bc\}$. If $x = b$ then $c^* \in [b, G] \cap [c, G]$, a contradiction, so $x \neq b$. Similarly $x \neq c$. Hence $x = bc$. In particular, $\text{br}_G(bc) = 2$, so that Lemma 3.2 gives $C_G(bc) = C_G(b) = C_G(c)$. Also, for suitable u and v in G we have $[b, u] = b^* = [bc, v]$. Then $[c, v] = [b, uv] \in [b, G] \cap [c, G] = 1$. Hence $v \in C_G(c) = C_G(bc)$, which is impossible as $[bc, v] = b^* \neq 1$. This proves (i).

Part (ii) follows from the fact that G is generated by $\{a\} \cup \mathcal{B}$, because of Lemma 3.1 (i). Finally, if $|G'| > 8$, we may apply Lemma 3.3 to $\mathcal{S} = \{[G, b] \mid b \in \mathcal{B}\}$ to obtain that $K := \bigcap_{b \in \mathcal{B}} [b, G]$ has order 2. \square

Lemma 3.5. *Let G be a core-2 nilpotent 2-group of class 2. Assume that G has a noncentral involution a and no elements of breadth 1. Further assume that $|G/Z| > 16$, where $Z = Z(G)$. Then all elements of $G \setminus \langle a \rangle Z$ have the same order $\exp G$ and $\exp G = 2 \exp Z$.*

Moreover, if $2^\lambda = \exp G > 4$ then the mapping $g \in G \mapsto g^{2^{\lambda-1}} \in G$ is an endomorphism whose kernel is $\langle a \rangle Z$ and which maps every $g \in G \setminus \langle a \rangle Z$ to g^ .*

Proof. The core of the proof is the following claim:

Let b be an element of minimal order in $G \setminus \langle a \rangle Z$. If $\circ(b) \leq \exp(Z)$ then:

- (i) $\circ(b) = \exp(Z)$ and $Z = \langle z \rangle \times Z_1$ where $\exp(Z_1) < \exp(Z)$ and $z^* = [a, b]$;
- (ii) for all $c \in G \setminus \langle a, b \rangle Z$ we have $\circ(b) = \circ(c^2)$ and $c^* = [a, b]$.

To prove this claim, let $z \in Z$ be such that $\circ(b) \leq \circ(z)$. By Lemma 2.2 (iv) all involutions in G lie in $\langle a \rangle Z$; hence $\circ(b) > 2$ and $\circ(ab) > 2$. Also $(ab)^4 = b^4$ by Lemma 2.1, so $\circ(b) = \circ(ab)$. In view of Lemma 3.1, at the expense of replacing b by ab we may assume that $\text{br}_G(b) = 2$ and hence $[b, G] = \langle b^* \rangle \times \langle [a, b] \rangle$. Of course $\text{br}_G(zb) = 2$ and so $[b, G] = [zb, G] = \langle (zb)^* \rangle \times \langle [a, b] \rangle$. The minimality of $\circ(b)$ yields $\langle b, z \rangle = \langle b \rangle \times \langle z \rangle$. Then $(zb)^*$ is either z^* or z^*b^* , according to whether $\circ(b) < \circ(z)$ or $\circ(b) = \circ(z)$; in any case $(zb)^* \neq b^*$. Also, by the above, $(zb)^* \in \langle b^*, [a, b] \rangle \setminus \langle [a, b] \rangle$. Hence $(zb)^* = [a, b]b^*$; that is, $[a, b] = (zb)^*b^*$. Assume that $\circ(b) < \circ(z)$. Then $[a, b] = z^*b^*$. On the other hand z has a power z_1 of the same order as b . By substituting z_1 for z in the argument just set out we get $(z_1b)^* = z_1^*b^*$ and $[a, b] = z_1^*$. This is a contradiction because $z_1^* = z^*$. Therefore $\circ(b) = \circ(z)$ and so $[a, b] = z^*$. This also shows that $[a, b]$ belongs to all cyclic subgroups of maximal order in Z . Part (i) of the claim follows.

Now let $c \in G \setminus \langle a, b \rangle Z$. Assume that $\circ(c) = \circ(b)$. Then we can replace b with c in part (i) and obtain $[a, c] = z^* = [a, b]$. This yields $bc \in C_G(a) = \langle a \rangle Z$, contrary to our choice of c . Thus $\circ(c) > \circ(b)$. Hence $c^2 \in Z$ and $\circ(b) \leq \circ(c^2)$. By (i) it follows that $\circ(b) = \circ(c^2)$ and $[a, b] = (c^2)^* = c^*$, so the claim is proved.

To complete the proof, now pick an element b of minimal order in $G \setminus \langle a \rangle Z$ and assume that $\circ(b) = 2^e < \exp G$. Then $\circ(b) \leq \exp(Z)$, because $G^2 \leq Z$. Since $e > 1$ by Lemma 2.2 (iv), and $\exp G' = 2$, the mapping $\varphi : x \in G \mapsto x^{2^e} \in G$ is an endomorphism. The above claim implies that $\ker \varphi = \langle a, b \rangle Z$ and $\text{im } \varphi = \langle [a, b] \rangle$. Thus $|G/\langle a, b \rangle Z| = 2$ and $|G/Z| = 8$, a contradiction. Therefore $\circ(b) = \exp G$. This makes part (ii) of the claim impossible; hence we also have $\circ(b) > \exp Z$. This proves the first paragraph of the statement. Finally, if $\exp G > 4$ the fact that the mapping in the statement is an endomorphism follows since $\exp G' = 2$; the rest is an immediate consequence of what was just proved. \square

Lemma 3.6. *Let G be a core-2 nilpotent 2-group of class 2. Assume that G has a noncentral involution a and no elements of breadth 1. Then $|G/Z(G)| \leq 16$.*

Proof. Let $Z = Z(G)$ and suppose that $|G/Z| > 16$. The proof is split into two cases, according to the exponent of G . Let $\mathcal{B} = \{b \in G \mid \text{br}_G(b) = 2\}$. Also let $C = \langle a \rangle Z$ and note $|G/C| > 8$.

Case 1 — $\exp G > 4$.

By appealing to the final clause in the statement of Lemma 3.5 for justifying ψ , we can define the following two monomorphisms from G/C to $\text{Soc } G^2$:

$$\varphi : gC \mapsto [a, g]; \quad \psi : gC \mapsto \begin{cases} 1, & \text{if } g \in C \\ g^*, & \text{otherwise.} \end{cases}$$

Since $b^* \neq [a, b]$ for all $b \in \mathcal{B}$, because of Lemma 3.1, the mapping

$$\rho = \varphi + \psi : gC \in G/C \mapsto \begin{cases} 1, & \text{if } g \in C \\ [g, a]g^*, & \text{otherwise} \end{cases} \in \text{Soc } G^2$$

is also a monomorphism. For a fixed $b \in \mathcal{B}$ consider the preimages $F := ([G, b])\varphi^{-1}$, $P := ([G, b])\psi^{-1}$ and $R := ([G, b])\rho^{-1}$. Every nontrivial element of G/C can be written as gC for some $g \in \mathcal{B}$, by Lemma 3.1. By the same lemma and Lemma 3.4 (i) one of $(gC)^\varphi$, $(gC)^\psi$, and $(gC)^\rho$ belongs to $[G, b]$. This proves that $F \cup P \cup R = G/C$, which is a contradiction since each of F , P and R has order 4 while $|G/C| \geq 16$.

Case 2 — $\exp G = 4$.

Since $|[G, a]| = |G/C| > 8$ we have $|G'| > 8$ and are in position to apply Lemma 3.4 (iii). Let z be the nontrivial element of $\bigcap_{b \in \mathcal{B}} [b, G]$. For all $b \in \mathcal{B}$ we have $z \in \{b^*, [a, b], [a, b]b^*\}$, in view of Lemma 3.1 (i). We shall show that $z = b^*$. Let $u \in C_G(b) \setminus \langle b \rangle Z$. By Lemma 2.2 (iv) (or by Lemma 3.5) the subgroup $\langle b, u \rangle = \langle b \rangle \times \langle u \rangle$ is homocyclic (of exponent 4). By the core-2 property the Frattini subgroup $\langle b^2, u^2 \rangle$ of $\langle b, u \rangle$ is $[G, x]$ for some $x \in \{b, u, bu\}$. Then $x \in \mathcal{B}$ and so $z \in [G, x] = \langle b^2, u^2 \rangle$. As $|C_G(b)/Z| \geq 8$ we may choose two elements c and d in $C_G(b)$ in such a way that b, c and d are independent modulo C . Applying the last remark to c, d and cd gives:

$$z \in \{b^2, c^2, b^2c^2\} \cap \{b^2, d^2, b^2d^2\} \cap \{b^2, (cd)^2, b^2(cd)^2\}.$$

Suppose that $z \neq b^2$. Then z is one of c^2 and $(bc)^2$. At the expense of replacing c with bc if necessary we may assume that $z = c^2$. Similarly, we may assume that $z = d^2$. If $z = (cd)^2$ too, then $\langle c, d \rangle \simeq Q_8$, which is impossible by Lemma 2.2 (ii). Therefore $z = b^2(cd)^2$, whence $[c, d] = (cd)^2 = b^2z$. Now consider the subgroup $H = \langle bc, bd \rangle$. What was just worked out gives $(bc)^2 = (bd)^2 = b^2z = [c, d] = [bc, bd]$. Thus either $H \simeq Q_8$ — a contradiction again — or H is abelian; hence $b^2z = 1$. Therefore $z = b^2$, as claimed.

What we have proved is that all elements of breadth 2 in G have the same square z . Let again $b \in \mathcal{B}$. For all $u \in C_G(b) \setminus \langle b \rangle$ we have $\text{br}_G(u) > 2$, as $u^2 \neq b^2$. Hence applying the property core-2 to $\langle b, u \rangle$ yields $\langle b^2, u^2 \rangle = [G, b]$. Once again choose two elements c and d in $C_G(b)$ which are independent modulo $\langle b \rangle Z$. Then $\langle b^2, c^2 \rangle = [G, b] = \langle b^2, d^2 \rangle$, so $c^2 \in \{d^2, (bd)^2\}$. Without loss of generality assume that $c^2 = d^2$. Then the Frattini subgroup of $K := \langle c, d \rangle$ has rank at most 2. However c, d and cd have breadth greater than 2. Property core-2 makes this impossible. \square

Lemma 3.6, together with Corollary 2.4 of [3] and Lemma 2.3, proves the special case of the theorem that we are considering in this section, namely that every core-2 nilpotent 2-group of class 2 containing a noncentral element of order 2 has an abelian subgroup of index 4. However, more structure information is available for such groups.

Proposition 3.7. *Let G be a core-2 nilpotent 2-group of class 2 containing a noncentral involution. Then either*

- (i) G has an element of breadth 1; or
- (ii) $G/Z(G)$ has order 8.

In both cases G has a (normal) abelian subgroup of index 4.

Proof. As just remarked, the final clause holds. We shall assume that G has no element of breadth 1 and shall prove that $|G/Z| = 8$, where $Z := Z(G)$. Suppose to the contrary that $|G : Z| \neq 8$. Lemma 3.6, the absence of elements of breadth 1 and the fact that G is not abelian yield $|G/Z| = 16$. Let $\mathcal{B} = \{b \in G \mid \text{br}_G(b) = 2\}$ and let \mathcal{A} be the set of all abelian subgroups of index 4 in G . Each element of \mathcal{A} contains Z , otherwise G would have an abelian subgroup of index 2, contrary to Lemma 2.2(v). For every $b \in \mathcal{B}$ the subgroup $\langle b \rangle Z$ is central and maximal in $C_G(b)$, which is therefore abelian. From this remark it follows that

$$\mathcal{B} = \bigcup_{A \in \mathcal{A}} (A \setminus Z).$$

Moreover, the latter is a disjoint union. Indeed, let $U, V \in \mathcal{A}$. If $U \neq V$ and $U \cap V \neq Z$ then $UV \triangleleft G$ and so $U \cap V = Z$ by Lemma 2.2(v) again. But this is impossible as $|G : U \cap V| = 8$. Let $\overline{\mathcal{B}} = \{bZ \mid b \in \mathcal{B}\}$. For every $A \in \mathcal{A}$ the set $A \setminus Z$ is union of three elements of $\overline{\mathcal{B}}$; hence 3 divides $|\overline{\mathcal{B}}|$. Moreover, by Lemma 3.1 each nontrivial coset of $\langle a \rangle Z$ in G contains at least one element of $\overline{\mathcal{B}}$, so $|\overline{\mathcal{B}}| \geq 7$. Therefore $|\overline{\mathcal{B}}| > 7$ and there exists $u \in G$ such that both u and au belong to \mathcal{B} . As $[u, au] \neq 1$ we have that $A_1 := C_G(u)$ and $A_2 := C_G(au)$ are distinct elements of \mathcal{A} . Choose $v \in A_1 \setminus \langle u \rangle Z$ and $w \in A_2 \setminus \langle au \rangle Z$, so that $\{a, u, v, w\}$ is a basis of G modulo Z . At least one of vw and avw has breadth 2; call it x . Similarly, there exists $y \in \{uvw, auvw\} \cap \mathcal{B}$. Both $A_3 := C_G(x)$ and $A_4 := C_G(y)$ are in \mathcal{A} and are of course different from each of A_1 and A_2 . If $A_3 = A_4$, then $xy \in A_3$. But xy is congruent to either u or au modulo Z , so one of u and au belongs to A_3 . This is certainly false as $A_1 \cap A_3 = A_2 \cap A_3 = Z$. Thus $A_3 \neq A_4$. Hence $|\mathcal{A}| \geq 4$ and so $|\overline{\mathcal{B}}| = 3|\mathcal{A}| \geq 12$. Since there are 15 nontrivial cosets of Z in G and $aZ \notin \overline{\mathcal{B}}$ by Lemma 2.2(iv), it follows that $|\overline{\mathcal{B}}| = 12$ and $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$. Hence exactly two of the 14 cosets of Z in G different from Z and aZ contain elements of breadth more than 2. Thus, at least two elements of \mathcal{A} have the property that for each element g they contain, ag is also in \mathcal{B} . Without loss of generality we may assume that A_1 and A_2 have this property. In particular, av and auw are in \mathcal{B} . They do not commute, as $[u, av] \neq 1$. Therefore one of them belongs to A_3 , the other one to A_4 . It follows that for one of the sets $\{(av)x, (auw)y\}$ and $\{(av)y, (auw)x\}$ the following condition is satisfied: of its two elements one belongs to A_3 , the other to A_4 ; hence they are not congruent modulo Z and do not lie in $A_1 \cup A_2$. A simple direct check shows that this is impossible: working out the first pair, from $x \in \{vw, avw\}$ we get that $(av)x$ is congruent modulo Z to either aw or w , but the latter has to be excluded since $w \in A_2$, so $(av)xZ = awZ$. Similarly from $y \in \{uvw, auvw\}$ it follows that $(auw)yZ = awZ$; thus we get the contradiction $(av)xZ = (auw)yZ$. Analogous computation for the second pair gives $(av)yZ = uwZ = (auw)xZ$, a contradiction again. This proves our statement. \square

It is worth noting that it is indeed possible for groups like those in the statement of Proposition 3.7 to have no elements of breadth 1. This is shown by the next example. At the other extreme, it is clear that a semidirect product $A \rtimes \langle a \rangle$, where A is an abelian group of exponent 4 and a has order 2 and acts on A like the inversion map, satisfies the hypothesis of Proposition 3.7 and can be made to have central factor group of arbitrarily high cardinality.

Example 3.8. Let $M = L \times \langle z \rangle$, where $o(z) = 2$ and $L = \langle u \rangle \rtimes \langle v \rangle$ is the nonabelian semidirect product of two cyclic groups of order 4. For each $i \in \{1, 2, 3\}$ let $G_i = M \rtimes \langle w_i \rangle$, where w_i has order 2 and acts on M as specified here:

$$\begin{array}{llll} w_1 : & u \mapsto uz, & v \mapsto v^{-1}u^2, & z \mapsto z; \\ w_2 : & u \mapsto uv^2, & v \mapsto vz, & z \mapsto z; \\ w_3 : & u \mapsto u^{-1}v^2, & v \mapsto vz, & z \mapsto z. \end{array}$$

Then $|G_i| = 64$ and $G'_i = Z(G_i) = G_i^2 = \langle u^2, v^2, z \rangle$. Both $Z(G_i)$ and $G_i/Z(G_i)$ are elementary abelian of order 8. All noncentral elements of G_i have breadth 2. Of course w_i is a noncentral involution.

Let G be any of the groups G_i . We want to prove that G is core-2. Assume that this is false. Then $|H/H_G| > 2$ for some $H \leq G$. Since all groups of order 16 and nilpotency class 2 are core-2 (because their centres have index 4) it follows that $|H/H_G| \geq 32$ and $|H_G| \leq 2$. Also, $|H| > 2$; hence $D := H \cap M \neq 1$. As all involutions of M are central in G it follows that H_G has order 2 and is the socle of D . Thus $|H| = 8$. Assume that $H \leq M$. Since $H \cap G' \leq H_G$ and so $|H : H \cap G'| \geq 4 = |M : G'|$ we have $M = HG'$. Thus $H \triangleleft M$ and M/H has exponent 2, as also happens for M/G' . Hence $M^2 \leq H \cap G' \leq H_G$, which is false as $|M^2| = 4$. Therefore $H \not\leq M$. It follows that $|D| = 4$. Hence D is cyclic since its socle H_G has order 2; say $D = \langle d \rangle$. Also, $H_G = D^2 \leq M^2 = \langle u^2, v^2 \rangle$. Since $G^2 = Z(G)$ it even holds that $H^2 = H_G$.

Set $w := w_i$ and let $h \in H \setminus D$. Then $h = mw$ for some $m \in M$. For either $\lambda \in \{0, 1\}$ we have $(d^\lambda mw)^2 \in H^2 \leq M^2$. Hence $[d^\lambda m, w] \in M^2$. It follows that both $[d, w]$ and $[m, w]$ are in M^2 . From this and from the description of the conjugation action of w on M , since $z \notin M^2$ one gets that both d and m lie in $\langle v \rangle G'$ if $i = 1$ or in $\langle u \rangle G'$ if $i \neq 1$. In either case $[d, m] = 1$. But $D = \langle d \rangle \triangleleft H$; hence D must be normalized by w , which amounts to saying that $[d, w] \in \langle d^2 \rangle$. Suppose that $i = 1$. Then $d \in vG'$, as $\circ(d) = 4$, so $d^2 = v^2$ and $[d, w] = [v, w]$ but, on the other hand, $[v, w] = u^2 v^2 \notin \langle v^2 \rangle$. If $i \neq 1$ we obtain an analogous inconsistency from $[u, w] \notin \langle u^2 \rangle$. These contradictions prove that each of the groups G_1, G_2 and G_3 is core-2. \square

The above examples are somehow typical, according to the next proposition.

Proposition 3.9. *Let G be a core-2 finite 2-group of nilpotency class 2 and breadth 2. If $|G'| = 8$ then G has no elements of breadth 1.*

Proof. Lemma 2.4 of [8] shows that G has a 3-generator subgroup H such that $H' = G'$. It is clear that if u, v and w are any three elements generating H then $H' = \langle [u, v] \rangle \times \langle [u, w] \rangle \times \langle [v, w] \rangle$, so that each of the subgroups $[h, H]$ with $h \in \{u, v, w\}$ has order 4 and coincides with $[h, G]$, and the intersection of these three subgroups is trivial.

Let $x \in G$. We want to prove that $\text{br}_G(x) \neq 1$. To this end assume first that $[x, H] = 1$ and let $H = \langle u, v, w \rangle$. Then, for all $h \in \{u, v, w\}$ we have $[xh, H] = [h, H]$. Since $|[xh, G]| \leq 4$ this gives $[xh, G] = [h, H] = [h, G]$, from which it follows that $[x, G] \leq [h, G]$. Hence $[x, G] \leq [u, G] \cap [v, G] \cap [w, G] = 1$ and $x \in Z(G)$. So our result is proved in this case and we may assume that $[x, H] \neq 1$. Let $C = C_H(x)$. Then $H = \langle u, v, w \rangle$ for suitable $u, v, w \in H \setminus C$. Suppose that $|H : C| = 2$. Then for every $h \in \{u, v, w\}$ it holds that $H = C\langle h \rangle$, so $[xh, C] = [h, C] = [h, H] = [h, G]$ and $[xh, G] = [h, G]$ by comparison of orders. It follows that $[x, G] \leq [h, G]$. This leads to a contradiction as for the previous case. Hence $|H : C| > 2$ and so $\text{br}_G(x) = 2$, as wished. \square

4. Proof of the Theorem

This final section is devoted to proving the main result of the paper. Let us start with two lemmas in the spirit of Lemma 2.2.

Lemma 4.1. *Let G be a core-2 nilpotent 2-group of class 2. Assume that G has a maximal subgroup M such that $|M'| = 2$. Then M has an abelian subgroup of index 2, or some element of $G \setminus M$ has order 2, or G has some element of breadth 1. In any case G has a normal abelian subgroup of index 4.*

Proof. Assume that none of the three possibilities occurs. Since G has no elements of breadth 1, Lemma 2.2(v) yields $Z := Z(G) = Z(M)$.

Let a be an element in $G \setminus M$. Then $a^2 \neq 1$. For every $x \in C_M(a)$ we have $\text{br}_G(x) = \text{br}_M(x) \leq 1$, as $|M'| = 2$; hence $C_M(a) = Z$. Thus $\text{br}_G(a) = n$ where $|M/Z| = 2^n$. We claim that M' is not contained in $[M, a]$. Otherwise $[u, a] \in M'$ for some $u \in M \setminus Z$, so $[u, a] = [u, v]$ for some other $v \in M$, but this is impossible as $C_M(av^{-1}) = Z$. Let N be a normal subgroup of M , maximal with respect to the conditions $[M, a] \leq N$ and $N \cap M' = 1$. By [3], Lemma 2.6, the quotient M/N is isomorphic to the central product of D_8 and Q_8 . In particular, M/N has a noncentral element xN of order 2 and its centre has index 16. Thus $|M/Z| \geq 16$ and so all elements of $G \setminus M$ have breadth greater than 3. Hence, if $H = \langle x, a \rangle$, the core-2 property gives $[G, x] \leq H^2 = \langle x^2, [x, a], a^2 \rangle$. Now $M' = [M, x] \leq [G, x]$. Since $x^2, [x, a] \in N$ and $M' \not\leq N$ it follows that $a^2 \notin N$. Hence G/N is isomorphic to the central product of D_8 , Q_8 and a cyclic group of order 4. This is impossible because such a product has a subgroup isomorphic to V_4 that intersects the centre trivially; hence it cannot be a core-2 group. \square

Lemma 4.2. *Let G be a core-2 nilpotent 2-group of class 2. Let A be a homocyclic subgroup of G of rank 3 and such that $AZ(G)/Z(G)$ has rank 2. Then there exists $x \in A$ such that $\text{br}_G(x) = 1$.*

Proof. For suitable $a, b \in A$ and $c \in Z(G)$ we have $A = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$. Let H be any of the four subgroups $\langle a, b \rangle$, $\langle ac, b \rangle$, $\langle a, bc \rangle$, $\langle ac, bc \rangle$. Assume that none of a , b and ab has breadth 1 in G . By the core-2 property there exists $h \in H \setminus H^2$ such that $[G, h] \leq H^2$. Clearly $[G, h]$ is one of $[G, a]$, $[G, b]$ and $[G, ab]$, as $c \in Z(G)$. Thus $|[G, h]| = 4$ and so $[G, h] = \text{Soc}(H)$. However the four subgroups considered for H have pairwise different socles, while, as just seen, $[G, h]$ may range over three possible values only, a contradiction. \square

We are now in position to prove the theorem. By the Mal'cev Local Theorem it will be enough to prove it for finite groups. Arguing by means of contradiction, assume that the finite 2-group G is a minimal counterexample; that is to say, G is a core-2 group of nilpotency class 2 of the minimal possible order for having no (normal) abelian subgroup of index 4. We will reach a contradiction after several steps, as follows.

Let $Z := Z(G)$. From Lemma 2.4 and Lemma 2.6 of [3] we get $|G/Z| \geq 32$ and $|G'| \geq 8$. Also, G has no element of breadth 1, by Lemma 2.3. Furthermore, Proposition 3.7 and Lemma 4.1 show that every element of order 2 in G is central and $|M'| > 2$ for every maximal subgroup M of G .

By minimality of $|G|$ every maximal subgroup and every proper quotient of G has a normal abelian subgroup of index less than or equal to 4. It follows that if we let

$$\mathcal{A} := \{A \leq G \mid A \text{ is abelian and } |G : A| = 8\} \quad \text{and} \quad \mathcal{L} := \{L \triangleleft G \mid |G/L| = 4 \text{ and } |L'| = 2\}$$

then we have:

1. Every maximal subgroup of G contains some element of \mathcal{A} .
2. For every subgroup X of order 2 in Z there exists $L \in \mathcal{L}$ such that $L' = X$.

Thus every maximal subgroup of G must contain Z , since $A = C_G(A)$ for all $A \in \mathcal{A}$, and every subgroup of order 2 in Z is contained in G' . Hence:

3. $Z = G^2$ and $G' = \text{Soc}(Z)$.

We want to show that every element of \mathcal{L} has an abelian subgroup of index 2. To this end, let \mathcal{L}_1 be the set of all elements of \mathcal{L} that have an abelian subgroup of index 2 and let $\mathcal{L}_2 := \mathcal{L} \setminus \mathcal{L}_1$. If $L \in \mathcal{L}_1$ then $|L/Z(L)| = 4$, as $|L'| = 2$, while elements of \mathcal{L}_2 have centre of index 16, according to Lemma 2.6 of [3]. Other easy remarks are:

4. For every $L \in \mathcal{L}$ we have $Z \leq L$, and $L = C_G(x)$ for every $x \in L \setminus Z$.

Indeed, that Z is contained in every $L \in \mathcal{L}$ follows from Lemma 4.1: if there existed $z \in Z \setminus L$ then $M := L\langle z \rangle$ would be either G or a maximal subgroup of G with derived subgroup $M' = L'$ of order 2. The second part of (4), is also clear since $|G : L| = 4$ and x cannot have breadth 1 in G .

5. Let $L, K \in \mathcal{L}$. If $G = LK$ then $Z = Z(L) \cap K$.

For, let $x \in Z(L) \cap K$. If $x \notin Z$ then $L \cap K = C_K(x)$ by (4). Now $G = LK$ yields $\text{br}_K(x) = 2$, which is impossible since $|K'| = 2$.

6. If $\mathcal{L}_1 \neq \emptyset$ then $|G/Z| = 32$.

To prove this statement, let $L \in \mathcal{L}_1$. By (2) and since $|G'| > 2$ there exists $K \in \mathcal{L}$ such that $L' \neq K'$. Then $D := L \cap K$ is abelian. If $G = LK$ then $Z = Z(L) \cap D$ by (5). Now $L > DZ(L)$; otherwise L would be abelian. Since $|L : D| \leq 4 = |L : Z(L)|$ it follows that $|L : Z| \leq 8$ and so $|G/Z| = 32$. Otherwise, if $LK < G$ then D is maximal in both L and K . Hence $K \in \mathcal{L}_1$. Again $L > DZ(L)$, so $Z(L)$ is a maximal subgroup of D . For the same reason $Z(K) \triangleleft D$. Thus $|D : Z(L) \cap Z(K)| \leq 4$. Now (4) implies $Z(L) \cap Z(K) = Z$, and we get $|G/Z| = 32$, as required.

7. $\mathcal{L} = \mathcal{L}_1$ and $|G/Z| = 32$.

Suppose that $\mathcal{L}_2 \neq \emptyset$. Let $L \in \mathcal{L}_2$. Assume that $Z \neq Z(L)$ and let $x \in Z(L) \setminus Z$. Then $L = C_G(x)$ by (4), and Lemma 2.3 proves that L has an abelian subgroup of index 2. This is impossible by definition of \mathcal{L}_2 . Therefore $Z = Z(L)$. Hence $|G/Z| = 64$. By (6) it follows that $\mathcal{L}_1 = \emptyset$. Now let A and B be different elements of \mathcal{A} . Then $Z \leq C := A \cap B \leq Z(AB)$. If $AB < G$ then G/AB has order 2 or 4, so $|G : C| \leq 32$ and $Z < C$. If $|G/AB| = 2$ then $C \leq Z$ by Lemma 2.2(v), a contradiction; if $|G/AB| = 4$ then $Z(AB) = C$ has index 4 in AB and it follows that $AB \in \mathcal{L}_1$, again a contradiction. Therefore $G = AB$ and so $A \cap B = Z$. Since $G^2 = Z$ it follows that G has exactly 63 maximal subgroups. By (1) and by what just proved each of these maximal subgroups contains exactly one element of \mathcal{A} . On the other hand every element of \mathcal{A} is contained in precisely seven maximal subgroups of G . Therefore $|\mathcal{A}| = 63/7 = 9$. For each $X \leq G$ such that $Z \leq X$ let $X^* = (X/Z) \setminus \{Z\}$, the set of all nontrivial cosets of Z in X . By the above and by comparing orders the set $\{A^* \mid A \in \mathcal{A}\}$ is a partition of G^* . Now let $L \in \mathcal{L}$. Then $A^* \cap L^* = (A \cap L)^*$ for every $A \in \mathcal{A}$ and $\{(A \cap L)^* \mid A \in \mathcal{A}\}$ is a partition of L^* in seven blocks. As $|L^*| = 15$ there must exist $A \in \mathcal{A}$ such that $|(A \cap L)^*| < 3$, which amounts to saying that $|(A \cap L)/Z| \leq 2$. As $|G : L| = 4$ and $|G : A| = 8$ we have $|G : A \cap L| \leq 32$ and so $Z < A \cap L$. It follows that $|(A \cap L)/Z| = 2$ and $G = AL$. Let $x \in (A \cap L) \setminus Z$. Then $\text{br}_G(x) = \text{br}_L(x) = 1$, a contradiction. This proves that $\mathcal{L} = \mathcal{L}_1$. Now (6) gives $|G/Z| = 32$.

The next step in the proof will consist in bounding the possible size of G' to 8.

Let \mathcal{B} be the set of all elements of breadth 2 in G . For all $b \in \mathcal{B}$ we shall write \bar{b} for the set bZ (which is still contained in \mathcal{B}); let $\bar{\mathcal{B}} := \{\bar{b} \mid b \in \mathcal{B}\}$. Conversely, throughout this proof, a notation like \bar{b} will always refer to elements $b \in \mathcal{B}$.

Let $b \in \mathcal{B}$ and set $L = C_G(b)$. Then $|G/L| = 4$, so that L is not abelian, and $|L/Z| = 8$. The centre of L contains $\langle b \rangle Z$, of index 4 in L . Hence $|L/Z(L)| = 4$ and so $|L'| = 2$ and $L \in \mathcal{L}$. Therefore we can consider the mapping $\bar{b} \in \bar{\mathcal{B}} \mapsto C_G(b) \in \mathcal{L}$. This mapping is bijective: its inverse maps every $L \in \mathcal{L}$ to \bar{b} , defined by the equality $\langle b \rangle Z = Z(L)$. Moreover $\bar{\mathcal{B}} \subseteq (G/Z) \setminus \{Z\}$ and, by (2), the mapping $L \mapsto L'$ from \mathcal{L} to the set of all subgroups of G' of order 2 is surjective. Since the last set has cardinality $|G'| - 1$ we conclude that

$$|G'| - 1 \leq |\mathcal{L}| = |\bar{\mathcal{B}}| \leq |G/Z| - 1 = 31. \quad (*)$$

This implies that $|G'| \leq 32$. Furthermore, if $|G'| = 32$ then $\bar{\mathcal{B}} = (G/Z) \setminus \{Z\}$, which means that G has breadth 2. By [9] this would imply that $|G'| = 8$, a contradiction. Thus $|G'| \leq 16$. Define the equivalence relation \sim in $\bar{\mathcal{B}}$ by setting, for all $\bar{x}, \bar{y} \in \bar{\mathcal{B}}$,

$$\bar{x} \sim \bar{y} : \iff [G, x] = [G, y].$$

Assume that $|G'| = 16$. To show that this assumption yields a contradiction we shall consider two cases separately. First note that (*) gives $15 \leq |\bar{\mathcal{B}}|$. From this it follows that either $V := \langle \mathcal{B} \rangle = G$ or $V < G$. In either case $G' = \langle [G, b] \mid b \in \mathcal{B} \rangle$.

Case 1 — For all $x, y \in \mathcal{B}$, $[G, x] \cap [G, y] \neq 1$.

In this case Lemma 3.3 shows that $U := \bigcap_{b \in \mathcal{B}} [G, b]$ has order 2. If $x, y \in \mathcal{B}$ and $\bar{x} \sim \bar{y}$ then $[x, y] \in [G, x] \cap [G, y] = U$. Since G'/U has rank 3 and is generated by the rank-1 subgroups $[G, b]/U$, with b ranging over a complete set of representatives of \mathcal{B} modulo \sim , the quotient set $\overline{\mathcal{B}}/\sim$ has at least 3 elements. Choose $y \in \mathcal{B}$ by choosing $\bar{y} \in \overline{\mathcal{B}}$ in the following way. Let X be a basis of V/Z . If one of the \sim -equivalence classes has no representative in X , let \bar{y} be one element of this class. Otherwise, one of the classes has only one representative in X , since $|X| \leq 5$, and we can choose \bar{y} to be that element of X . In either case $\bar{x} \sim \bar{y}$ for all $\bar{x} \in X \setminus \{\bar{y}\}$; thus $[V, y] \leq U$ by the above remark. Now, $[G, y] \not\leq U$, because $\text{br}_G(y) = 2$; hence $V \neq G$ and so $V < G$. By comparing orders it follows that $V = \mathcal{B} \cup Z$. For every $c \in G' \setminus 1$ step (2) provides $L \in \mathcal{L}$ such that $L' = \langle c \rangle$. Now $|L : L \cap V| \leq 2$; hence there exists $b \in L \cap V \setminus Z(L)$. By what was just observed $b \in \mathcal{B}$ and $c \in L' = [L, b] \leq [G, b]$. This proves that $G' = \bigcup_{b \in \mathcal{B}} [G, b]$. It follows that each of the seven subgroups of order 4 of G' containing U is $[G, b]$ for some $b \in \mathcal{B}$. Thus $|\overline{\mathcal{B}}/\sim| = 7$. Let R be a complete set of representatives of the \sim -equivalence classes. If $\langle R \rangle \neq V/Z$ then $\langle R \rangle = R \cup \{Z\}$, because $|R| = 7$ and $|V/K| = 16$. In this case it is enough to replace one element in R with another element in the same \sim -equivalence class (which is certainly possible, as $|\overline{\mathcal{B}}| \geq 15$) to obtain a complete set of representatives of the \sim -equivalence classes that generates V/Z . So we may assume that $\langle R \rangle = V/Z$. Then, for any different elements $\bar{x}, \bar{y} \in R$ we have $\bar{x} \sim \bar{y}$ and so $[x, y] \leq U$. Hence $V' \leq U$. However this is impossible because of Lemma 4.1. Thus Case 1 is excluded.

Case 2 — There exist $x, y \in \mathcal{B}$ such that $[G, x] \cap [G, y] = 1$.

For such x and y we have $G' = [G, x] \times [G, y]$. Let $C_x := C_G(x)$, $C_y := C_G(y)$ and $C_{xy} := C_G(xy)$. By Lemma 3.2 we have $\langle x, y \rangle Z \leq C_{xy} = C_x \cap C_y$. As $|G/Z| = 32$ and $|\langle x, y \rangle Z/Z| = 4$ (otherwise $\bar{x} = \bar{y}$ and $[G, x] = [G, y]$) we have $\langle x, y \rangle Z < C_x$. If $C_{xy} = C_x$ then $C_x = C_y$ and $\langle x, y \rangle Z$ would be central in C_x , so the latter would be abelian. Hence $C_{xy} = \langle x, y \rangle Z$ and $\text{br}_G(xy) = 3$. This implies that \mathcal{B} generates G , since V/Z contains at least 17 elements of G/Z , namely Z , xyZ and the elements of $\overline{\mathcal{B}}$. As $|G : C_x \cap C_y| = 8$ we have $|G : C_x C_y| = 2$; hence we can pick $d \in \mathcal{B} \setminus C_x C_y$. Then $C_d \cap C_{xy} = Z$, so $G/Z = (C_{xy}/Z) \times (C_d/Z)$. Clearly $C_d = \langle a, b, d \rangle Z$ where $\langle a \rangle Z = C_x \cap C_d$ and $\langle b \rangle Z = C_y \cap C_d$. Thus $\{[x, d], [x, b], [y, d], [y, a]\}$ is a basis of G' .

We shall use this description of G to exhibit more elements of breadth greater than 2 than G can contain. Besides xy other elements of breadth at least 3 in G are:

— those of the form $g = tab$, where $t \in \{x, y, xy\}$.

Indeed, the description of a basis of G' just given shows that the three commutators $[g, d] = [t, d]$, $[g, x] = [x, b]$ and $[g, y] = [y, a]$ are independent, so the rank of $[G, g]$ is at least 3. Thus we have three cosets of Z in G different from xyZ and consisting of elements of breadth greater than 2.

— those of the form $g = tcd$, where $t \in \{x, y, xy\}$, $c \in \langle a, b \rangle$ and $[c, t] \neq 1$.

For, let t' be an element of $\{x, y, xy\}$ different from t . Then the commutators $[g, c] = [t, c]$, $[g, d] = [t, d]$ and $[g, t'] = [t', c][t', d]$ are independent. This provides seven further cosets mod Z not belonging to $\overline{\mathcal{B}}$: two cosets each for $t = x$ and $t = y$, three for $t = xy$.

— those of the form $g = td$, where $t \in \{x, y, xy\}$ again.

For, choose $c \in \langle a, b \rangle$ such that $[c, t] \neq 1$. Then $[g, c] = [t, c]$, $[g, x] = [x, d]$ and $[g, y] = [y, d]$ are independent. This gives other three cosets not in $\overline{\mathcal{B}}$.

The argument so far has provided 14 cosets of Z in G containing elements of breadth greater than 2. Since $|G/Z| = 32$ and $|\overline{\mathcal{B}}| \geq 15$ (and taking into account the trivial coset Z), to get a contradiction it will be enough to exhibit three more such cosets. To this end we turn our attention to $k := [a, b]$. Certainly $k \neq 1$, otherwise C_d would be abelian. Since $[G, ad] = \langle [x, d], [y, ad], k \rangle$ and $[G, bd] = \langle [y, d], [x, bd], k \rangle$ we have:

$$\text{br}_G(ad) = 2 \iff k \in \langle [x, d], [y, ad] \rangle; \quad \text{br}_G(bd) = 2 \iff k \in \langle [y, d], [x, bd] \rangle.$$

As $\langle [x, d], [y, ad] \rangle \cap \langle [y, d], [x, bd] \rangle = 1$ one of the two conditions fails, and one of ad and bd has breadth greater than 2. Of course neither of ad and bd belong to any of the 14 cosets modulo Z already listed. To find two more cosets not in $\bar{\mathcal{B}}$ consider xa, ya, xb and yb . We have

$$\begin{aligned} [G, xa] &= \langle [x, d], [y, a], [x, b]k \rangle, & [G, ya] &= \langle [y, d], [y, a], k \rangle, \\ [G, xb] &= \langle [x, d], [x, b], k \rangle, & [G, yb] &= \langle [y, d], [x, b], [y, a]k \rangle; \end{aligned}$$

hence

$$\begin{aligned} \text{br}_G(xa) = 2 &\iff k \in [x, b] \langle [x, d], [y, a] \rangle; & \text{br}_G(ya) = 2 &\iff k \in \langle [y, d], [y, a] \rangle; \\ \text{br}_G(xb) = 2 &\iff k \in \langle [x, d], [x, b] \rangle; & \text{br}_G(yb) = 2 &\iff k \in [y, a] \langle [y, d], [x, b] \rangle. \end{aligned}$$

Since $[x, b] \langle [x, d], [y, a] \rangle \cap \langle [y, d], [y, a] \rangle = \emptyset = \langle [x, d], [x, b] \rangle \cap [y, a] \langle [y, d], [x, b] \rangle$ we conclude that at least one of xa and ya and one of xb and yb has breadth greater than 2. Now we have found that at least 17 cosets of Z in G consist of elements of breadth more than 2, and this leads to a contradiction. Thus also Case 2 is impossible and we have proved:

8. $|G'| = 8$.

Now, $G' = \text{Soc}(Z)$ by **(3)**; hence **(8)** means that Z has rank 3. We shall prove that $Z = G'$, i.e., that G has exponent 4.

As $\exp(G') = 2$ the mapping $g \in G \mapsto g^4 \in G$ is an endomorphism; thus $W := \{g \in G \mid g^4 = 1\}$ is a (normal) subgroup of G and $G/W \simeq G^4 = Z^2$. Hence $3 = \text{rk}(Z) \geq r := \text{rk}(Z^2) = \text{rk}(G/WZ)$ (for the last equality recall that $Z = G^2$ from **(3)**). In particular $\text{rk}(WZ/Z) = 5 - r \geq 2$. As regards squares of noncentral elements we have:

9. For all $g \in G \setminus Z$ we have $g^2 \notin Z^2$.

Otherwise $g^2 = z^2$ for some $z \in Z$ and gz^{-1} would be a noncentral element of order 2.

Keeping in mind that G' is the socle of Z we can therefore consider the mapping defined by $gZ \mapsto g^2Z^2$ from the set of all nontrivial cosets of Z in WZ to the set of all nontrivial cosets of Z^2 in $G'Z^2$. We claim that the image I of this mapping has more than one element. If not, let x and y be elements of W independent modulo Z (such elements do exist, as $\text{rk}(WZ/Z) \geq 2$). Then $x^2Z^2 = y^2Z^2 = (xy)^2Z^2$ is the only element of I . Then $x^2 = (yc)^2$ for some $c \in Z$; at the expense of substituting yc for y we may assume that $x^2 = y^2$. Then $[x, y] = (xy)^2 = x^2z^2$ for some $z \in Z$. Now let $x_1 := xz$ and $y_1 := yz$. Then $x_1^2 = y_1^2 = [x, y] = [x_1, y_1]$ and so $\langle x_1, y_1 \rangle \simeq Q_8$, a contradiction by Lemma 2.2 (ii). Hence $|I| > 1$, which implies $|G'Z^2/Z^2| > 2$. Therefore $Z^2 \cap G' = \text{Soc}(Z^2)$ has order at most 2; i.e., $r \leq 1$. Suppose that $r = 1$. Then $\text{rk}(WZ/Z) = 5 - r = 4$. By minimality of $|G|$ (or because $|W/Z(W)| \leq 16$) W contains an abelian subgroup A of index 4. Pick two elements a and b independent modulo Z and belonging to A . Then $\langle a, b \rangle = \langle a \rangle \times \langle b \rangle$, since $\text{Soc } A \leq Z$. Let c be an element of order 4 in Z . It follows from **(9)** that $\langle a, b, c \rangle$ is homocyclic; by Lemma 4.2 this is impossible. This contradiction proves that $r = 0$, so $\exp(G^2) = \exp(Z) = 2$. Whence:

10. $\exp(G) = 4$.

Look back at the equivalence relation \sim over $\bar{\mathcal{B}}$ introduced by proving **(8)**. For all $x, y \in \mathcal{B}$, we have $\bar{x} \sim \bar{y}$ if and only if the maximal subgroups $[G, x]$ and $[G, y]$ of G' coincide. Let $M \triangleleft G'$ and $U/M = Z(G/M)$. Lemma 2.6 (i) of [3] shows that $|G/U|$ is either 4 or 16; hence the set $U^* = (U/Z) \setminus \{Z\}$ is not empty. For all $x \in U \setminus Z$ we have $[G, x] = M$, as $\text{br}_G(x) > 1$. Hence U^* is an equivalence class with respect to \sim . Since G' has seven maximal subgroups, then $\bar{\mathcal{B}}$ is split into seven \sim -equivalence classes. Moreover each class U^* may only have order 1 or 7, according to whether $|G/U| = 16$ or $|G/U| = 4$. The latter case may occur for at most one class. For, if M and N are different maximal subgroups of G' such that both $U/M = Z(G/M)$ and $V/N = Z(G/N)$ have index 4 (in G/M and G/N respectively) then $Z < U \cap V$ and, for any $x \in U \cap V \setminus Z$, since $[G, x] \leq M \cap N$ we would have $\text{br}_G(x) = 1$, a contradiction.

Thus either $|\bar{\mathcal{B}}| = 7$ and \sim is the equality relation in $\bar{\mathcal{B}}$ or there is one \sim -class of order 7 and $|\bar{\mathcal{B}}| = 13$.

Let us now define a (simple, nondirected) graph $\widehat{\mathcal{B}}$ whose vertices are the elements of $\overline{\mathcal{B}}$ and two of them, say \bar{x} and \bar{y} , are adjacent if and only if $[x, y] = 1$ and $\bar{x} \neq \bar{y}$.

11. Let $b \in \mathcal{B}$ and let $L = C_G(b)$. Then $L = \langle b, u, v \rangle Z$ for some $u, v \in \mathcal{B}$. Hence every vertex of $\widehat{\mathcal{B}}$ has valency at least 2.

Indeed, assume that the first part of the statement fails for b . As L/Z has rank 3 there exists $u \in L \setminus \langle b \rangle Z$ such that $\text{br}_G(x) > 2$ for every $x \in L \setminus \langle b, u \rangle Z$. By property core-2, for such an x we must have:

$$\langle b, x \rangle^2 = \langle b^2, x^2 \rangle = [G, b] = \langle b^2, (ux)^2 \rangle = \langle b, ux \rangle^2.$$

Then one of the following holds: either $x^2 = (ux)^2$ or $x^2 = (bux)^2$. Since we may substitute bu for u if necessary, we may assume that $x^2 = (ux)^2$, so $u^2 = [u, x]$. Then $\langle u, x \rangle^2 = \langle u^2, x^2 \rangle$ has rank 2 at most, and again by core-2 we get $\langle u^2, x^2 \rangle = [G, u]$. Similarly, from $u^2 = [u, bx]$ it follows that $\langle u^2, b^2x^2 \rangle = \langle u, bx \rangle^2 = [G, u]$; hence $\langle u^2, b^2x^2 \rangle = \langle u^2, x^2 \rangle \simeq V_4$. As $b^2 \neq 1$ it follows that $x^2 = u^2b^2x^2$, so $u^2 = b^2$ and $u^{-1}b$ is a noncentral element of order 2, a contradiction. This proves the first part of (11). The rest is an immediate consequence: if $u, v \in \mathcal{B}$ are as in the statement then \bar{u} and \bar{v} are distinct and both adjacent to \bar{b} .

12. Let \bar{b} be a vertex of valency 2 in $\widehat{\mathcal{B}}$. Let u and v be the two elements of \mathcal{B} such that $L := C_G(b) = \langle b, u, v \rangle$. Then $L' = \langle b^2 \rangle$ and $u^2 \notin [G, b] = \langle b^2, u^2v^2 \rangle$. Furthermore $[G, u] = \langle u^2, b^2 \rangle$.

By hypothesis the only elements of breadth 2 in G lying in L are those congruent to b, u or v modulo Z . Therefore no element of $H := \langle bu, bv \rangle$ has breadth 2 and property core-2 shows that $H^2 = \langle b^2u^2, b^2v^2, [u, v] \rangle$ has rank 3 and so coincides with G' . Hence $[u, v] \notin \langle b^2u^2, b^2v^2 \rangle$. Again by core-2 we also have $\langle b, uv \rangle^2 = \langle b^2, u^2v^2[u, v] \rangle = [G, b] \simeq V_4$, which yields $[u, v] \neq b^2u^2v^2$. We claim $[u, v] \in \langle b^2, u^2, v^2 \rangle$. Indeed, if this is false then property core-2 and the fact that $[u, v] = [bu, v] \notin \langle b, u \rangle^2$ yield $\langle b^2, u^2 \rangle = \langle b, u \rangle^2 = [G, b]$. By comparing this with the previous description of $[G, b]$ we obtain $[u, v] \in \langle b^2, u^2, v^2 \rangle$, so that our claim is proved. The information collected so far on $[u, v]$ shows that $[u, v] \in \{b^2, u^2, v^2\}$. It follows that $G' = H^2 = \langle b^2 \rangle \times \langle u^2 \rangle \times \langle v^2 \rangle$.

Suppose that $[u, v] = u^2$. Then $\langle u, bv \rangle^2 \simeq V_4$ and $[G, u] = \langle u, bv \rangle^2 = \langle u^2, b^2v^2 \rangle$ by core-2. By the same property, since $v^2 \notin [G, u]$ and so $\langle u, v \rangle^2 \neq [G, u]$ we have $\langle u, v \rangle^2 = [G, v]$. Hence $b^2 \notin [G, u] \cup [G, v]$. By using property core-2 once more it follows that $\langle b, u \rangle^2 = [G, b] = \langle b, v \rangle^2$. Then $G' = \langle b^2, u^2, v^2 \rangle \leq [G, b]$, a contradiction. Thus $[u, v] \neq u^2$. Substituting v for u in the previous argument gives $[u, v] \neq v^2$. Therefore $[u, v] = b^2$. Finally, $L' = \langle [u, v] \rangle$ and $[G, b] = \langle b^2, u^2v^2[u, v] \rangle = \langle b^2, u^2v^2 \rangle$. Thus $u^2 \notin [G, b]$ and core-2 shows that $\langle u, b \rangle^2 = [G, u]$. So (12) is proved.


A further consequence is that \bar{u} cannot have valency 2 in $\widehat{\mathcal{B}}$. For, it had then we could apply (12) to \bar{u} in place of \bar{b} ; from $b \in C_G(u)$ it would follow that $b^2 \notin [G, u]$, against the last clause in the statement of (12). Since a vertex \bar{x} is adjacent to \bar{b} if and only if $x \in \mathcal{B} \cap C_G(b)$ this remark proves next statement.

13. $\widehat{\mathcal{B}}$ has no adjacent vertices of valency 2.

14. $\widehat{\mathcal{B}}$ has no subgraph of the form 

Indeed, if such a subgraph exists then the subgroup $A := \langle a, c \rangle Z$ is abelian of index 8 in G and is central in $B := \langle a, b, c, d \rangle Z$. Now, $B \neq A$, because B/Z has at least four nontrivial elements. So A is not self-centralizing and G has an abelian subgroup of index 4, a contradiction.

An equivalence relation σ can be defined in $\overline{\mathcal{B}}$ by setting $\bar{x} \sigma \bar{y} : \iff C_G(x)' = C_G(y)'$, for all $x, y \in \mathcal{B}$.

15. Assume that $\widehat{\mathcal{B}}$ has a subgraph of the form . Then $\bar{a} \sigma \bar{c}$ and $\bar{b} \sigma \bar{d}$.

For, $[a, c] \neq 1$ by (14). Now both $C_G(b)$ and $C_G(d)$ contain a and c ; hence they have $\langle [a, c] \rangle$ as derived subgroup. So $\bar{a} \sigma \bar{c}$. Of course this also yields $\bar{b} \sigma \bar{d}$.

16. $|\overline{\mathcal{B}}| = 13$.

To prove this equality it suffices to exclude the possibility that $\overline{\mathcal{B}}$ has only seven elements. Suppose that $|\overline{\mathcal{B}}| = 7$. The set Σ of all subgroups of order 2 of G' has order 7. As seen above the mapping $f : \bar{b} \in \overline{\mathcal{B}} \mapsto C_G(b)' \in \Sigma$ is surjective. Hence f is bijective and $\bar{x} \sigma \bar{y} \iff \bar{x} = \bar{y}$ for all $x, y \in \mathcal{B}$. By (15) it follows that $\widehat{\mathcal{B}}$ has no circuit of length 4. Furthermore, if $\widehat{\mathcal{B}}$ has a circuit of length 3 then this cannot involve any vertex of valency 2. For, if $\bar{a} \xrightarrow{\bar{c}} \bar{b}$ were a subgraph of $\overline{\mathcal{B}}$ and \bar{b} had valency 2 in $\widehat{\mathcal{B}}$ then $C_G(b) = \langle b, a, c \rangle Z$ by (11), so that $C_G(b)$ would be abelian of index 4 in G .

Next, $\widehat{\mathcal{B}}$ has no vertices of valency more than 3. Indeed, let $b \in \mathcal{B}$ and $L = C_G(b)$. Let the vertex \bar{x} be adjacent to \bar{b} ; that is to say, $x \in \mathcal{B} \cap L \setminus \langle b \rangle Z$. For such an x we have $L' = [L, x] \triangleleft [G, x]$. Since $[G, x]$ has only three maximal subgroups the injectivity of the above mapping f gives that the valency of \bar{x} is at most 3, hence either 2 or 3 by (11). Let n be the number of the vertices of valency 3. These are the only vertices of odd valency in $\widehat{\mathcal{B}}$; hence n is even. By (13) any vertex of valency 2 is adjacent to two vertices of valency 3. If two different vertices of valency 2 were adjacent to the same two vertices then $\widehat{\mathcal{B}}$ would have a circuit of length 4, which we have excluded. It follows that $n > 2$. Assume that $n = 4$. Suppose first that one of the vertices of valency 3, say \bar{x} , is adjacent to each of the three vertices of valency 2; call them \bar{a} , \bar{b} and \bar{c} . By (12) we have $\langle a^2 \rangle = C_G(a)'$, $\langle b^2 \rangle = C_G(b)'$ and $\langle c^2 \rangle = C_G(c)'$, and also $[G, x] = \langle a^2, x^2 \rangle = \langle b^2, x^2 \rangle = \langle c^2, x^2 \rangle$. Hence a^2 , b^2 , c^2 and x^2 are four pairwise different nontrivial elements of $[G, x]$, a plain contradiction. Having disposed of this possibility, it is easy to see that the same argument used to exclude $n = 2$ gives that the subgraph of $\widehat{\mathcal{B}}$ obtained by cancelling all edges joining two vertices of valency 3 is of one of the following types:



where the labelled vertices have valency 3 and the unlabelled ones have valency 2. In the former case x cannot be adjacent to z , otherwise there would be a circuit of length 3 involving a vertex of valency 2. Then x is adjacent to both y and t thus giving rise to a circuit of length 4, which is impossible. In the second case x must be adjacent to y , z and t and again $\widehat{\mathcal{B}}$ has circuits of length 4. This contradiction shows that $n \neq 4$. The only possibility left is $n = 6$, which means that $\overline{\mathcal{B}}$ has only one vertex, say a , of valency 2. Let u and v be the vertices adjacent to a . Since there are neither circuits of length 3 involving a nor circuits of length 4, drawing the edges of $\overline{\mathcal{B}}$ with endpoint u or v gives a subgraph \mathcal{G} with endpoint u or v gives a subgraph \mathcal{G} , call it \mathcal{G} . The four unlabelled vertices, that have valency 1 in \mathcal{G} , have valency 3 in $\overline{\mathcal{B}}$. Let \mathcal{S} be the subgraph on these four vertices whose edges are the edges of $\overline{\mathcal{B}}$ not appearing in \mathcal{G} . Each of the vertices will have valency 2 in \mathcal{S} ; hence the edges of \mathcal{S} will give a circuit of length four. This is the final contradiction, which proves that $|\overline{\mathcal{B}}| = 13$.

Now the description of the \sim -equivalence classes set out just before (11) shows that G has a subgroup of index 4, say B , such that $(B/Z) \setminus \{Z\}$ is an equivalence class with respect to \sim , consisting of seven elements, and the remaining six \sim -equivalence classes are singletons.

Moreover \mathcal{B} is split into seven equivalence classes with respect to σ . To compute their possible sizes we first observe the following.

17. Let L, K be distinct elements of \mathcal{L} such that $L' = K'$. Then $LK < G$.

Indeed, assume that $G = LK$. Then $[G, L \cap K] \leq L'$; hence the elements of $L \cap K$ have breadth at most 1 in G . Thus $L \cap K \leq Z$, which is impossible since $|G : L \cap K| = 16$.

18. Each σ -equivalence class has order 1 or 3.

Let \bar{a} and \bar{b} be different elements of $\overline{\mathcal{B}}$ such that $\bar{a} \sigma \bar{b}$. Let $L = C_G(a)$ and $K = C_G(b)$, so $L' = K'$. Since $\bar{x} \in \overline{\mathcal{B}} \mapsto C_G(x) \in \mathcal{L}$ is bijective it will be enough to show that there exists exactly one more element $U \in \mathcal{L}$ such that $U' = L'$. By (17) we have $M := LK < G$. Let $D := L \cap K$. Hence $M/D \simeq V_4$ and there exists exactly one subgroup strictly contained between D and M and different from L and K ; call it U . Now, $[D, M] = [D, LK] \leq L'$; hence $D/L' \leq Z(M/L')$ and $D < U$

gives $U' = L'$ (and $U \in \mathcal{L}$). Thus U has the required property. Also, $M' \neq L'$ by Lemma 4.1; hence $D/L' = Z(M/L')$. For a contradiction, suppose that there exists $T \in \mathcal{L} \setminus \{L, K, U\}$ such that $T' = L'$. If $T \leq M$ then $M = LT$, so $(L \cap T)/L' \leq Z(M/L') = D/L'$. This implies $D < T < M$, which is impossible by the definition of U . Therefore $T \not\leq M$ and $G = MT$. Hence $[G, D \cap T] \leq [M, D]T' = L'$. Thus $\text{br}_G(x) \leq 1$ for all $x \in D \cap T$, so $D \cap T \leq Z$. As $|G : D| = 8$ and $|G : T| = 4$ it follows that $D \cap T = Z$ and $G = DT$. So $G = LT$, against (17). Thus (18) is proved.

For all $x \in B \setminus Z$ we have $[G, x] = [G, B] \simeq V_4$. Let $b \in \mathcal{B}$ and let $L = C_G(b)$. If $LB < G$ then $|L : L \cap B| \leq 2$, so $L' = [L, L \cap B] \leq [G, B]$. Otherwise, if $G = LB$ then $G' \leq L'[G, B]$ and so $L' \not\leq [G, B]$. There are four subgroups of order 2 in G' not contained in $[G, B]$; hence there are four σ -equivalence classes in \mathcal{B} of elements $\bar{b} = bZ$ for which the second case occurs. For any such b we have $[L, L \cap B] \leq L' \cap [G, B] = 1$ and $|L : L \cap B| = 4$; hence $L \cap B = Z(L) = \langle b \rangle Z$. Thus $b \in B$. Now, $|B : L \cap B| = 4$, so $\text{br}_B(b) = 2$. The last equality yields $|B/Z(B)| > 4$; hence $Z(B) = Z$ and $B \notin \mathcal{L}$.

Noncentral elements of B have breadth 1 or 2 in B . So we can distinguish among three types of elements of \mathcal{B} :

- (\circ): those of the form \bar{b} such that $b \in \mathcal{B} \setminus B$;
- (\triangle): those of the form \bar{b} such that $b \in B$ and $\text{br}_B(b) = 1$;
- (\square): those of the form \bar{b} such that $b \in B$ and $\text{br}_B(b) = 2$.

Let us have a look at how the 13 elements of \mathcal{B} are divided between the three types. The elements of type \triangle or \square form the (only) \sim -equivalence class of order 7. As just seen every $\bar{b} \in \mathcal{B}$ is of type \square if and only if $G = BC_G(b)$, and such elements fill four σ -equivalence classes. Each of these classes has an odd number of elements by (18); hence the number of elements of type \square is even, at least 4. Hence the number of elements of type \triangle is odd, at most 3. In particular there are elements of breadth 1 in B . Thus B has a maximal subgroup A that is abelian. Clearly the three nontrivial cosets of Z in A are of type \triangle . We conclude that \mathcal{B} has 6 elements of type \circ , 3 of type \triangle and 4 of type \square (those contained in $B \setminus A$). This last piece of information, together with our observation about \sim -classes, shows also that each of the elements of type \square is σ -equivalent to itself only.

19. Let $b \in \mathcal{B}$ and assume that \bar{b} is of type \circ . Then $b^2 \in [G, b]$.

For $\{\bar{b}\}$ is a \sim -equivalence class, i.e., the centre of $G/[G, b]$ is $\langle b \rangle Z/[G, b]$, of index 16. From [3], Lemma 2.6, we also get that G has a normal subgroup N such that $N \cap Z = [G, b]$ and G/N is isomorphic to the central product of D_8 and Q_8 . Now $NZ/[G, b] \leq Z(G/[G, b]) = \langle b \rangle Z/[G, b]$. By comparing orders we get $\langle b \rangle Z/[G, b] = NZ/[G, b] \simeq V_4$. Hence $b^2 \in [G, b]$, as claimed.

Now we shall examine in some detail the graph $\widehat{\mathcal{B}}$. In drawing subgraphs of its the symbols \circ , \triangle and \square will represent vertices of the corresponding types, while plain dots will represent vertices whose type is not specified.

20. $\widehat{\mathcal{B}}$ has no subgraph of the form .

This is a direct consequence of (15), since each element of type \square is σ -equivalent to itself only.

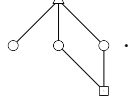
21. Let \bar{b} a vertex of $\widehat{\mathcal{B}}$ of type \circ . Then \bar{b} is adjacent to exactly one vertex of type \triangle and two vertices of type \square .

Let $L = C_G(b)$. By the characterization of the vertices of type \square we have $LB < G$, so $B < LB$ and $L \cap B < B$. Moreover $L = (L \cap B)Z(L)$, whence $L \cap B$ is not abelian and $L \cap B \neq A$. Now every nontrivial coset of Z in B is a vertex of $\widehat{\mathcal{B}}$; it is adjacent to \bar{b} if and only if it is contained in L , and it is of type \triangle or \square according to whether it is contained in A or not. This proves (21).


22. The three vertices of type \triangle are pairwise adjacent and each of them is adjacent to exactly two vertices of type \circ .

Indeed, the vertices of type \triangle are the cosets \bar{b} such that $b \in A \setminus Z$, where A is our subgroup of index 8. Since A is abelian they are pairwise adjacent. Assume that one of them is adjacent to three

vertices of type \circ . By (21) each of these vertices is adjacent to two vertices of type \square . Since there are only four vertices of type \square it follows that $\widehat{\mathcal{B}}$ has a subgraph of the form



However, this contains a subgraph forbidden by (20). Since there are six vertices of type \circ and three of type \triangle , (22) now is an easy consequence of (21).

23. $\widehat{\mathcal{B}}$ has no subgraph of the form .

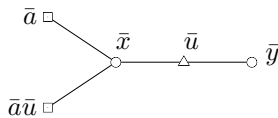
For, assume that $\widehat{\mathcal{B}}$ has such a subgraph. Let \bar{u} be its vertex of type \triangle and \bar{x} one of the two vertices of type \circ . The remaining vertex must be $\bar{u}\bar{x}$, otherwise the three vertices would generate an abelian subgroup of index 4 in G . Let $v \in A \setminus \langle u \rangle Z$. Then (21) shows that $[x, v] = [ux, v] \neq 1$. Also, $x^2 \in [G, x]$ and $u^2x^2 = (ux)^2 \in [G, ux]$, by (19). We remind the reader that G has a subgroup B of index 4 such that $(B/Z) \setminus \{Z\}$ is an equivalence class with respect to the relation \sim described just before (11). As $[G, u] = [G, v] = [G, uv] = [G, B]$ property core-2 yields $\langle u, v \rangle^2 = [G, B]$; in particular $u^2 \in [G, B]$. Now, suppose that $x^2 = [x, v]$. Then $u^2x^2 \in [G, B] \cap [G, ux]$. The latter intersection is $\langle [x, v] \rangle$, because $[G, B] \neq [G, ux]$ as $\bar{u} \approx \bar{u}\bar{x}$ (a vertex of type \circ is \sim -equivalent to itself only). Hence $u^2x^2 = [x, v] = x^2$, a contradiction. Therefore $x^2 \neq [x, v]$. Similarly $(ux)^2 \neq [ux, v] = [x, v]$. Thus $[G, x] = \langle [x, v], x^2 \rangle$ and $[G, ux] = \langle [x, v], u^2x^2 \rangle$. Now, apply property core-2 to the abelian subgroup $\langle x, u \rangle$. As $[x, v] = [ux, v]$ belongs to $[G, x]$, to $[G, ux]$ and also to $[G, u] = [G, v]$ we have $[x, v] \in \langle x, u \rangle^2$. But then $[G, x] = \langle u^2, x^2 \rangle = [G, ux]$. As $\bar{x} \approx \bar{u}\bar{x}$ this is a contradiction, and (23) is proved.

24. $\widehat{\mathcal{B}}$ has no edge of the form $\circ \text{---} \circ$.

By contradiction, let \bar{x} and \bar{y} be two adjacent vertices of type \circ . Step (21) provides two vertices \bar{u} and \bar{v} of type \triangle such that $[x, u] = 1 = [y, v]$. Moreover, $\bar{u} \neq \bar{v}$ by (23). So, $\bar{x}, \bar{y}, \bar{v}$ and \bar{u} form a circuit of length 4. As $C_B(x)$ has index 2 in $C_G(x)$ we have $y = ax$ for some $a \in B$. If $a \in A$ then $[y, u] = [a, u] = 1$ in contradiction to (14); hence $a \notin A$; i.e., \bar{a} is of type \square . Now xv commutes with both u and av , because $[x, a] = [x, y] = 1$ and so $[xv, av] = [x, v][v, a] = [x, v][v, x^{-1}][v, y] = 1$. Since u, av and xv are independent modulo Z , we get $\text{br}_G(xv) \leq 2$, and $xv \in \mathcal{B}$. Similarly $yu \in \mathcal{B}$. Of course $\bar{x}\bar{v}$ and $\bar{y}\bar{u}$ are of type \circ . Now apply (22) to the three vertices of type \triangle , that are \bar{u}, \bar{v} and $\bar{u}\bar{v}$. The two vertices of type \circ adjacent to \bar{u} are \bar{x} and $\bar{x}\bar{v}$; those adjacent to \bar{v} are \bar{y} and $\bar{y}\bar{u}$. Thus the remaining two vertices of type \circ , call them \bar{t} and \bar{s} , are adjacent to $\bar{u}\bar{v}$. Also, since $G = BC_G(a)$ and $\{x, y, xv, yu\} \subseteq B\langle x \rangle$ it follows from (11) that one of t and s , say t , does not lie in $B\langle x \rangle$ and commutes with a . Next, $C_G(uv) = A\langle t \rangle$; hence $\bar{s} = \bar{t}\bar{w}$, where w is one of u, v and uv . If $w = uv$ then $\bar{u}\bar{v}, \bar{t}$ and \bar{s} give rise to a subgraph of the type excluded by (23). Hence $w \in \{u, v\}$. By (21) we know that \bar{s} is adjacent to two of the four vertices of type \square , which are $\bar{a}, \bar{a}\bar{u}, \bar{a}\bar{v}$ and $\bar{a}\bar{u}\bar{v}$. If one of the two were \bar{a} or $\bar{a}\bar{u}\bar{v}$ then s would commute with a , which is false because $[t, a] = 1 \neq [w, a]$. Hence $[s, av] = [s, au] = 1$. Now $[tu, au] = [t, u][u, a] = [u, at]$ and $[tv, av] = [v, at]$. As $s \in \{tu, tv\}$ one of u and v commutes with at . But $C_G(u) = A\langle x \rangle$ and $C_G(v) = A\langle y \rangle$ are contained in $B\langle x \rangle$, while $at \notin B\langle x \rangle$. This contradiction proves (24).

We are now in position to complete the proof of the Theorem.

Steps (21) and (22) ensure that, starting from a vertex \bar{x} of type \circ , we can construct a subgraph of $\widehat{\mathcal{B}}$ of the form



As in the proof for (24), from $C_G(u) = A\langle x \rangle$ it follows that $\bar{y} = \bar{x}\bar{w}$ for some $w \in \{u, v, uv\}$, and by the partial result proved there $[y, x] \neq 1$; hence $w \neq u$. Thus the four vertices of type \square are \bar{a} , $\bar{a}\bar{u}$, $\bar{a}\bar{v}$ and $\bar{a}\bar{uv}$. From (20) we get $[y, a] \neq 1 \neq [y, au]$. Therefore (21) yields $[y, aw] = [y, auw] = 1$. Now $1 = [y, aw] = [xw, aw] = [w, ax]$. Then $C_G(ax)$ contains a , x and w , which are independent modulo Z , and it follows that $ax \in \mathcal{B}$. But $[ax, x] = 1$, so, by (24), we have reached the final contradiction. The proof of the Theorem is now complete. \square

References

- [1] J.T. BUCKLEY, J.C. LENNOX, B.H. NEUMANN, H. SMITH, J.WIEGOLD, Groups with all subgroups normal-by-finite, *J. Austral. Math. Soc. Ser. A* **59** (1995) 384–398.
- [2] G. CUTOLO, E.I. KHUKHRO, J.C. LENNOX, S.RINAURO, H. SMITH, J.WIEGOLD, Locally finite groups all of whose subgroups are boundedly finite over their cores, *Bull. London Math Soc.* **29** (1977) 563–570.
- [3] G. CUTOLO, E.I. KHUKHRO, J.C. LENNOX, S.RINAURO, H. SMITH, J.WIEGOLD, Finite core- p -groups, *J. Algebra* **188** (1997) 701–719.
- [4] THE GAP GROUP, “GAP—Groups, Algorithms, and Programming”, Version 4.2; Aachen, St. Andrews 1999. <http://www-gap.dcs.st-and.ac.uk/~gap>.
- [5] J.D. GILLAM, A note on finite metabelian p -groups, *Proc. Amer. Math. Soc.* **25** (1970) 189–190.
- [6] J.C. LENNOX, H. SMITH, J.WIEGOLD, Finite p -groups in which subgroups have large cores, in ‘Infinite groups 1994 (Ravello)’, de Gruyter, Berlin, 1996, pp. 163–169.
- [7] H. SMITH, J.WIEGOLD, Locally graded groups with all subgroups normal-by-finite, *J. Austral. Math. Soc. Ser. A* **60** (1996) 222–227.
- [8] M.R. VAUGHAN-LEE, J. WIEGOLD, Breadth, class and commutator subgroups of p -groups, *J. Algebra* **32** (1974) 268–277.
- [9] J. WIEGOLD, Groups with boundedly finite classes of conjugate elements, *Proc. Roy. Soc. London Ser. A* **238** (1957) 389–401.