The nilpotency class of p-groups in which subgroups have few conjugates

GIOVANNI CUTOLO, HOWARD SMITH AND JAMES WIEGOLD

ABSTRACT. We consider the problem of how the nilpotency class of a finite p-group can be bounded in terms of the maximum length of the conjugacy classes of (cyclic) subgroups. We sharpen some previously known bounds and also prove that a p-group in which every cyclic subgroup has at most p^2 conjugates has class at most 4.

Dedicated to Charles Leedham-Green on the occasion of his 65th birthday

The breadth of an element x in a finite p-group G is defined to be that integer $b = \mathrm{br}(x)$ (or $\mathrm{br}_G(x)$, if G needs to be emphasized) such that $p^b = |G : C_G(x)|$, while the breadth $\mathrm{br}(G)$ of G is the supremum of $\{\mathrm{br}_G(x) \mid x \in G\}$ (as usual, p is tacitly assumed to be a prime number, throughout). There is a wide literature on the relations between the breadth b and the nilpotency class c of G, especially on how c is bounded in terms of b—some results are collected as Lemma 1.1 below, more can be found in the introduction of [4]. C.R. Leedham-Green has been interested in this topic since its earliest stages. Although the class-breadth conjecture, stating that $c \le b+1$, has been confirmed in several cases, this conjecture is known to be false in general, at least for 2-groups, (see [4, 3]). The best general bound known still is that given by $c < 1+(pb-1)/(p-1)$, established in [5] by A.J. Gallian, a slight improvement on the bound $c < 1 + pb/(p-1)$ proved in [9]. A refinement due to M. Cartwright [1] for the case of 2-groups yields $c \le 1 + (5b/3)$ independently of the prime p.

Compared to the 'element' breadth, the analogous concept of 'subgroup' breadth has not received the same amount of attention. If H is a subgroup of the finite p-group G the subgroup breadth (or *s-breadth*) $\mathrm{sbr}_G(H)$ of H in G is defined by $p^{\mathrm{sbr}_G(H)} = |G : N_G(H)|$, and the s-breadth of G is $\mathrm{sbr}(G) := \max\{\mathrm{sbr}_G(H) \mid H \le G\}$. As far as we are aware, the first paper in the literature dealing with explicit bounds concerning s-breadth is [11], where I.D. Macdonald investigates numerical relations involving the biggest size of the conjugacy classes of subgroups in centre-by-finite groups. For instance, a special case of his Lemma 3.18 is that $\mathrm{br}(G) \le 3\,\mathrm{sbr}(G)$ for every finite p-group G. Macdonald and others also consider what we call the 'cyclic subgroup breadth', or c-breadth for short. The *c-breadth* of a finite p-group G, denoted by $\mathrm{cbr}(G)$, is the maximum of the s-breadths of cyclic subgroups of G, an invariant which in some sense provides a link between the breadth and the s-breadth of G; it is of course less than or equal to each of them. A. Mann shows in [13], Theorem 3, that $\mathrm{br}(G) \le 3\,\mathrm{cbr}(G)$ for every finite p-group G, thus improving Macdonald's result in the case of p-groups. Together with the bounds in the previous paragraph bounds like this lead to a linear bound for the class of a finite p-group depending on the c-breadth only. The aim of this paper is to contribute to improving on this bound. This will be done by showing (Proposition 1.8) that $\mathrm{br}(G)$ is actually bounded by $1 + 2\,\mathrm{cbr}(G)$ or, better, by $2\,\mathrm{cbr}(G)$ if p is odd. By comparison, it is interesting to observe that the s-breadth of a finite p-group cannot be bounded above in terms of the breadth nor, therefore, in terms of the c-breadth: for instance, for every positive integer n, if G is an extraspecial p-group of order p^{2n+1} and p is odd, then $\mathrm{br}(G) = 1$ and $\mathrm{sbr}(G) = n$; for $p = 2$ there is also the possibility $\mathrm{sbr}(G) = n - 1$".

2000 *Mathematics Subject Classification.* 20D15, 20E45.

Key words and phrases. conjugacy classes, normalizers, breadth, finite p-groups .

The first author thanks the School of Mathematics at Cardiff University for its friendly hospitality.

Our main concern is with the nilpotency class of groups with small c- or s-breadth. It is almost immediate that p-groups of c-breadth at most 1 have class at most 3; our main result (see Section 2) is that p-groups of c-breadth 2 have class at most 4. It might be that $c \leq 2 + \mathrm{sbr}(G)$ for every finite p-group G, where c still denotes the class of G. The counterexamples in [4] and [3] show that the same result is generally false if $\mathrm{sbr}(G)$ is replaced by $\mathrm{cbr}(G)$.

A final remark is that our results are stated for finite p-groups, but every p-group with finite c-breadth (with the obvious meaning) is an FC-group (by a well-known theorem of B.H. Neumann [14] it actually has finite derived subgroup, and the size of the latter is bounded in terms of the breadth and hence of the c-breadth, see [18]) and so our results immediately extend to infinite groups.

1. General results and preliminary lemmas

We shall make use of some known results relating (element) breadth and nilpotency class of finite p-groups:

Lemma 1.1. *Let G be a finite p-group of breadth b and nilpotency class c. Then:*

(*i*) (see [5]) $c < 1 + (pb-1)/(p-1)$;
(*ii*) (see [1]) *if* $p = 2$ *then* $c \leq 1 + (5b/3)$;
(*iii*) (see [8, 9, 12]) *if* $b \leq 4$ *or G is metabelian then* $c \leq b+1$;
(*iv*) (see [7]) $b = 1$ *if and only if* $|G'| = p$;
(*v*) (see [6, 10, 15]) $b = 2$ *if and only if either* $|G'| = p^2$ *or* $|G'| = |G/Z(G)| = p^3$.

Lemma 1.2 ([8]; see [13] for a generalization)**.** *Let G be a finite p-group generated by elements of breadth at most 2. Then the nilpotency class of G is at most 3.*

It is proved in [17] that if G is a finite p-group and n is an integer greater than 1 such that the elements of G of breadth at least n generate a proper subgroup then $\mathrm{br}(G) \leq 2n-3$. In the special case when $n = 2$ this gives:

Lemma 1.3. *Let G be a p-group, and assume that the elements of breadth greater than 1 in G generate a proper subgroup of G. Then* $\mathrm{br}(G) \leq 1$.

Groups with s-breadth (or, equivalently, c-breadth) 0 are nothing other than Dedekind groups, hence abelian if $p > 2$, of class at most 2 if $p = 2$. As stated in the introduction, it is very easy to prove that finite p-groups with c-breadth 1 must have class 3 at most.

Proposition 1.4. *Let G be a finite p-group. If* $\mathrm{cbr}(G) = 1$ *then the nilpotency class of G is at most* 3.

Proof. That $\mathrm{cbr}(G) \leq 1$ means that all normalizers of cyclic subgroups of G are either G itself or maximal in it, hence the Frattini subgroup is contained in the kern of G and hence in $Z_2(G)$ (see, [16, 2]; recall that the kern, or norm, of a group is the intersection of all subgroup normalizers). This proves the result. □

At least when the prime p is odd, p-groups G of c-breadth 1 are very close to having class 2: for instance, from the upcoming Proposition 1.8 and from Lemma 1.1 (v) it follows that G' has order at most p modulo $Z(G)$ in this case. Nonetheless, for every prime, it is possible for the nilpotency class to equal 3, so the bound in Proposition 1.4 is sharp, even with reference to the s-breadth. In fact, the generalized quaternion group of order 16 and the groups

$$\langle a,b,c \mid a^9 = c^3 = [b,c] = 1,\ [b,a] = c,\ [c,a] = a^3 = b^{-3}\rangle,$$
$$\langle a,b,c \mid a^{p^2} = b^p = c^p = [b,c] = 1,\ [b,a] = c,\ [c,a] = a^p\rangle, \qquad \text{if } p > 3$$

all have (order p^4, for the appropriate prime p and) class 3 and s-breadth 1, as they have kern equal to the Frattini subgroup and of index p^2.

For p-groups G with c-breadth $s > 1$ the analogue of the argument in Proposition 1.4 is obtained by looking at the actions of G on each conjugacy class of cyclic subgroups, which has size at most p^s. For every cyclic subgroup H of G, if $K_G(H)$ denotes the normal core of $N_G(H)$ in G then $G/K_G(H)$ is isomorphic to a p-subgroup of the symmetric group of degree p^s, hence

$G/K_G(H)$ can be embedded in a Sylow p-subgroup of $\mathbb{S}_{p^s}$, which is isomorphic to the s-fold iterated wreath product of groups of order p. Now the kern $K(G)$ is the intersection of all such subgroups $K_G(H)$. We draw two conclusions; the first settles the case '$p = 2$' of the problem that we are mainly interested in: bounding the class of p-groups of c-breadth 2. The bound is sharp, as is shown by the example of the generalized quaternion group of order 32.

Lemma 1.5. *Every finite 2-group of c-breadth 2 has nilpotency class at most 4.*

Proof. If $p = 2 = s$ then all the quotients $G/K_G(H)$ in the previous discussion embed in the wreath product of two groups of order two, hence $\gamma_3(G) \leq K(G) \leq Z_2(G)$. □

Lemma 1.6. *Let G be a finite p-group of c-breadth s. Then $G^{p^s} \leq K(G)$. If G is regular then $G^{p^s} \leq Z(G)$.*

Proof. By the above remarks, $G^{p^s} \leq \bigcap_{h\in G} K_G(\langle h\rangle) = K(G)$. Therefore, for every $g \in G$, the element g^{p^s} acts by conjugation on G by means of a power automorphism. Suppose that G is regular, so that all power automorphisms of G are universal (see [2]), and let x be an element of G of maximal order. Then x^{p^s} induces a universal power automorphism of G centralizing x, which has order $\exp G$, therefore $x^{p^s} \in Z(G)$. Since G^{p^s} is generated by the p^sth powers of elements of maximal order in G we have $G^{p^s} \leq Z(G)$. □

For odd primes, a special case of interest that can be easily dealt with is that of metacyclic groups.

Lemma 1.7. *Let G be a metacyclic p-group of breadth b and c-breadth s. Then $\mathrm{sbr}(G) = s$ and $p^b = |G'|$; moreover:*

- (i) *if $p > 2$ then $s = b$;*
- (ii) *if $p = 2$ then $b - 1 \leq s \leq b$.*

Proof. Since every subgroup of G is cyclic modulo its normal core we easily have that $\mathrm{sbr}(G) = s \leq b$. Let $G = \langle x\rangle\langle y\rangle$, and suppose that $\langle x\rangle \lhd G$. Then $G' = \{[x^i, y] \mid i \in \mathbb{N}\}$ and so $|G'| = p^{\mathrm{br}_G(y)}$. As clearly $p^b \leq |G'|$ we have $p^b = |G'|$ and $b = \mathrm{br}_G(y)$.

Suppose that $p > 2$. Then G is regular, so $p^b = \exp G' = \exp\big(G/Z(G)\big) \leq p^s$ by Lemma 1.6. Hence $s = b$ and we have (i).

To prove (ii), let $p = 2$ and $D = \langle x\rangle \cap \langle y\rangle$. It is clear that $s \geq \mathrm{sbr}_G\big(\langle y\rangle\big) = \mathrm{sbr}_{G/D}\big(\langle yD\rangle\big) = \mathrm{br}_{G/D}(yD) =: b'$, since the normalizer and the centralizer of $\langle yD\rangle$ in G/D coincide. Moreover $p^{b'} = |(G/D)'| \geq p^b/|D|$, thus (ii) is proved if $|D| \leq 2$. Henceforth we may assume that $|D| > 2$ and G is not abelian. Then $x^y = x^n$ where n is an integer such that $n \equiv 1 \pmod 4$. This latter congruence implies that the order of n modulo $\circ(x)$ is exactly $\circ(x)/\bar{n}$, where $\bar{n}$ is the maximal power of 2 dividing $n - 1$. It follows that $|G'| = |\langle y\rangle/C_{\langle y\rangle}(x)| \leq |G/\langle x\rangle|$ and that $b = \mathrm{br}_G(x)$.

Suppose that $\circ(x) \geq \circ(y)$, and let $q = |G/\langle x\rangle|$. Then $(G')^q = 1$; moreover $y^q x^{tq} = 1$ for some integer t, and since $G' \leq \langle x\rangle$, standard commutator collection yields:

$$(yx^t)^q = y^q x^{tq}[x, y]^{t\binom{q}{2}}[x, y, y]^{t\binom{q}{3}} \cdots [x, {}_i y]^{t\binom{q}{i+1}} \cdots [x, {}_{q-1} y]^t.$$

For every integer i such that $1 \leq i < q$ we have $[x, {}_i y] \in (G')^{4^{i-1}}$, while $\binom{q}{i+1}$ is divisible by q/r, where r is the largest power of 2 dividing $i + 1$. If $i = 1$ then $r = 2$. If $i > 1$ then r divides 2^{i-1} and so $[x, {}_i y]^{\binom{q}{i+1}} \in (G')^{4^{i-1}q/r} \leq (G')^q = 1$. Therefore $(yx^t)^q = [x, y]^{t\binom{q}{2}} \in (G')^{q/2}$. It follows that $y' := yx^t$ has order $2q$ at most, so that $G = \langle x\rangle\langle y'\rangle$ and $|\langle x\rangle \cap \langle y'\rangle| \leq 2$. Thus the proof is completed, if $\circ(x) \geq \circ(y)$, by reduction to the previous case. Therefore we may assume that $\circ(x) < \circ(y)$. There exists a power y_1 of y which has the same order as x. By applying the previous argument to y_1 in the place of y we obtain that $|\langle x\rangle \cap \langle g\rangle| \leq 2$, where $g = y_1 x^t$ for a suitable odd integer t. Now $|\langle y\rangle/C_{\langle y\rangle}(g)| = |\langle y\rangle/C_{\langle y\rangle}(x)| = p^b$, hence $\mathrm{br}_G(g) = b$. Moreover $|G' \cap \langle g\rangle| \leq 2$, so that $|N_G(\langle g\rangle)/C_G(g)| \leq 2$ and hence $s \geq \mathrm{sbr}_G(\langle g\rangle) \geq b - 1$. This proves part (ii). □

It actually happens that $s = b - 1$ in the case of (generalized) quaternion groups.

Proposition 1.8. *Let G be a finite p-group of breadth b and c-breadth s. Then $b \leq 2s$ if $p > 2$, and $b \leq 2s + 1$ if $p = 2$.*

Proof. Let $x \in G$, $C = C_G(x)$ and $N = N_G(\langle x\rangle)$. If $p > 2$ then $N = \langle y\rangle C$ for some y; since $\langle x, y\rangle$ is metacyclic of c-breadth at most s, Lemma 1.7 shows that $y^{p^s} \in C$, hence $|N/C| \le p^s$ and so $|G : C| \le p^{2s}$. The argument is similar when $p = 2$: in this case $|N : \langle y\rangle C| \le 2$ for some y, and $y^{2^{s+1}} \in C$ by Lemma 1.7, hence $|N/C| \le 2^{s+2}$ and $|G : C| \le 2^{2s+2}$. Furthermore, if $|G : C| = 2^{2s+2}$ then $|G : N| = 2^s$ and $|N/C| = 2^{s+2}$, hence $\circ(x) > 2^{s+2}$, and N/C is not cyclic, so that there exists $y \in N$ such that $x^y = x^{-1}$. Now $x^{2^{s+1}} = [x^{2^s}, y]^{-1} \in \langle x\rangle \cap \langle y\rangle$ because x^{2^s} is in the kern of G by Lemma 1.6. Then $x^{2^{s+2}} = 1$, a contradiction. □

This latter result improves on the bound $b \le 3s$ obtained by Mann [13] and quoted in the introduction. From Proposition 1.8 and from parts (i) and (ii) of Lemma 1.1 we can deduce a general bound for the nilpotency class of p-groups in terms of their c-breadths. For a further observation on Proposition 1.8 see the closing Remark 2.3.

Theorem 1.9. *Let G be a finite p-group of c-breadth s and nilpotency class c. If $p > 2$ then $c < 1 + (2ps - 1)/(p - 1)$, hence $c \le 3s$. If $p = 2$ then $c \le (8 + 10s)/3$.*

It is clear that every improvement on the bound in Lemma 1.1 (i) immediately yields an improvement on that in Theorem 1.9. In several special cases (among which are those in Lemma 1.1) it is known that the class of a p-group G is bounded by $\mathrm{br}(G) + 1$; when this happens the class of G will be at most $2s + 1$ if $p > 2$, or $2s + 2$ if $p = 2$, where $s = \mathrm{cbr}(G)$.

The following lemmas play a role in the proof in the next section. Although elementary, Lemma 1.11 could be of some independent interest and therefore we state it in a slightly more general form than strictly needed.

Lemma 1.10. *Let G be a finite p-group with c-breadth $s > 0$, and let T be a subgroup of G such that $\mathrm{sbr}_G(T) = s$ and T/T_G is cyclic. If S is the maximal subgroup of T containing T_G then, for every subgroup H of T not contained in S, we have $N_G(H) = N_G(T)$ and, in particular, $H \lhd T$.*

Proof. If $H \le T$ and $H \not\le S$ then $H = \langle H \smallsetminus S\rangle$. For every $h \in H \smallsetminus S$ we have $T = \langle h\rangle T_G$ and hence $N_G\big(\langle h\rangle\big) \le N_G(T)$. But $p^s = |G : N_G(T)|$ is the maximal possible index for the normalizer of a cyclic subgroup in G, hence $N_G\big(\langle h\rangle\big) = N_G(T)$. Thus $H \lhd N_G(T)$; as $T = HT_G$ we have $N_G(H) = N_G(T)$. □

Lemma 1.11. *Let T be a finite nonabelian p-group having a maximal subgroup S such that all subgroups of T not contained in S are normal in T. Then T has nilpotency class 2 and T' is cyclic. Moreover, if $p > 2$ there exists $x \in T \smallsetminus S$ such that $\circ(x) = \exp T$ and $T' = [x, T] \le \langle x\rangle$. For every such x we have $T = \langle x\rangle L$ where $L = \big\langle y \in T \bigm| \langle [x, y]\rangle = T'$ and $\langle x\rangle \cap \langle y\rangle = 1\big\rangle$ has exponent dividing $|\langle x\rangle/T'|$, and $S = \langle x^p\rangle L$.*

Proof. For all $x \in T \smallsetminus S$ we have $\langle x\rangle \lhd T$, hence $[T', x] = 1$. It follows that T has class 2. Arguing by contradiction, assume that T has minimal order subject to T' not being cyclic. Since the hypotheses are inherited by quotients modulo proper subgroups of T' it follows that T' is elementary abelian of rank 2. It follows that $\mathrm{br}(x) \le 1$ for every $x \in T \smallsetminus S$. By Lemmas 1.3 and 1.1 this implies that $|T'| = p$. This contradiction shows that T' must be cyclic.

To prove the remaining part of the statement assume that $p > 2$ and let $C/(T')^p = Z\big(T/(T')^p\big)$. Then $C < T$ and $T_1 := \{g \in T \mid \circ(g) < \exp T\}$ is a subgroup, because T has class 2, and $T_1 < T$. It follows that $X := C \cup T_1 \cup S \ne T$, as $p > 2$. Hence we can choose $x \in T \smallsetminus X$. Then $[x, T] = T'$. As $x \notin S$ then $\langle x\rangle \lhd T$, hence $[x, T] \le \langle x\rangle$ and x has the required properties. Fix any such x. Then $T = \langle \mathcal{T}\rangle$, where $\mathcal{T} = \{t \in T \mid \langle [x, t]\rangle = T'\}$ is the set of all elements of T that do not centralize x modulo $(T')^p$. Let $t \in \mathcal{T}$ and let p^α be the order of t modulo $\langle x\rangle$. Then $t^{p^\alpha} = x^{np^\alpha}$ for some $n \in \mathbb{N}$ (because $\circ(x) \ge \circ(t)$) and so $(tx^{-n})^{p^\alpha} = 1$. Thus $y := tx^{-n}$ has order p^α and $\langle x, t\rangle = \langle x\rangle \rtimes \langle y\rangle$. Therefore $y \in \mathcal{L} := \{u \in \mathcal{T} \mid \langle x\rangle \cap \langle u\rangle = 1\}$ and $T = \langle x\rangle L$, where $L = \langle \mathcal{L}\rangle$ is clearly normal in T. Moreover, $\mathcal{L} \subseteq S$, as $\langle y\rangle \ntriangleleft T$ for every $y \in \mathcal{L}$, hence $L \le S$; since $x^p \in S$ then $S = \langle x^p\rangle L$. It remains to prove that $\exp L \le q := |\langle x\rangle/T'|$; it will be enough to fix $y \in \mathcal{L}$ and show that $y^q = 1$. We have $|T'| \le q$, because T has class 2, hence $(xy)^q = x^q y^q$. As $xy \notin S$ we have that $\langle xy\rangle \lhd T$ and so $[x, y] = [x, xy] \in \langle xy\rangle$. Therefore $x^q \in \langle xy\rangle$ and so $y^q \in \langle xy\rangle$; as $\circ(x) \ge \circ(y)$ we have $y^q \in \langle x^q\rangle$, hence $y^q = 1$, as we wanted to prove. □

Remark 1.12. In the odd-p case the previous lemma actually characterises the groups with the property considered. In fact, let T be any finite p-group of odd order and class 2 that can be factorised as $T = \langle x \rangle L$ for some $x \in T$ and $L \le T$. If $T' = \langle x^q \rangle$ and $L^q = 1$ for some power q of p, and $S = \langle x^p \rangle L$, then every subgroup of T not contained in S contains T'; as a matter of fact it is easy to see that $H^q = T'$ for all such subgroups. (The case of 2-groups is different, the dihedral group of order 8 being an easy counterexample.) Hence, at least for groups of odd order, the property is equivalent to the apparently stronger requirement that all subgroups of T not contained in S contain T'.

We say that a p-group is minimal irregular if all its proper subgroups are regular but it is not itself regular.

Lemma 1.13. *Let G be a minimal irregular finite p-group. Then $[G^q, G] \le (G')^q$ for every power q of p.*

Proof. Let $a, b \in G$, and let $H = \langle a, a^b \rangle$. Then $H < G$ and so H is regular. Therefore

$$[a^q, b] = a^{-q}(a^b)^q = (a^{-1}a^b)^q c^q = [a, b]^q c^q$$

for some $c \in H'$, and the result follows. □

Lemma 1.14. *Let G be a torsion nilpotent 4-Engel group of class 5 with no element of order 2. Then $[a, b, b, a, a] = [a, b, a, b, a]$ and $[a, b, a, b, a]^{-2} = [a, b, a, a, b]$, for all a, $b \in G$.*

Proof. If $H = \langle a, b \rangle$ then $H/Z(H)$ is metabelian, hence $[a, b, a, b] \equiv [a, b, b, a]$ modulo $Z(H)$, so $[a, b, a, b, a] = [a, b, b, a, a]$ and $[a, b, a, b, b] = [a, b, b, a, b]$. For all integers i we have

$$1 = [a, a^i b, a^i b, a^i b, a^i b] = [a, b, a, a, b]^{i^2} [a, b, a, b, a]^{2i^2} [a, b, b, b, a]^i [a, b, b, a, b]^{2i}.$$

By considering the choices 1 and -1 for i it is easy to deduce that $1 = [a, b, a, a, b]^2 [a, b, a, b, a]^4$ and hence the result, because G has no elements of order 2. □

Clearly the lemma holds under more general hypotheses. Rather than asking that G be periodic and not involve the prime 2 it is enough to require that $\gamma_5(G)$ be a group in which square roots, where they exist, are unique. We will make use of this lemma in a situation when $\gamma_5(G)$ has exponent 3 and so the result takes the nicer form $[a, b, b, a, a] = [a, b, a, b, a] = [a, b, a, a, b]$.

2. Groups of c-breadth 2

This section contains the proof our main result:

Theorem 2.1. *Let G be a finite p-group. If $\mathrm{cbr}(G) = 2$ then the nilpotency class of G is at most 4.*

By Lemma 1.5, to prove the theorem we shall only have to consider the case when $p > 2$. The proof consists in deriving a contradiction from the assumption of the existence of a minimal counterexample. So we suppose that there exists a finite p-group G of c-breadth 2 such that all proper subgroups and quotients of G have class at most 4 while G has class 5. To simplify notation we shall write Z for $Z(G)$ and, for all positive integers i, Z_i and γ_i for $Z_i(G)$ and $\gamma_i(G)$ respectively. Every nontrivial normal subgroup of G contains γ_5, hence Z is cyclic and γ_5 is its socle. Moreover $Z_4 = \Phi(G)$, because G has class 5 and so the fact that $\gamma_5^p = 1$ implies that $G^p \le Z_4$, and, on the other hand, if $Z_4 \not\le \Phi(G)$ then $G = HZ_4$ for some $H < G$, and so G would have class 4 at most.

Lemma 2.2. *If $p > 3$ then every finite p-group of c-breadth 2 has class at most 4.*

Proof. The statement amounts to saying that our minimal counterexample G must be a 3-group. Suppose that it is not. We shall first show that then G is regular. This is straightforward if $p > 5$. If $p = 5$ we can argue as follows. Note first that if G is not regular then it is minimal irregular, given that all proper subgroups (and also quotients) of G have class at most 4. We have to prove that $(xy)^5 \equiv x^5 y^5$ modulo $(\langle x, y \rangle')^5$ for all x, $y \in G$. This is certainly true if $\langle x, y \rangle < G$, as $\langle x, y \rangle$ is regular in this case, hence we may assume that $G = \langle x, y \rangle$. For a similar reason $(xy)^5 \equiv x^5 y^5$ modulo $(G')^5 \gamma_5$. If $(G')^5 \ne 1$ then $\gamma_5 \le (G')^5$, as γ_5 is the monolith of G, and we obtain $(xy)^5 \equiv x^5y^5$ modulo $(\langle x,y\rangle')^5$, as required. If $(G')^5 = 1$ then $G^5 \le Z$ by Lemma 1.13. However it is clear that the breadth and the c-breadth of any group of prime exponent coincide, hence $\mathrm{br}(G/G^5) = \mathrm{cbr}(G/G^5) \le 2$ and so G/G^5 has class at most 3 by Lemma 1.1; hence G has class at most 4, a contradiction. Therefore G is regular, even if $p = 5$.

Now we may apply Lemma 1.6 to obtain that $G^{p^2} \le Z$. Let bars denote images modulo Z. For every $x \in G$ we have $\bar{x}^{p^2} = 1$ and so $|N_{\bar{G}}(\langle\bar{x}\rangle)/C_{\bar{G}}(\bar{x})| \le p$. It follows that $\mathrm{br}_{\bar{G}}(\bar{x}) \le 3$ and that if $\mathrm{br}_{\bar{G}}(\bar{x}) = 3$ then $N_{\bar{G}}(\langle\bar{x}\rangle) = N_G(\langle x\rangle)/Z$ and $[\bar{x}, N_{\bar{G}}(\langle\bar{x}\rangle)] \ne 1$, hence $[x,y] = x^p$ for some $y \in N_G(\langle x\rangle)$. Since $[x^{p^2}, y] = 1$ we have that x has order at most p^3. We know from Proposition 1.8 that $\mathrm{br}(G) \le 4$, hence $\mathrm{br}_G(x)$ is either 3 or 4. In the former case $C_G(x)/Z = C_{\bar{G}}(\bar{x})$ and so $x \in C_G(Z_2)$, in the latter $|N_G(\langle x\rangle)/C_G(x)| = p^2$ and so x has order p^3. Let $U = \langle g \in G \mid \mathrm{br}_{\bar{G}}(\bar{g}) \le 2\rangle$ and $\mathcal{W} = \{g \in G \mid \mathrm{br}_G(g) = 4 \text{ and } \mathrm{br}_{\bar{G}}(\bar{g}) = 3\}$. By the above discussion $G = U \cup \mathcal{W} \cup C_G(Z_2)$. Since $U < G$, because U/Z has class at most 3 by Lemma 1.2, and G cannot be the union of three proper subgroups (as $p \ne 2$) we have that $G = \langle\mathcal{W}\rangle$. We also showed that every element of $\mathcal{W}$ has order p^3, hence $\exp G = p^3$ by regularity. Now G^{p^2} is contained in Z and has exponent p, therefore $G^{p^2} = \gamma_5$.

Fix $x \in \mathcal{W}$. As we showed, there exists $y \in N_G(\langle x\rangle)$ such that $[x,y] = x^p$, and so $y^p \ne 1$. We may also choose y such that it has order p^2: if $y^{p^2} \ne 1$ then $\langle y^{p^2}\rangle = \gamma_5 = \langle x^{p^2}\rangle$, and so some element of the coset $y\langle x\rangle$ will have order p^2. Fix such an element y, and let $H = \langle x,y\rangle = \langle x\rangle \rtimes \langle y\rangle$. Since $\langle y\rangle$ has p^2 conjugates in H and $\mathrm{cbr}(G) = 2$ then the G-conjugates of $\langle y\rangle$ are exactly the H-conjugates of $\langle y\rangle$, so that $\langle y\rangle^G = \langle y\rangle^H = \langle y, x^p\rangle$ (and $G = \langle x\rangle N_G(\langle y\rangle)$). Now $|\langle y, x^p\rangle| = p^4$, thus $y \in Z_4 = \Phi(G)$ (see the remarks immediately preceding this lemma). On the other hand H/H_G is cyclic, because $H = \langle x\rangle\langle y\rangle^G$, and H has class 3, so Lemmas 1.10 and 1.11 imply that $|G : N_G(H)| \le p$. Also, $N_G(\langle x\rangle) \le N_G(H)$ and $\langle x^p\rangle = H'$ is normal in $N_G(H)$ but not in G, for otherwise $[\Phi(G), x^p] = 1$, which is false as $y \in \Phi(G)$ and $[y, x^p] \ne 1$. Thus $N_G(\langle x\rangle) \lessdot N_G(H) = N_G(\langle x^p\rangle) \lessdot G$ (the symbol '$\lessdot$' meaning 'is a maximal subgroup of'). Let $N = N_G(\langle x\rangle) \cap N_G(\langle y\rangle)$ and $L = N_G(\langle x^p\rangle) \cap N_G(\langle y\rangle)$. As $G = \langle x\rangle N_G(\langle y\rangle)$ we have $N \lessdot L \lessdot N_G(\langle y\rangle)$. Since y acts faithfully on $\langle x\rangle$ it is easy to see that N centralizes y. Let $g \in N_G(\langle y\rangle) \smallsetminus L$. If g^p normalizes $\langle x\rangle$ then $[x, g^p] \in \langle x^{p^2}\rangle \lhd G$ (recall that $g^{p^2} \in Z$). But then, by regularity, $[x^p, g] \in \langle x^{p^2}\rangle$ and so g normalizes $\langle x^p\rangle$, which is false. Therefore $g^p \notin N$, hence $L = N\langle g^p\rangle$ and so $[L, y] = 1$. Now $G' \le N_G(H) \cap \langle x^p\rangle N_G(\langle y\rangle) = \langle x^p\rangle L$, hence $[G', y] \le \langle x^{p^2}\rangle = \gamma_5$. On the other hand $[y, G, x] = [y, \langle x\rangle N_G(\langle y\rangle), x] \le [\langle x^p, y^p\rangle, x] = \gamma_5$, hence the Hall-Witt identity yields $[x^p, g] = [x, y, g] \in \gamma_5$, and this is again a contradiction, since g does not normalize $\langle x^p\rangle$. □

Now we know that our minimal counterexample G must be a 3-group. Let K be the kern of G. By the same argument used to prove Lemma 1.5 we have that K is the intersection of normal subgroups $K_G(H)$ such that $G/K_G(H)$ is isomorphic to a subgroup of the wreath product W of two groups of order 3, each $K_G(H)$ being the normal core of the normalizer of a cyclic subgroup H of G. Extending the first half of Lemma 1.6 we conclude that:

$$\Phi(G'G^3) \cdot [G^3, G] \le K \le Z_2, \text{ in particular } G^3 \le Z_3, \tag{1}$$

since the corresponding verbal subgroups in W are trivial. Let $u,v,w,g \in G$ and $k = [u,v,w,g]$. Then $\big[[u,v,w],k\big] = 1$ and $\big[[u,v],[u,v,w]\big] \in Z$, hence $k^3 = \big[[u,v,w]^3, g\big] = \big[[u,v]^3, w, g\big]$, so that $k^3 = 1$ because $[u,v]^3 \in Z_2$ by (1). This shows that

$$\gamma_4^3 = 1. \tag{2}$$

Since the class of G/K is at least 3, we must have that $G/K_G(H) \simeq W$ for at least one (cyclic) $H \le G$. Choose one such H and let $S := K_G(H)$. Then $G/S \simeq W$, hence $G/S = (B/S) \rtimes (T/S)$, where $|T/S| = 3$ and B/S is elementary abelian. By looking at the structure of W, we also have that $SG^3 = S\gamma_3$ and $T \lessdot N_G(T) = T\gamma_3$. Therefore T and $S = T_G$ satisfy the hypothesis of Lemma 1.10 and hence T has the structure described in Lemma 1.11 if it is not abelian, in particular, T' is cyclic and central in T. In agreement with the notation in Lemma 1.11, choose $x \in T \smallsetminus S$ so that $\circ(x) = \exp T$ and $T' = [T, x]$, and let $\mathcal{L} = \{y \in T \mid \langle[x,y]\rangle = T' \text{ and } \langle x\rangle \cap \langle y\rangle = 1\}$. For every $y \in \mathcal{L}$ we can apply Lemma 1.7 to $\langle x,y\rangle$ and conclude that $|T'| \le 9$. Also fix $b \in B \smallsetminus SG'$, so that $G = \langle S, x, b\rangle$. We aim at proving that $G = \langle x, b\rangle$. To this purpose it will be enough to show that $S \le Z_4$, since $Z_4 = \Phi(G)$. Suppose first that $|T'| = 9$. For each $y \in \mathcal{L}$

the subgroup $\langle y\rangle$ has 9 conjugates in $H_y := \langle x, y\rangle$, hence $\langle y\rangle^G = \langle y\rangle^{H_y} = \langle y\rangle T'$. As $G^3 \leq Z_3$ and $T' \leq \langle x^3\rangle$, now $\langle y^3\rangle T' \leq Z_3$, but $|\langle y\rangle^G/\langle y^3\rangle T'| = 3$, hence $\langle y\rangle^G \leq Z_4$. Therefore $S \leq Z_4$ in this case, and we may assume that $|T'| \leq 3$. Let $N := N_G(\langle b\rangle)$. We have $N \leq B$, because B is the normalizer of $\langle b\rangle$ modulo S, hence $|B/N| \leq 3$ and so $[S, b] \leq B' \leq N$. Thus $[S, b, b, b] = 1$. Suppose that $T' \lhd G$. Then $T' \leq \gamma_5$ and so $[S, b, b, T] \leq [S, b, T] \leq [S, T] \leq Z$. Since $G = \langle T, b\rangle$ it follows that $S \leq Z_4$. Otherwise, if $T' \ntriangleleft G$ then $S' < T'$, hence S is abelian, and $Z(T) \lessdot S$. Also, $|S/S \cap N| \leq 3$ and $b^3 \in S$; it follows that $|S/C_S(b)| \leq 9$. Therefore $Z = C_{Z(T)}(b)$ has index at most 27 in S, hence $S \leq Z_4$ also in this case. So we have that

$$G = \langle x, b\rangle.$$

Now, since $\operatorname{cbr}(G) = 2$ every cyclic subgroup of G has subnormal defect at most 3, hence G is 4-Engel. As $\gamma_5^3 = 1$, Lemma 1.14 shows that:

$$\begin{aligned} &[x, b, x, b, b] = [x, b, b, x, b] = [x, b, b, b, x]\\ &[x, b, b, x, x] = [x, b, x, b, x] = [x, b, x, x, b]. \end{aligned} \tag{3}$$

In order that G be of class 5 the commutators in at least one of these two rows must be nontrivial. Then $[x, b, b, x] \notin Z$. Since $\gamma_3 \leq N_G(T)$ and $N_G(T) = N_G(\langle x\rangle)$ by Lemma 1.10, we have that $[\gamma_3, x] \leq \langle x\rangle \cap \gamma_4$; by (2) it follows that $[\gamma_3, x]$ lies in the socle of $\langle x\rangle$. As $[x, b, b, x] \notin Z$ this implies that $\gamma_5 \nleq \langle x\rangle$. But $[\gamma_4, x] \leq \langle x\rangle \cap \gamma_5$, hence $[\gamma_4, x] = 1$. It follows that all the commutators in (3) are trivial, and this contradiction completes the proof.

Remark 2.3. As happens for $p = 2$ and the quaternion group of order 32, also for the odd primes p there exist finite p-groups of class 4 and c-breadth, and even s-breadth, 2. These groups can be chosen to have breadth 4, hence, at least for this small value of s, the bounds in Proposition 1.8 are attained. For $p = 3$ one such example is the group with the following presentation:

$$\begin{aligned} \langle a, b, x, y \mid\ & a^3 = y^9 = x^{27} = [a, y] = [b, y] = [a, b] = 1,\\ & b^3 = x^9,\ [x, y] = x^3,\ [x, b] = x^9 y^{-3},\ [x, a] = x^{-3} b\rangle, \end{aligned}$$

while for $p > 3$ the analogous example is:

$$\begin{aligned} \langle a, b, x, y \mid a^p = b^p = x^{p^3} = y^{p^2} = [a, y] = [b, y] = [a, b] = 1,\\ [x, y] = x^p,\ [x, b] = y^p,\ [x, a] = b\rangle. \end{aligned}$$

In both cases the group has order p^7 and the fact that it has s-breadth (and therefore c-breadth) 2 can be checked along the following lines. The elements of order at most p^2 form a maximal subgroup M such that $|M/Z(M)| = p^2$. If H is a subgroup with more than p^2 conjugates then its normalizer N has order at most p^4, hence $|H| \leq p^3$. On the other hand $H \nleq M$, for otherwise $Z(M) < N$. Therefore H must be cyclic of order p^3, but it can be directly checked that then there exists some element of N that induces by conjugation an automorphism of H of order p^2, so that $|N/H| \geq p^2$, which is again a contradiction.

It is also worthwhile to stress that, as anticipated in the introduction, the fact that the class c of a finite p-group G is bounded above by $2 + \operatorname{cbr}(G)$ for the small values of $\operatorname{cbr}(G)$ considered (that is 1 and 2) is far from being a general rule, at least when $p = 2$. As a matter of fact the counterexamples in [4] show that for every integer n there are finite 2-groups G such that $c - \operatorname{br}(G)$ and, a fortiori, $c - \operatorname{cbr}(G)$ is greater than n.

References

[1] M. Cartwright, *Class and breadth of a finite p-group*, Bull. London Math. Soc. **19** (1987), no. 5, 425–430.
[2] C.D.H. Cooper, *Power automorphisms of a group*, Math. Z. **107** (1968), 335–356.
[3] B. Eick, M.F. Newman, and E.A. O'Brien, *The class breadth conjecture revisited*, preprint.
[4] W. Felsch, J. Neubüser, and W. Plesken, *Space groups and groups of prime-power order. IV. Counterexamples to the class-breadth conjecture*, J. London Math. Soc. (2) **24** (1981), no. 1, 113–122.
[5] J.A. Gallian, *On the breadth of a finite p-group*, Math. Z. **126** (1972), 224–226.
[6] N. Gavioli, A. Mann, V. Monti, A. Previtali, and C.M. Scoppola, *Groups of prime power order with many conjugacy classes*, J. Algebra **202** (1998), no. 1, 129–141.
[7] H.-G. Knoche, *Über den Frobenius'schen Klassenbegriff in nilpotenten Gruppen*, Math. Z. **55** (1951), 71–83.
[8] ——, *Über den Frobeniusschen Klassenbegriff in nilpotenten Gruppen. II*, Math. Z. **59** (1953), 8–16.

[9] C.R. Leedham-Green, P.M. Neumann, and J. Wiegold, *The breadth and the class of a finite p-group*, J. London Math. Soc. (2) **1** (1969), 409–420.
[10] P. Longobardi and M. Maj, *On p-groups of breadth two*, Algebra Colloq. **6** (1999), no. 2, 121–124.
[11] I.D. Macdonald, *Some explicit bounds in groups with finite derived groups*, Proc. London Math. Soc. (3) **11** (1961), 23–56.
[12] ———, *Groups of breadth four have class five*, Glasgow Math. J. **19** (1978), no. 2, 141–148.
[13] A. Mann, *Groups generated by elements of small breadth*, J. Group Theory **4** (2001), no. 3, 241–246.
[14] B.H. Neumann, *Groups with finite classes of conjugate subgroups*, Math. Z. **63** (1955), 76–96.
[15] G. Parmeggiani and B. Stellmacher, *p-groups of small breadth*, J. Algebra **213** (1999), no. 1, 52–68.
[16] E. Schenkman, *On the norm of a group*, Illinois J. Math. **4** (1960), 150–152.
[17] M.R. Vaughan-Lee and J. Wiegold, *Breadth, class and commutator subgroups of p-groups*, J. Algebra **32** (1974), 268–277.
[18] J. Wiegold, *Groups with boundedly finite classes of conjugate elements*, Proc. Roy. Soc. London. Ser. A. **238** (1957), 389–401.

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 address: cutolo@unina.it
URL: http://www.dma.unina.it/~cutolo/

Department of Mathematics, Bucknell University, Lewisburg, Pennsylvania 17837, USA.
E-mail address: howsmith@bucknell.edu

School of Mathematics, Cardiff University, Cardiff CF 24 4AG, United Kingdom
E-mail address: wiegoldj@cardiff.ac.uk