Can. J. Math., Vol. XXXII, No. 6, 1980, pp. 1448–1458

ON THE NUMBER OF AUTOMORPHISMS OF A FINITE p-GROUP

THEODOROS EXARCHAKOS

Introduction. In this paper we find a new bound for the function $g(h)$, for which $|A(G)|_p \geqq p^h$ whenever $|G| \geqq p^{g(h)}$, G a finite p-group. The existence of such a function was first conjectured by W. R. Scott in 1954, who proved that $g(2) = 3$. In 1956 Ledermann and Neumann proved that in the general case of finite groups $g(h) \leqq (h-1)^3 \cdot p^{h-1} + h$ [**10**]. Since then, J. A. Green, J. C. Howarth and K. H. Hyde have reduced this bound considerably. The best (least) bound to date for finite p-groups was obtained by K. H. Hyde [**9**]. He proved that $g(h) = \frac{1}{2}h(h-3) + 3$ for $h \geqq 5$ and $g(h) = h + 1$ for $h \leqq 4$. For finite non-abelian p-groups, we improve this bound to: $g(h) = \frac{1}{6}h^2$ for $h \geqq 13$, $g(h) = 2h - 5$ for $5 < h \leqq 8$, $g(h) = h$ for $h \leqq 5$ and for $8 < h \leqq 12$ we prove that $g(9) = 14$, $g(10) = 17$, $g(11) = 20$, $g(12) = 23$.

The following notation is used: G is taken to be a finite non-abelian p-group with commutator subgroup G' and center Z. The order of G is denoted by $|G|$ and $|H|_p$ is the largest power of p dividing $|H|$. Hom (G, Z) is the set of all homomorphisms of G into Z and $A(G)$, $A_c(G)$, $I(G)$ are the groups of automorphisms, central automorphisms, inner automorphisms of G respectively. G is called a *PN-group* if it has no non-trivial abelian direct factor. We denote the lower and the upper central series of G by

$$G = L_0 > L_1 = G' > \ldots > L_c = 1 \quad \text{and}$$
$$G = Z_c > Z_{c-1} > \ldots > Z_1 = Z > Z_0 = 1.$$

Throughout this paper c is the class of G and we take the invariants of G/G' to be $m_1 \geqq m_2 \geqq \ldots \geqq m_t \geqq 1$ and the invariants of Z to be $k_1 \geqq k_2 \geqq \ldots \geqq k_s \geqq 1$, where t and s are the numbers of invariants of G/G' and Z respectively. For non-cyclic p-groups G, $t \geqq 2$, as G/G' is cyclic, if and only if G is cyclic. Also we take $|G/G'| = p^m$ and $|Z| = p^k$. The cyclic group of order p^r is denoted by C_{p^r}.

It has been conjectured that for finite non-cyclic p-groups of order greater than p^2, $g(h) \leqq h$. This has been established for abelian p-groups, for p-groups of class two and for some other special classes of finite p-groups. I believe that in the general case the above conjecture is not valid and that $g(h) > h$.

Received March 20, 1979 and in revised form June 2, 1980.

For $c = 2$ we have $g(h) \leqq h$ [**5**]. Therefore we shall assume that $c > 2$, whenever $g(h) > h$.

LEMMA 1. *If G is a PN-group, then $|A_c(G)| = p^a$, where*

$$(1) \qquad a = \sum_{j,i} \min (m_j, k_i) \quad \textit{and}$$

(i) $a \geqq jk + (t - j)s$, *if* $m_j \geqq k_1$ *for some* j, $t \geqq j \geqq 1$.
(ii) $a \geqq im + (s - i)t$, *if* $k_i \geqq m_1$ *for some* i, $s \geqq i \geqq 1$. *In particular, if* $k_i \geqq m_1 > k_{i+1}$ *then* $a \geqq im + k - (k_1 + \ldots + k_i) + (t - 1)(s - i)$, *and if* $k_s \geqq m_1$, *then* $a = sm$.

Proof. Since G is a PN-group, $|A_c(G)| = |\text{Hom}\,(G, Z)|$ [**1**]. Hence

$$|A_c(G)| = |\text{Hom}\,(G, Z)| = |\text{Hom}\,(G/L_1, Z)|$$
$$= \left|\text{Hom}\left(\prod_j C_{p^{m_j}}, \prod_i C_{p^{k_i}}\right)\right| = \prod_{j,i} |\text{Hom}\,(C_{p^{m_j}}, C_{p^{k_i}})| = p^a,$$

where

$$a = \sum_{j,i} \min (m_j, k_i).$$

Therefore

$$a \geqq jk + \sum_{x=j+1,\, i=1}^{t,s} \min (m_x, k_i) \geqq jk + (t - j)s \quad \text{for } m_j \geqq k_1.$$

Similarly $a \geqq im + (s - i)t$ for $k_i \geqq m_1$. If $k_i \geqq m_1 > k_{i+1}$,

$$a \geqq im + \sum_{f=i+1}^{s} k_f + \sum_{j=2,\, f=i+1}^{t,s} \min (m_j, k_f) \geqq im + k$$
$$- (k_1 + \ldots + k_i) + (t - 1)(s - i).$$

For $k_s \geqq m_1$, $\min (m_j, k_i) = m_j$, so that $a = ms$.

LEMMA 2. *Let G be a PN-group of class $c > 2$. Then $|A_c(G)| \cdot p^{c-1}$ is a factor of $|A(G)|$.*

Proof. Since G/Z_{c-1} is not cyclic and $|Z_i/Z_{i-1}| \geqq p$, $i = 1, \ldots, c - 1$,

$$|G/Z_2| \geqq p^{c-1} \quad \text{and}$$
$$|A(G)| \geqq |A_c(G) \cdot I(G)| = |A_c(G)| \cdot |I(G)|/|A_c(G) \cap I(G)|$$
$$= |A_c(G)|\,|G/Z_2| \geqq |A_c(G)| \cdot p^{c-1}.$$

From Lemmas 1 and 2 we get:

LEMMA 3. *If G is a PN-group of class $c > 2$, then*

$$|A(G)| \geqq p^{a+c-1} \geqq p^{2s+c-1},$$

where s is the number of invariants of Z.

https://doi.org/10.4153/CJM-1980-114-0 Published online by Cambridge University Press

LEMMA 4. *If G is a 2-generator finite p-group of class c, then*

$$Z_{c-1} \leqq \Phi(G) \quad \text{and} \quad \exp(G/Z_{c-1}) = \exp L_{c-1}.$$

Proof. If $Z_{c-1} \nleqq \Phi(G)$, we can find two generators a and b for G with $a \in Z_{c-1}$. Then all $(c-1)$-fold commutators in a and b are 1 and so G has class less than c, a contradiction. For $a_0, a_1, \ldots, a_{c-1} \in G$,

$$[a_0, a_1, \ldots, a_{c-1}]^{p^n} = [a_0^{p^n}, a_1, \ldots, a_{c-1}]$$

for any positive integer n. This implies that $\exp(G/Z_{c-1}) = \exp L_{c-1}$.

LEMMA 5. *If $m_1 \geqq m_2 \geqq \ldots \geqq m_t \geqq 1$ are the invariants of G/L_1, then*

$$\exp G \leqq p^{m_1+m_2(c-1)}.$$

For $t = 2$ and $c > 2$,

$$\exp Z \leqq \exp Z_{c-2} \leqq p^{m_1+m_2(c-1)-2}.$$

Proof. By [**2**] $p^{m_2} \geqq \exp(L_1/L_2) \geqq \ldots \geqq \exp(L_{c-1}/L_c)$. So $\exp L_1 \leqq p^{m_2(c-1)}$ and hence $\exp G \leqq p^{m_1+m_2(c-1)}$.

Let $t = 2$. Then G can be generated by two elements. From Lemma 4 we have

$$\exp(G/Z_{c-1}) = \exp L_{c-1} = p^n \text{ (say)}.$$

Since G/Z_{c-1} is not cyclic, $|G/Z_{c-1}| \geqq p^{n+1}$ and so $|G/Z_{c-2}| \geqq p^{n+2}$. Also

$$|L_1/L_2| \leqq p^{m_2} \quad \text{and} \quad |G/L_2| = |G/L_1|\cdot|L_1/L_2| \leqq p^{m_1+2m_2}.$$

But $L_2 \leqq Z_{c-2}$. So

$$|Z_{c-2}/L_2| = |G/L_2|/|G/Z_{c-2}| \leqq p^{m_1+2m_2-n-2}.$$

Therefore,

$$\exp Z \leqq \exp Z_{c-2} \leqq |Z_{c-2}/L_2|\cdot\exp L_2 \leqq p^{m_1+m_2(c-1)-2},$$

as $\exp L_2 \leqq p^{m_2(c-3)+n}$.

The following is an immediate consequence of Lemma 8.5 in [**10**].

LEMMA 6. *If G is a finite p-group, $|G/Z| = p^b$ and $k_1 \geqq k_2 \geqq \ldots \geqq k_s \geqq 1$ are the invariants of Z, then $A(G)$ has a p-subgroup F of outer automorphisms which is isomorphic to $F \cong F_1 \times F_2 \times \ldots \times F_s$, where $|F_i| = \sup(1, p^{k_i-b})$ and $|F| \geqq |Z|\cdot p^{-bs}$.*

We also need the following result by W. Gaschütz [**6**].

LEMMA 7. *Every finite non-abelian p-group has an outer automorphism of order p^i for some $i \geqq 1$.*

Remark 1. K. G. Hummel [**7**] (generalized by J. Buckley [**4**]) showed that if K is a maximal subgroup of G and $Z \nleqq K$, then $p|A(K)|_p$ divides

$|A(G)|$. If $g(h)$ is a strictly increasing integer function, then $g(h) - 1 \geqq g(h-1)$ and so, inductively, we may assume that $Z \leqq K$ for every maximal subgroup K of G. This means we may assume that G is a PN-group and $Z \leqq \Phi(G)$, where $\Phi(G)$ is the Frattini subgroup of G.

THEOREM 1. *Let G be a finite p-group of class $c > 2$. If $|G| \geqq p^h$, then $|A(G)|_p \geqq p^h$, where h is an integer with $h \leqq 5$.*

Proof. Since $c > 2$, by Lemma 3 the only case to consider is $c = 3$, $h = 5$, $s = 1$. For $|Z| = p$, Lemma 7 gives $|A(G)|_p \geqq p|I(G)| = |G| \geqq p^h$. Let $|Z| > p$. If $m = 2$, Lemma 5 gives $k_1 \leqq c - 2 = p$, where $\exp Z = p^{k_1}$. Then Z is not cyclic, a contradiction. If $m \geqq 3$, Lemma 1 gives $a \geqq 3$ and by Lemma 3 we get $|A(G)|_p \geqq p^5 = p^h$.

THEOREM 2. *Let G be a finite p-group of class $c > 2$. If $|G| \geqq p^{g(h)}$, then $|A(G)|_p \geqq p^h$, where h is an integer, $5 < h \leqq 8$ and $g(h) = 2h - 5$.*

Proof. Let $|G/Z| = p^b$. If $b \geqq h - 1$, then by Lemma 7 $|A(G)|_p \geqq p \cdot p^b \geqq p^h$. So we take $b \leqq h - 2$. Then

(1) $\quad k \geqq g(h) - (h-2) = h - 3,$

where $|Z| = p^k$. If $k_1 \leqq m_1$, by Lemma 1(i), $a \geqq k + 1 \geqq h - 2$ and Lemma 3 gives $|A(G)|_p \geqq p^h$. Thus we take $k_1 > m_1$. Then Lemma 1(iii) gives

$$a \geqq m + (s-1)t.$$

By Lemma 3 we may assume that

(2) $\quad m + (s-1)t + c \leqq h \leqq 8;$

otherwise we have nothing to show. Since $m \geqq 2$, $t \geqq 2$, $c \geqq 3$ from (2) we get $s \leqq 2$.

(a) $s = 2$. Then $m + t + c \leqq h$, $h = 7$ or 8. For $h = 7$, $m = 2$, $t = 2$, $c = 3$, $k \geqq h - 3 = 4$. By Lemma 5, $k_1 \leqq c - 2 = 1$ and so $s = k \geqq 4$, a contradiction.

Let $h = 8$. Then $k \geqq 5$, $k_1 > 2$, $m \leqq 3$. For $m = 2$, $k_1 \leqq c - 2 \leqq 2$. For $m = 3$, $c = 3$ and $t = 2$. Then G/G' has type (p^2, p) and Lemma 5 gives $k_1 \leqq c - 1 = 2$. In both cases we have a contradiction.

(b) $s = 1$. Then $k_1 = k \geqq h - 3$, $m + c \leqq h \leqq 8$. So $m \leqq 5$ and $c \leqq h - 2 \leqq 6$. Consider the following subcases:

(b_1) $m = 2$. Then $k_1 \leqq c - 2$, $h - 3 \leqq k_1 \leqq c - 2$. So $c \geqq h - 1$, a contradiction.

(b_2) $m = 3$. If $t = 2$, $k_1 \leqq c - 1$ and so $h - 3 \leqq c - 1$, which gives $c \geqq h - 2$. But $m + c \leqq h$ gives $c \leqq h - 3$. If $t = 3$, then $G' = \Phi(G) \geqq Z$ and $\exp G' \leqq p^{c-1}$. Hence $k_1 \leqq c - 1$, a contradiction.

(b_3) $m = 4$. Then $c \leqq h - 4$. If $m_1 = 1$, then $G' = \Phi(G) \geqq Z$, $\exp G' \leqq p^{c-1}$ and so $k_1 \leqq c - 1$. So $h - 3 \leqq k_1 \leqq c - 1$ and $c \geqq h - 2$.

Take $m_1 > 1$. Then G/G' has type (p, p^3), (p, p, p^2) or (p^2, p^2). In the first case Lemma 5 gives $k_1 \leqq c$. In the second case $\exp Z \leqq \exp \Phi(G) \leqq p^c$, so that $k_1 \leqq c$. Then in both cases $c \geqq h - 3$, a contradiction.

Let G/L_1 have type (p^2, p^2). Then L_1/L_2 is cyclic of order at most p^2. For $c = 3$, $h \geqq 7$, $|L_2| \geqq p^3$ and $\exp L_2 \leqq p^2$. This is a contradiction, as $L_2 \leqq Z$ and Z is cyclic. But $3 \leqq c \leqq h - 4 \leqq 4$. So we may assume that $c = 4$ and $h = 8$. Since

$$|A(G)|_p \geqq |A_c(G)||G/Z_2| \quad \text{and} \quad |A_c(G)| \geqq p^4$$

we get $|G/Z_2| = p^3$. So $|G/Z_3| = p^2$, $|Z_3/Z_2| = p$, $|L_1Z/L_1| \leqq p$ and $|L_2Z/L_2| \leqq p^2$. Let $|L_2Z/L_2| \leqq p$. Since $\exp L_3 = \exp\ (G/Z_3) = p$ and $\exp\ (L_2/L_3) \leqq p^2$ we get

$$\exp Z \leqq \exp\ (L_2Z) \leqq p^4,$$

which contradicts (1). So $|L_2Z/L_2| = p^2$. Since $L_2 \leqq Z_2$ and $L_2 < L_1 \leqq C_G(Z_2)$, $L_2 \leqq Z(Z_2)$. Hence $L_2Z \leqq Z(Z_2)$. This gives that Z_2 is abelian, as $|Z_2/L_2Z| \leqq p$. Now $L_1 \nleqq Z_2$. Pick an element $x \in L_1$ with $x \notin Z_2$. Since $x \in Z_3 \backslash Z_2$ and $|Z_3/Z_2| = p$ we get that $Z_3 = \langle x, Z_2 \rangle$. Hence Z_3 is abelian as $x \in C_G(Z_2)$. Let $a \in G$, $b \in L_1$. Then

$$[a^p, b] \equiv [a, b^p] \equiv [a, b]^p \bmod L_3.$$

But a^p, b are both elements of Z_3 which is abelian. So $[a^p, b] = 1$. Therefore $[a, b]^p \in L_3\ \forall\ a \in G$ and $\forall\ b \in L_1$. This implies that $\exp L_2/L_3 = p$. Then

$$\exp Z \leqq \exp\ (L_2Z) \leqq p^4,$$

a contradiction.

(b_4) $m = 5$. Then $h = 8$, $c = 3$.

Let $m_2 = 1$. If $t = 2$, by Lemma 5, $k_1 \leqq 4$. If $t > 2$, $\exp \Phi(G) \leqq p^4$ and again $k_1 \leqq 4$, a contradiction. So we take $m_2 > 1$ and G/G' has type either (p^3, p^2) or (p^3, p^2, p). In the first case $|L_1/L_2| \leqq p^2$ and so $|L_2| \geqq p^4$. But $\exp L_2 \leqq p^2$ and L_2 is cyclic. This is a contradiction. In the second case $|L_1/L_2| \leqq p^4$ and so $|G/L_2| \leqq p^9$, which gives that $|L_2| \geqq p^2$. Since $|A_c(G)| \geqq p^5$, by the proof of Lemma 2 we get $|G/Z_2| = p^2$. Also $L_1 \leqq Z(Z_2)$, as $Z_2 \leqq C_G(L_1)$. Let $x \in L_2 \leqq Z$. Then x is a product of commutators of the form $[a, b]$ and $[a, b]^{-1} = [b, a]$ with $a \in G$, $b \in L_1$. But $[a, b]$ and $[b, a]$ commute with both a and b, so $[a, b]^p = [a^p, b] = 1$ and $[b, a]^p = [b, a^p] = 1$, as $a^p \in Z_2$ and $b \in L_1 \leqq Z(Z_2)$. This gives $x^p = 1\ \forall\ x \in L_2$, as L_2 is abelian. Therefore $\exp L_2 = p$. But L_2 is cyclic of order greater than p. This is a contradiction.

THEOREM 3. *Let G be a finite p-group of class $c > 2$.*

https://doi.org/10.4153/CJM-1980-114-0 Published online by Cambridge University Press

(i) *If* $|G| \geqq p^{14}$ *then* $|A(G)|_p \geqq p^9$,
(ii) *If* $|G| \geqq p^{17}$ *then* $|A(G)|_p \geqq p^{10}$,
(iii) *If* $|G| \geqq p^{20}$ *then* $|A(G)|_p \geqq p^{11}$ *and*
(iv) *If* $|G| \geqq p^{23}$ *then* $|A(G)|_p \geqq p^{12}$.

Proof. We give the proof of the case (iv), which is the more complicated. The proofs of the other cases are of the same pattern and are therefore omitted.

Let $|G/Z| = p^b$. If $b \geqq 11$, $|A(G)|_p \geqq p \cdot p^b \geqq p^{12}$. Therefore we take $b \leqq 10$. So

(1) $k \geqq 23 - 10 = 13$.

If Z is cyclic, by Lemma 6 we get

$$|A(G)| \geqq |F| \cdot |I(G)| \geqq p^k \cdot p^{-b} \cdot p^b = p^k \geqq p^{13}.$$

Assume that Z is not cyclic and so $s > 1$. If $k_1 \leqq m_1$, Lemma 1 gives $a \geqq k + s > 13$. Take $k_1 > m_1$. By Lemma 3 it is enough to show that $a + c - 1 \geqq 12$. Therefore we may assume that

(2) $a + c \leqq 12$.

Since $k_1 > m_1$, Lemma 1 gives $a \geqq m + (s-1)t$ and so

(3) $m + (s-1)t + c \leqq 12$,

which gives $s \leqq 4$.

(a) $s = 4$. Then $m + 3t + c \leqq 12$, $t = 2$, $m \leqq 3$, $c \leqq 4$. By Lemma 5 we get $k_1 \leqq c - 1 \leqq 3$. Then $s \geqq \frac{1}{3}k > 4$.

(b) $s = 3$. Then (3) gives $m + 2t + c \leqq 12$, $m \leqq 5$, $c \leqq 6$ and $k_1 \geqq 5$. For $m = 2$, $k_1 \leqq c - 2 \leqq 4$, a contradiction. For $m = 3$ and $t = 2$, $k_1 \leqq c - 1 \leqq 4$, as $c \leqq 5$ in this case. For $m = 3$ and $t = 3$, $c = 3$, $k_1 \leqq c = 3$, a contradiction. For $m = 4$, $c \leqq 4$ and Lemma 5 gives $k_1 \leqq 2c - 2 \leqq 6$. Then $k_2 \geqq 4$ and Lemma 1(i) gives $a \geqq 10$. This is impossible as $a + c \leqq 12$. For $m = 5$, $c = 3$, $t = 2$. Then $k_1 \leqq 2c - 1 \leqq 5$. So $k_2 \geqq 4$ and by Lemma 1, $a \geqq 12$, a contradiction.

(c) $s = 2$. Then $m + t + c \leqq 12$, $m \leqq 7$, $c \leqq 8$ and $k_1 \geqq 7$. For $m = 2$, $k_1 \leqq c - 2 \leqq 6$, a contradiction. For $m = 3$ and $t = 3$, $c \leqq 6$ and $k_1 \leqq c \leqq 6$. For $m = 3$ and $t = 2$, $c \leqq 7$ and $k_1 \leqq c - 1 \leqq 6$. For $m = 4$, $c \leqq 6$ and $k_1 \leqq 2c - 2 \leqq 10$. So $k_2 \geqq 3$ and by Lemma 1, $a \geqq 8$ which together with (2) gives $c \leqq 4$. Then $k_1 \leqq 2c - 2 \leqq 6$. For $m = 5$, $c \leqq 5$ and Lemma 5 gives $k_1 \leqq 2c \leqq 10$. Then $k_2 \geqq 3$ and $a \geqq 9$, which gives $c = 3$. So $k_1 \leqq 2c = 6$. Hence in all the above cases we have a contradiction, as $k_1 \geqq 7$.

For $m = 6$, $c \leqq 4$ and $k_1 \leqq 3c - 2 \leqq 10$. So $k_2 \geqq 3$, $a \geqq 10$, a contradiction.

For $m = 7$, $c = 3$, $t = 2$. So $k_1 \leqq 3c - 1 = 8$, $k_2 \geqq 5$ and $a \geqq 13$, a contradiction.

https://doi.org/10.4153/CJM-1980-114-0 Published online by Cambridge University Press

THEOREM 4. *Let G be a finite p-group of class $c > 2$ and $g(h) = h^2/6$, where h is an integer, $h \geqq 13$. If $|G| \geqq p^{g(h)}$, then $|A(G)|_p \geqq p^h$.*

Proof. By Remark 1, we shall assume that G is a PN-group. Let $|G/Z| = p^b$. If $b \geqq h - 1$, Lemma 7 gives $|A(G)|_p \geqq p|I(G)| = p^{b+1} \geqq p^h$. Take $b \leqq h - 2$. Then

(1) $\quad k \geqq g(h) - (h - 2) = h^2/6 - h + 2 > h.$

If $k_1 \geqq h$ Lemma 6 gives

$$|A(G)|_p \geqq |F_1| \cdot |I(G)| \geqq p^h.$$

So $k_1 \leqq h - 1$. If $k_1 = h - 1 = k_2$,

$$|A(G)|_p \geqq |F_1||F_2||I(G)| \geqq p^{2h-b-2} \geqq p^h,$$

as $b \leqq h - 2$. Therefore we may assume that

(2) $\quad k_1 \leqq h - 1 \quad$ and $\quad k_i \leqq h - 2 \quad$ for $i \geqq 2$

Then

$$(h - 2)(s - 1) \geqq k - k_1 \geqq \tfrac{1}{6}h^2 - h + 2 - (h - 1) = \tfrac{1}{6}(h - 10)(h - 2) - \tfrac{1}{3}.$$

Since s is an integer we get

(3) $\quad s - 1 \geqq (h - 10)/6.$

Let $|A_c(G)| = p^a$. By Lemma 3 it is enough to show that $a \geqq h - c + 1$. So we take

(4) $\quad h \geqq a + c.$

If $k_1 \leqq m_1$, by Lemma 1(i) we get $a \geqq k + s > h$, a contradiction. So $k_1 > m_1$ and applying Lemma 1(ii) we get

(5) $\quad a \geqq im + t(s - i) \quad$ for $k_i \geqq m_1$,

(6) $\quad a \geqq im + k - (k_1 + \ldots + k_i) + (t - 1)(s - i) \quad$ for $\quad k_i \geqq m_1 > k_{i+1}$.

Next applying Lemma 5 we get: For $m = 6$, $k_1 \leqq 3c - 2$ if $t = 2$, and $k_1 \leqq 2c + 1 \leqq 3c - 2$ if $t > 2$. So

(7) $\quad k_1 \leqq 3c - 2 \quad$ for $m = 6$.

Also,

(8) $\quad k_1 \leqq 2c \quad$ for $m = 5$,

(9) $\quad k_1 \leqq 2c - 2 \quad$ for $m = 4$,

(10) $\quad k_1 \leqq c \quad$ for $m = 3 \quad$ and

(11) $\quad k_1 \leqq c - 2 \quad$ for $m = 2$.

Consider the following cases.

(a) $m \geqq 5$. Let $k_i \geqq m_1 > k_{i+1}$ and $m \geqq 6$. By (4) $h \geqq 6i + 5$. Then for $i > 1$,

$$\begin{aligned} 0 &\leqq 6i - 11 = (3i-1)^2 - 9i^2 + 12i - 12 \\ &\leqq (h - 3i - 6)^2 - 9i^2 + 12i - 12 \\ &= h^2 - 6h(i+2) + 48i + 24. \end{aligned}$$

For $i = 1$ this inequality reduces to $h^2 - 18h + 72 \geqq 0$, which is valid for $h \geqq 13$.

From (1), (2) and (6) we have

$$\begin{aligned} a &\geqq 6i + k - (k_1 + \ldots + k_i) + 1 \\ &\geqq 6i + \tfrac{1}{6}h^2 - h + 2 - h + 1 - (i-1)(h-2) + 1 \\ &\geqq \tfrac{1}{6}h^2 - h(i+1) + 8i + 2 \geqq h - 2 \geqq h - c + 1. \end{aligned}$$

Next let $m = 5$. Then (8) gives

(12) $\quad 2cs \geqq k \geqq \frac{1}{6}h^2 - h + 2.$

First let $k_i \geqq m_1 > k_{i+1}$. Then from (4) and (6), $h \geqq 5i + c + 2 > 4i + c + 2$. For $i > 1$,

$$\begin{aligned} 0 &< (2i - c + 1)^2 + 12i^2 - 6i - 9 = (4i + c - 4)^2 - 24 \\ &\qquad\qquad + 30i - 12ci + 6c \\ &\leqq (h-6)^2 - 24 + 30i - 12ci + 6c \\ &= h^2 - 12h + 12 + 30i - 12ci + 6c. \end{aligned}$$

So

(13) $\quad h^2 - 12h + 12 + 30i - 12ci + 6c > 0.$

For $i = 1$ this inequality reduces to $h^2 - 12h + 42 - 6c > 0$, which is valid for $h \geqq 13$, $h \geqq 6 + c$. Therefore (6) gives

$$\begin{aligned} a &\geqq 5i + k - (k_1 + \ldots + k_i) + 1 \\ &\geqq 5i + \tfrac{1}{6}h^2 - h + 2 - 2ci + 1 \geqq h - c + 1 \end{aligned}$$

by (13). Now let $k_s \geqq m_1$. Then by (4), (5) and Lemma 1 we get

(14) $\quad h \geqq ms + c \quad$ and $\quad a = ms.$

For $m \geqq 7$, (3) gives

$$a \geqq 7s \geqq \tfrac{7}{6}(h - 10) + 7 \geqq h - 2 \geqq h - c + 1,$$

as $h \geqq 7s + c \geqq 17$ since (3) implies $s > 1$. Similarly for $m = 6$,

$$a = 6s \geqq h - 10 + 6 \geqq h - c + 1,$$

unless $c \leqq 4$. For $c \leqq 4$, (7) gives $k_1 \leqq 10$ so that $10s \geqq k$ and

https://doi.org/10.4153/CJM-1980-114-0 Published online by Cambridge University Press

$h \geqq 6s + c \geqq 15$. Hence

$$60s \geqq 6k \geqq h^2 - 6h + 12 \geqq 10(h - 2).$$

Thus $a = 6s \geqq h - 2 \geqq h - c + 1$.

Finally take $m = 5$. By (14), $h \geqq 10 + c$. Here $5h^2 - 6h(5 + 2c) + 12c^2 - 12c + 60 \geqq 0$, since the discriminant $D = -96c^2 + 96c - 300$ of the left side of the inequality is negative. So by (12)

$$10cs \geqq 5k \geqq \tfrac{5}{6}h^2 - 5h + 10 \geqq 2c(h - c + 1).$$

Hence $a = 5s \geqq h - c + 1$.

(b) $m = 4$. Let $k_i \geqq m_1 > k_{i+1}$. By (9) $k_1 \leqq 2c - 2$ and so

(15) $\quad 2s(c - 1) \geqq k \geqq \tfrac{1}{6}h^2 - h + 2.$

From (4) and (5) we get $h \geqq 4i + c + 2$. So substituting in (6),

$$a \geqq 4i + \tfrac{1}{6}h^2 - h + 2 - i(2c - 2) + 1$$
$$= \tfrac{1}{6}h^2 - h + 6i - 2ci + 3 \geqq h - c + 1$$

by (13). Let $k_s \geqq m_1$. Then $a = 4s$ and $h \geqq 4s + c$. For $h \geqq 17$, (3) gives $s \geqq 3$. So $h \geqq 12 + c$. Therefore

$$h^2 - 6h + 12 \geqq 3(c - 1)(h - c + 1) \quad \text{or}$$
$$h^2 - 3h(c + 1) + 3c^2 - 6c + 15 \geqq 0,$$

since if the discriminant $D = -3c^2 + 42c - 51$ of the left side of the inequality is not negative, then $c \leqq 12$ and

$$2h \geqq 24 + 2c = 3(c + 1) + (21 - c) \geqq 3(c + 1) + \sqrt{D}.$$

For $c = 3$ or 4 this inequality reduces to $h^2 - 12h + 24 \geqq 0$, $h^2 - 15h + 39 \geqq 0$, which are valid for $h \geqq 13$. Substituting in (15) we get

$$4s(c - 1) \geqq 2k \geqq \tfrac{1}{3}h^2 - 2h + 4 \geqq (c - 1)(h - c + 1).$$

This gives $a = 4s \geqq h - c + 1$ for $h \geqq 17$ or $c \leqq 4$. Let $16 \geqq h \geqq 13$, $c > 4$. From (4) and (5), $c \leqq 8$. Then $a = 4s \geqq h - c + 1$, unless $c = 8$, $h = 16$; $c = 7$, $h = 15, 16$; $c = 6$, $h = 14, 15, 16$; $c = 5$, $h = 13, 14, 15, 16$. For these cases by substituting in (15) we get $s \geqq 3$, so again $a = 4s \geqq h - c + 1$.

(c) $m = 3$. Let $k_i \geqq m_1 > k_{i+1}$. Then $t = 2$ and Lemma 5 gives $k_1 \leqq c - 1$. From (4) and (6), $h \geqq 3i + c + 2$. Then for all i,

$$0 < \tfrac{1}{6}(9i^2 + c^2 - 2c - 8) = \tfrac{1}{6}(3i + c - 4)^2 - 4 - ic + 4i + c$$
$$\leqq \tfrac{1}{6}(h - 6)^2 - 4 - ic + 4i + c = \tfrac{1}{6}h^2 - 2h - ic + 4i + c + 2.$$

Substituting in (6),

$$a \geqq 3i + \tfrac{1}{6}h^2 - h + 2 - i(c - 1) + 1$$
$$= \tfrac{1}{6}h^2 - h - ic + 4i + 3 \geqq h - c + 1.$$

Let $k_s \geqq m_1$. From (10), $k_1 \leqq c$. Then $cs \geqq k \geqq \frac{1}{6}h^2 - h + 2$ so that

$$3cs \geqq \tfrac{1}{2}h^2 - 3h + 6 \geqq c(h - c + 1),$$

since $h^2 - 2h(c + 3) + 2c^2 - 2c + 12 \geqq 0$. In fact, if the discriminant $D = -4c^2 + 32c - 12$ of the left side of the inequality is not negative, then $c \leqq 7$ and $h > 12 = (3 + c) + (9 - c) \geqq 3 + c + \frac{1}{2}\sqrt{D}$. Hence $a = 3s \geqq h - c + 1$.

(d) $m = 2$. From (11), $k_1 \leqq c - 2$ so that

$$(16) \quad (c - 2)s \geqq k.$$

Here $h^2 - 3ch + 3c^2 - 9c + 18 \geqq 0$ for $h \geqq 15$, or for $h \geqq 13$ provided $c \leqq 6$ or $c \geqq 10$. In fact, if the discriminant $D = -3c^2 + 36c - 72$ of the left side of the inequality is not negative, then $c \leqq 9$ and

$$2h \geqq 30 = 3c + 3(10 - c) \geqq 3c + \sqrt{D}.$$

Similarly for $h \geqq 13$, if $D \geqq 0$ then $c \leqq 9$ and

$$2h > 24 = 3c + 3(8 - c) \geqq 3c + \sqrt{D}$$

provided $c \leqq 6$. From (16),

$$(17) \quad 2(c - 2)s \geqq 2k \geqq \tfrac{1}{3}h^2 - 2h + 4.$$

Therefore

$$2(c - 2)s \geqq \tfrac{1}{3}h^2 - 2h + 4 \geqq ch - c^2 + 3c - 2 - 2h$$
$$= (c - 2)(h - c + 1),$$

which gives $a = 2s \geqq h - c + 1$, except when $c = 7, 8, 9$ and $h = 13, 14$. For these cases direct substitution of the values of h and c in (17) gives $a = 2s \geqq h - c + 1$.

Remark 2. I think that the bound $g(h) = 2h - 5$, $5 < h \leqq 8$ is the best possible. But the bound $g(h) = h^2/6$, $h \geqq 13$ is definitely not the best. For example, using a similar technique, we can take $g(18) = 52$ instead of $(18)^2/6 = 54$. Even for large values of h, $g(h) = h^2/6$ can be reduced.

References

1. J. E. Adney and Ti Yen, *Automorphisms of a p-group*, Illinois J. Math. *9* (1965), 137–143.
2. N. Blackburn, *On a special class of p-groups*, Acta Math. *100* (1958), 45–92.
3. ——— *On prime-power groups with two generators*, Proc. Camb. Phil. Soc. *54* (1958), 327–337.
4. J. Buckley, *Automorphism groups of isoclinic p-groups*, J. London Math. Soc. *12* (1975), 37–44.
5. R. Faudree, *A note on the automorphism group of a p-group*, Proc. Amer. Math. Soc. *19* (1968), 1379–1382.
6. W. Gaschütz, *Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen*, J. of Algebra *4* (1966), 1–2.

7. K. G. Hummel, *The order of the automorphism group of a central product*, Proc. Amer. Math. Soc. *47* (1975), 37–40.
8. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin, Heidelberg, 1967).
9. K. H. Hyde, *On the order of the Sylow subgroups of the automorphism group of a finite group*, Glasgow Math. J. *11* (1970), 88–96.
10. W. Ledermann and B. H. Neumann, *On the order of the automorphism group of a finite group II*, Proc. Roy. Soc. Ser. A. *235* (1956), 235–246.

Koridallos, Athens,
Greece