Proceedings of the Edinburgh Mathematical Society (1998) **41**, 369–384 ©

THE NUMBER OF CONJUGACY CLASSES IN SOME QUOTIENTS OF THE NOTTINGHAM GROUP

by P. P. PÁLFY*

(Received 19th August 1996)

We determine the number of conjugacy classes in the natural quotient groups of the Nottingham group over the p-element field up to the quotient of order p^{3p+1}.

1991 *Mathematics subject classification:* primary 20D60, secondary 20D15, 20E18.

Introduction

The number of conjugacy classes, $k(G)$, is a measure of commutativity of a finite group G, since it is equal to the number of commuting pairs of elements in G, divided by the order of G. Finite p-groups tend to have a relatively large degree of commutativity in one sense or another, hence it can be expected that they have a relatively large number of conjugacy classes. If $|G| = p^{2n+e}$ with $n \geq 0, e \in \{0, 1\}$, then a nice result of Philip Hall (see [**3**, p. 549]) states that

$$k(G) = (p^2 - 1)n + p^e + (p^2 - 1)(p - 1)a, \tag{1}$$

where a is a non-negative integer, called the *abundance* of the finite p-group G. This yields a logarithmic lower bound

$$k(G) \geq (p^2 - 1)n + p^e$$

for the number of conjugacy classes in a p-group. However, for many types of finite p-groups a lower bound of the form $k(G) > |G|^\epsilon$ (for some $\epsilon > 0$) has been established; see the excellent survey paper of A. Shalev [**10**], in particular Propositions 4.8, 6.4 and 7.6 there. It is unknown how sharp the logarithmic bound obtained from Hall's formula is. L. Pyber [**6**] formulated the problem of deciding whether there exists an infinite series of p-groups (with fixed p) such that $k(G) < c \log |G|$ for some constant c. Concerning this question A. Shalev (see [**10**, p. 409]) writes: "It is a common belief that the finite quotients of the Nottingham group have this property; this has not been verified." (For the definition of the Nottingham group and its natural quotients see Section 1 below.)

* Research supported by the Hungarian National Research Foundation (OTKA), grant no. 16432.

I. O. York proved in his thesis ([11, p. 105]) that for the natural quotient group of order p^{2n+e} with $2n+e \le p+1$ of the Nottingham group over the p-element field the number of conjugacy classes is $(p^2-1)n+p^e$, so these quotients have abundance 0. (In fact York determined the number of conjugacy classes in the natural quotients of the Nottingham group over the p^r-element field up to the order $p^{r(p+1)}$.) However, no p-group of order more than p^{p+2} can have abundance 0 (see Poland [5]). In fact, groups of order p^{p+2} and abundance 0 exist only for $p=2,3,5$, and 7 (see Rothe [7] for their construction; and Fernández-Alcober [2] for their nonexistence if $p \ge 11$). It is an open problem (see [10, Problem 4]) if there are only finitely many p-groups (with fixed p) of any given abundance.

In the present paper we extend the calculation of the number of conjugacy classes of the natural quotients of the Nottingham group up to the quotient of order p^{3p+1} and show the following

Theorem. *The abundance of the natural quotient of order p^t of the Nottingham group over the p-element field is*

$$\begin{array}{rll} 0 & \textit{if} & 1 \le t \le p+1; \\ \left[\dfrac{t-p}{2}\right] & \textit{if} & p+2 \le t \le 2p+1; \\ p\left[\dfrac{t-2p}{2}\right]+\left[\dfrac{t-p}{2}\right] & \textit{if} & 2p+2 \le t \le 3p+1. \end{array} \tag{2}$$

These formulae have been anticipated on the basis of extensive computer calculations by A. Caranti (for $p=3$) and by L. Lévai (for $p=3,5,7,11,13,17$) using the GAP package [9].

J. Sangroniz [8] has independently determined the number of conjugacy classes in the natural quotients of the Nottingham group over an arbitrary finite field of q elements for the quotients of order q^t with $p+2 \le t \le 2p+1$, where $p>2$ is the characteristic of the field. He obtained (using the notation $t=2n+e$, $n \ge 0$, $e \in \{0,1\}$) that the number of conjugacy classes is

$$(q^2-1)n+q^e+(q^2-1)(q-1)\left(n+e-\frac{p+1}{2}\right)-(q-p)(q-1)^2.$$

Although our result has only limited scope, it does not seem to substantiate the expectation that the finite quotients of the Nottingham group would provide a series of p-groups with $k(G) < c\log|G|$. Notice also that for the (not typical) prime $p=2$ there are finite 2-groups with the same order but with smaller number of conjugacy classes than certain quotients of the Nottingham group, notably of orders $2^4, 2^6, 2^7$, where our result gives 10, 22, and 23 conjugacy classes, whereas the minimum number of conjugacy classes for groups of these orders are 7, 13, and 14, respectively. (See Boston and Walker [1], where they determine this minimum for the groups of order 2^t, $t \le 14$.)

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press

In Lemma 4 we will show that every nonidentity element of the Nottingham group is conjugate to an element of the form

$$x + ax^{1+j+rp} + b_0x^{1+2j+rp} + b_1x^{1+2j+(r+1)p} + \cdots \tag{3}$$

where $a \neq 0, b_0, b_1, \ldots \in F$ are arbitrary elements, $1 \leq j \leq p, r \geq 0$. Later (see Remark 14) we show that in the natural quotient group of order p^{3p+1} or less the corresponding elements form a set of class representatives. Counting these elements will give the result. For the quotient of order p^{3p+2} this is, however, no longer true; see Example 15. Attacking the latter case would require more sophisticated calculations, hence we had to stop at the quotient of order p^{3p+1}. The numerical data suggest that the abundance of the quotient of order p^{3p+2} is $\frac{1}{2}p^2 + \frac{3}{2}p + 2$, but we haven't yet been able to verify this in general.

The methods of the present paper are elementary but involve tedious calculations. Unfortunately, they do not offer any insight.

In Section 1 we gather the basic properties of the Nottingham group. In Section 2 we show that each conjugacy class contains at least one element of the special form (3). Then we determine the order of the centralizer of each element in the quotient groups G_k for $k - 1 \leq 3p + 1$. The crucial point of the whole proof lies in Lemma 7, where the coefficient of a_2^3 in b_5 miraculously vanishes, allowing us to prove Lemma 8. Section 4 just sums up the results.

1. The Nottingham group

Let us fix a prime number p. (In some calculations we will require $p > 5$, although all results – with slightly modified proofs perhaps – are valid for $p \leq 5$ as well.) Let F be the p-element field.

Let $R = F[[x]]$ be the ring of formal power series over F. Formal power series will be denoted by lower case Greek letters:

$$\alpha = \sum_{i=0}^{\infty} a_i x^i.$$

In R we have a chain of ideals

$$I_k = \left\{ \alpha \in F[[x]] \mid \alpha = \sum_{i=k+1}^{\infty} a_i x^i \right\}.$$

Let now

$$G = \left\{ \alpha \in F[[x]] \mid \alpha = x + \sum_{i=2}^{\infty} a_i x^i \right\}.$$

Composition of elements $\alpha, \beta \in G$ is defined in the obvious way:

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press

$$\alpha \circ \beta = \beta + \sum_{i=2}^{\infty} a_i \beta^i,$$

which makes sense, since β has constant term 0. Equipped with this operation G becomes a group (see [4]), which is called the *Nottingham group* (over the p-element field). Powers in this group will be denoted by $\alpha^{(k)}$ (i.e. $\alpha^{(2)} = \alpha \circ \alpha$, etc.). We will frequently use group commutators $[\alpha, \beta] = \alpha^{(-1)} \circ \beta^{(-1)} \circ \alpha \circ \beta$. In G we have a chain of normal subgroups

$$N_k = \left\{ \alpha \in F[[x]] \mid \alpha = x + \sum_{i=k+1}^{\infty} a_i x^i \right\}.$$

We will consider the *natural quotient groups*

$$G_k = G/N_k.$$

Obviously, we have

$$|G_k| = p^{k-1}. \tag{4}$$

It is easy to verify (see [4, Lemma 1]):

$$\alpha^{(-1)} \circ \beta \in N_k \Longleftrightarrow \alpha - \beta \in I_k.$$

It follows that

$$[\alpha, \beta] \in N_k \Longleftrightarrow \alpha \circ \beta - \beta \circ \alpha \in I_k. \tag{5}$$

We shall write $\alpha = x + ax^k + \cdots$ to indicate that the coefficients of $x^2, \ldots, x^{k-1}$ are all zero ($a \in F$ is not necessarily different from zero). The basic commutator formula (see [4], (3)) says:

$$[x + ax^m + \cdots, x + bx^n + \cdots] = x + (m-n)abx^{m+n-1} + \cdots. \tag{6}$$

Hence we have

$$[N_m, N_n] \subseteq N_{m+n},$$

and even

$$[N_m, N_n] \subseteq N_{m+n+1} \quad \text{whenever} \quad m \equiv n \pmod{p}. \tag{7}$$

We shall need more detailed information about nonzero terms in commutators. For $\alpha = \sum a_i x^i \in F[[x]]$ let us define

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press

$$E(\alpha) = \{j \geq 1 \mid a_{j+1} \neq 0\}. \tag{8}$$

Lemma 1. *Let $\alpha, \beta \in G$. Then*

$$\begin{aligned} E(\alpha \circ \beta - \beta \circ \alpha) \subseteq \Bigg\{ & \sum_{\mu=1}^{M} i_\mu + \sum_{\nu=1}^{N} j_\nu \mid i_\mu \in E(\alpha), j_\nu \in E(\beta), \\ & (M = 1, N > 1) \text{ or } (M > 1, N = 1) \text{ or } (M = N = 1, i_1 \not\equiv j_1 \pmod{p})\Bigg\} \end{aligned} \tag{9}$$

Proof. Let $\alpha = x + \sum_{i \in E(\alpha)} a_{i+1} x^{i+1}$, $\beta = x + \sum_{j \in E(\beta)} b_{j+1} x^{j+1}$. Then we have

$$\begin{aligned} \alpha \circ \beta - \beta \circ \alpha = {} & x + \sum_{j \in E(\beta)} b_{j+1} x^{j+1} + \sum_{i \in E(\alpha)} a_{i+1} x^{i+1} \Bigg(1 + \sum_{j \in E(\beta)} b_{j+1} x^j\Bigg)^{i+1} \\ & - x - \sum_{i \in E(\alpha)} a_{i+1} x^{i+1} - \sum_{j \in E(\beta)} b_{j+1} x^{j+1} \Bigg(1 + \sum_{i \in E(\alpha)} a_{i+1} x^i\Bigg)^{j+1} \\ = {} & \sum_{i \in E(\alpha)} a_{i+1} x^{i+1} \Bigg(\Bigg(1 + \sum_{j \in E(\beta)} b_{j+1} x^j\Bigg)^{i+1} - 1 - (i+1) \sum_{j \in E(\beta)} b_{j+1} x^j\Bigg) \\ & - \sum_{j \in E(\beta)} b_{j+1} x^{j+1} \Bigg(\Bigg(1 + \sum_{i \in E(\alpha)} a_{i+1} x^i\Bigg)^{j+1} - 1 - (j+1) \sum_{i \in E(\alpha)} a_{i+1} x^i\Bigg) \\ & + \sum_{i \in E(\alpha)} \sum_{j \in E(\beta)} (i - j) a_{i+1} b_{j+1} x^{i+j+1}, \end{aligned} \tag{10}$$

from which the statement follows. □

In order to compute powers we shall need the following two formulae. The first one can be checked by induction easily.

Lemma 2. *Let $\alpha = x + a_m x^m + \cdots + a_n x^n + \cdots$ with $2 \leq m \leq n \leq 2m - 2$. Then for any integer k we have*

$$\alpha^{(k)} = x + k a_m x^m + \cdots + k a_n x^n + \cdots \tag{11}$$

Lemma 3. *Let $\alpha = x + x^2 + a x^3 + \cdots$. Then we have*

$$\alpha^{(p)} = x + (1 - a) x^{p+2} + \cdots. \tag{12}$$

Proof. We apply the method of I. O. York [**12**], which goes back to an insight of R. W. K. Odoni. Let the infinite triangular matrix **M** be defined by

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press

$$\begin{pmatrix} \alpha \\ \alpha^2 \\ \alpha^3 \\ \vdots \end{pmatrix} = \mathbf{M} \begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix}.$$

Then $\alpha^{(p)}$ is the first component of

$$\mathbf{M}^p \begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix}.$$

Write $\mathbf{M} = \mathbf{I} + \mathbf{N}$, where $\mathbf{I}$ is the identity matrix. Then $\mathbf{M}^p = \mathbf{I} + \mathbf{N}^p$ and $(\mathbf{N}^p)_{1d} = \sum \mathbf{N}_{1j_1}\mathbf{N}_{j_1j_2}\cdots\mathbf{N}_{j_{p-1}d}$, where the summation is taken for all $(p-1)$-tuples satisfying $1 < j_1 < j_2 < \cdots < j_{p-1} < d$. This sum is empty for $d \leq p$; hence $(\mathbf{N}^p)_{1d} = 0$ for these d. For the ith row of $\mathbf{M}$ we have $\alpha^i = x^i(1 + x + ax^2 + \cdots)^i = x^i + ix^{i+1} + (\binom{i}{2} + ia)x^{i+2} + \cdots$, so $\mathbf{N}_{i,i+1} = i$, $\mathbf{N}_{i,i+2} = \binom{i}{2} + ia$. Hence

$$(\mathbf{N}^p)_{1,p+1} = \mathbf{N}_{12}\mathbf{N}_{23}\cdots\mathbf{N}_{p,p+1} = 1 \cdot 2 \cdots p = 0,$$

and

$$\begin{aligned}(\mathbf{N}^p)_{1,p+2} &= \sum_{i=1}^{p} \mathbf{N}_{12}\cdots\mathbf{N}_{i-1,i}\mathbf{N}_{i,i+2}\mathbf{N}_{i+2,i+3}\cdots\mathbf{N}_{p+1,p+2} \\ &= \sum_{i=1}^{p} 1\cdots(i-1)\left(\binom{i}{2} + ia\right)(i+2)\cdots(p+1).\end{aligned}$$

Here all terms except the one for $i = p-1$ are equal to 0 in F, so we get

$$(\mathbf{N}^p)_{1,p+2} = (p-2)!\left(\binom{p-1}{2} + (p-1)a\right)(p+1) = 1 \cdot (1-a) \cdot 1 = 1 - a,$$

by applying Wilson's theorem. □

2. Special conjugates

Lemma 4. *Every element $x + ax^{1+j+rp} + \cdots$ with $a \neq 0$, $1 \leq j \leq p$, $r \geq 0$ is conjugate to (at least one) element of the form*

$$x + ax^{1+j+rp} + \sum_{\nu=0}^{\infty} b_\nu x^{1+2j+(r+\nu)p}. \tag{13}$$

Proof. Let $\alpha = x + ax^{1+j+rp} + x^{2+j+rp}\alpha'$ be given. We want to find a $\beta = x + ax^{1+j+rp} + \sum_{\nu=0}^{\infty} b_\nu x^{1+2j+(r+\nu)p}$ and a $\gamma = x + \sum_{\sigma=2}^{\infty} c_\sigma x^\sigma$ such that $\gamma^{(-1)} \circ \beta \circ \gamma = \alpha$, i.e. $\beta \circ \gamma = \gamma \circ \alpha$ holds. Now we have

$$\begin{aligned}\beta \circ \gamma - \gamma \circ \alpha = x &+ \sum_{\sigma=2}^{\infty} c_\sigma x^\sigma \\ &+ a\left(x + \sum_{\sigma=2}^{\infty} c_\sigma x^\sigma\right)^{1+j+rp} + \sum_{\nu=0}^{\infty} b_\nu \left(x + \sum_{\sigma=2}^{\infty} c_\sigma x^\sigma\right)^{1+2j+(r+\nu)p} \\ &- x - ax^{1+j+rp} - x^{2+j+rp}\alpha' - \sum_{\sigma=2}^{\infty} c_\sigma \alpha^\sigma \\ &= \sum_{\sigma=2}^{\infty} c_\sigma (x^\sigma - \alpha^\sigma) + a\left(\left(x + \sum_{\sigma=2}^{\infty} c_\sigma x^\sigma\right)^{1+j+rp} - x^{1+j+rp}\right) \\ &+ \sum_{\nu=0}^{\infty} b_\nu \left(x + \sum_{\sigma=2}^{\infty} c_\sigma x^\sigma\right)^{1+2j+(r+\nu)p} - x^{2+j+rp}\alpha'.\end{aligned} \tag{14}$$

Up to degree $1 + j + rp$ we have the terms

$$\sum_{\sigma=2}^{\infty} c_\sigma (x^\sigma - x^\sigma) + a(x^{1+j+rp} - x^{1+j+rp}) = 0.$$

The terms in (14) involving c_σ and having degree $\leq j + rp + \sigma$ are

$$c_\sigma(x^\sigma - x^\sigma - \sigma x^{\sigma-1} a x^{1+j+rp}) + a(1 + j + rp)x^{j+rp} c_\sigma x^\sigma = c_\sigma a(-\sigma + 1 + j)x^{j+rp+\sigma}.$$

The lowest degree term in (14) involving b_ν is $b_\nu x^{1+2j+(r+\nu)p}$. We can choose the c_σ's with $\sigma \equiv j + 1 \pmod{p}$ arbitrarily. Then for each $\sigma = 2, 3, \ldots$ we can find recurrently either an appropriate c_σ (for $\sigma \not\equiv j + 1 \pmod{p}$) or a b_ν ($\nu = (\sigma - j - 1)/p$ for $\sigma \equiv j + 1 \pmod{p}$) which equates the coefficient of $x^{j+rp+\sigma}$ in (14) with 0. □

3. Centralizers

We will use the notation

$$U_j = \left\{\alpha \in G \mid \alpha = x + x^{j+1} + \sum_{i=j+2}^{\infty} a_i x^i\right\}.$$

Using the following lemma we will be able to determine the coefficients in some centralizing elements successively.

Lemma 5. *Let $\alpha \in U_i, \beta \in G$ with $[\alpha, \beta] \in N_k$. If $k \not\equiv 2i$ (mod p) then there exists a $b \in F$ such that for $\beta' = \beta + bx^{k-i+1}$ we have $[\alpha, \beta'] \in N_{k+1}$.*

Proof. Let $\alpha = x + x^{i+1} + \cdots, \alpha \circ \beta - \beta \circ \alpha = cx^{k+1} + \cdots$. Take $b \in F$ with $(k-2i).b = c$, and let $\beta' = \beta + bx^{k-i+1}$. Then calculating modulo I_{k+1} we obtain

$$\begin{aligned}\alpha \circ \beta' - \beta' \circ \alpha &= \alpha \circ (\beta + bx^{k-i+1}) - \beta \circ \alpha - b\alpha^{k-i+1}\\ &\equiv \alpha \circ \beta + bx^{k-i+1} + (i+1)\beta^i bx^{k-i+1} - \beta \circ \alpha - b(x^{k-i+1} + (k-i+1)x^{k+1})\\ &\equiv cx^{k+1} + (i+1-k+i-1)bx^{k+1} = 0.\end{aligned}$$

Hence $[\alpha, \beta'] \in N_{k+1}$. □

Proposition 6. *Let $1 \le j < p, r \ge 0, s \ge 0, m = \min(r, s)$. Then for every $\alpha \in U_{j+rp}$ there exists a $\beta \in U_{j+sp}$ such that $[\alpha, \beta] \in N_{(p+2)j+(r+s+m)p}$.*

Proof. In virtue of Lemma 4 we may assume without loss of generality that

$$\alpha = x + x^{1+j+rp} + \sum_{\mu=r}^{\infty} a_\mu x^{1+2j+\mu p}.$$

We will find an appropriate β of the form

$$\beta = x + x^{1+j+sp} + \sum_{\nu=s}^{\infty} b_{1+2j+\nu p} x^{1+2j+\nu p} + \sum_{\xi=3}^{p} \sum_{\nu=s+m}^{\infty} b_{1+\xi j+\nu p} x^{1+\xi j+\nu p}.$$

By (5) we have to find a β with $\alpha \circ \beta - \beta \circ \alpha \in I_{(p+2)j+(r+s+m)p}$. Now

$$E(\alpha) \subseteq \{j + rp\} \bigcup \{2j + \mu p \mid \mu \ge r\},$$

$$E(\beta) \subseteq \{j + sp\} \bigcup \{2j + \nu p \mid \nu \ge s\} \bigcup \{\xi j + \nu p \mid 3 \le \xi \le p, \nu \ge s + m\}.$$

Hence Lemma 1 yields that

$$E(\alpha \circ \beta - \beta \circ \alpha) \subseteq \{3j+\sigma p \mid \sigma \ge r + s\} \bigcup \{\rho j + \sigma p \mid 4 \le \rho \le p + 1, \sigma \ge r + s + m\}$$

$$\bigcup \{k \mid k \ge (p+2)j + (r+s+m)p\}.$$

No element $k \in E(\alpha \circ \beta - \beta \circ \alpha)$, $k < (p+2)j + (r+s+m)p$ is congruent to $2j$ modulo p, and for each such k we have a term of degree $k - (j + rp) + 1$ in β, hence by repeated use of Lemma 5 we can find recurrently suitable coefficients for β such that $\alpha \circ \beta - \beta \circ \alpha \in I_{(p+2)j+(r+s+m)p}$ will hold. □

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press

The most difficult task is to find elements centralizing an $\alpha \in U_1$. The following two lemmas are crucial in proving our main result.

Lemma 7. *There is a bijection $\Psi : F^{p-1} \to F^{p-1}$ such that $\alpha = x + x^2 + a_2x^3 + \cdots + a_px^{p+1} + \cdots$ and $\beta = x + x^{p+2} + b_2x^{p+3} + \cdots + b_px^{2p+1} + \cdots$ commute modulo N_{2p+2} if and only if $(b_2, \ldots, b_p) = \Psi(a_2, \ldots, a_p)$. Furthermore, if in $(b_2, \ldots, b_p) = \Psi(a_2, \ldots, a_p)$ each b_i $(i = 2, \ldots, p)$ is written as a polynomial in $a_2, \ldots, a_p$ then the degree of this polynomial in a_2 is at most 1 for $i = 2, 3$; at most 2 for $i = 4, 5$; and at most $i - 3$ for $6 \le i \le p$.*

Proof. Given $\alpha \in U_1$, the existence of a suitable $\beta \in U_{p+1}$ is guaranteed by Proposition 6 (with $j = 1, r = 0, s = 1$). To show the uniqueness, assume that there is another $(p-1)$-tuple $(b'_2, \ldots, b'_p) \neq (b_2, \ldots, b_p)$ such that $\beta' = x + x^{p+2} + b'_2x^{p+3} + \cdots + b'_px^{2p+1}$ centralizes α modulo N_{2p+2} as well. Then modulo N_{2p+2}, α commutes with $\gamma = \beta^{(-1)} \circ \beta' = x + cx^j + \cdots$, where $c \neq 0, p+3 \le j \le 2p+1$. Now (6) yields $[\alpha, \gamma] = x + (2-j)cx^{j+1} + \cdots \notin N_{2p+2}$, a contradiction. So the mapping Ψ is well-defined. Proposition 6 (with $j = 1, r = 1, s = 0$) also implies that Ψ is surjective, hence by finiteness it is injective as well.

Now we want to determine some b_i explicitly. Write $a_1 = 1, b_1 = 1$. Direct calculation modulo I_{2p+2} yields (cf. (10)):

$$\begin{aligned}
\alpha \circ \beta - \beta \circ \alpha &\equiv \sum_{\mu=1}^{p} \sum_{\nu=1}^{p} (\mu - p - \nu) a_\mu b_\nu x^{\mu+p+\nu+1} \\
&\quad - \sum_{\nu=1}^{p} b_\nu x^{p+\nu+1} \left(\left(1 + \sum_{\mu=1}^{p} a_\mu x^\mu\right)^{p+\nu+1} - 1 - (p+\nu+1) \sum_{\mu=1}^{p} a_\mu x^\mu \right) \\
&\equiv \sum_{\mu=1}^{p} \sum_{\nu=1}^{p} (\mu - \nu) a_\mu b_\nu x^{\mu+p+\nu+1} \\
&\quad - \sum_{\nu=1}^{p} b_\nu x^{p+\nu+1} \left(\left(1 + \sum_{\mu=1}^{p} a_\mu x^\mu\right)^{\nu+1} + x^p - 1 - (\nu+1) \sum_{\mu=1}^{p} a_\mu x^\mu \right) \\
&= (a_2 - b_2)x^{p+4} + (2a_3 - 2b_3)x^{p+5} + (3a_4 + a_3b_2 - a_2b_3 - 3b_4)x^{p+6} \\
&\quad + (4a_5 + 2a_4b_2 - 2a_2b_4 - 4b_5)x^{p+7} + \cdots \\
&\quad - x^{p+2}(x^2 + 2a_2x^3 + (2a_3 + a_2^2)x^4 + (2a_4 + 2a_2a_3)x^5 + \cdots) \\
&\quad - b_2x^{p+3}(3x^2 + (6a_2 + 1)x^3 + (6a_3 + 3a_2^2 + 3a_2)x^4 + \cdots) \\
&\quad - b_3x^{p+4}(6x^2 + (12a_2 + 4)x^3 + \cdots) - b_4x^{p+5}(10x^2 + \cdots) - \cdots \\
&= (a_2 - b_2 - 1)x^{p+4} + (2a_3 - 2b_3 - 2a_2 - 3b_2)x^{p+5} \\
&\quad + (3a_4 + a_3b_2 - a_2b_3 - 3b_4 - 2a_3 - a_2^2 - b_2(6a_2 + 1) - 6b_3)x^{p+6} \\
&\quad + (4a_5 + 2a_4b_2 - 2a_2b_4 - 4b_5 - 2a_4 - 2a_2a_3 - b_2(6a_3 + 3a_2^2 + 3a_2) \\
&\quad - b_3(12a_2 + 4) - 10b_4)x^{p+7} + \cdots,
\end{aligned} \tag{15}$$

assuming $p > 5$.

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press

By equating the coefficients with 0 we obtain

$$b_2 = a_2 - 1$$

$$b_3 = -\frac{5}{2}a_2 + a_3 + \frac{3}{2}$$

$$b_4 = -\frac{3}{2}a_2^2 + \frac{37}{6}a_2 + a_4 - 3a_3 - \frac{8}{3}$$

$$b_5 = \frac{49}{6}a_2^2 + \left(-\frac{7}{2}a_3 - \frac{46}{3}\right)a_2 + a_5 - \frac{7}{2}a_4 + 8a_3 + \frac{31}{6},$$

where in b_5 the coefficient of a_2^3 vanishes. (For $p \le 5$ we have to add 1 to the given formula for b_p due to the term $-b_1x^{p+2} \cdot x^p$ in (15).) Now for $i = 6, \ldots, p$ we can show by induction that the degree of b_i in a_2 is at most $i - 3$. Indeed, the coefficient of x^{p+2+i} in (15) is a polynomial in $a_2, \ldots, a_i, b_2, \ldots, b_i$, more precisely all terms are linear in the b_ν's and the degree in a_2 of the coefficient of b_ν is $[(i+1-\nu)/2]$, hence the estimate for the degree follows by induction. □

Lemma 8. *Let* $\alpha = x + x^2 + a_2x^3 + \cdots + a_px^{p+1} + \cdots$ *and* $\beta = x + x^{p+2} + b_2x^{p+3} + \cdots + b_px^{2p+1} + \cdots$ *with* $(b_2, \ldots, b_p) = \Psi(a_2, \ldots, a_p)$. *Then* $[\alpha, \beta] \in N_{2p+3}$.

Proof. We know by Lemma 7 that $[\alpha, \beta] \in N_{2p+2}$, hence $\alpha \circ \beta - \beta \circ \alpha = x + cx^{2p+3} + \cdots$, where c is a polynomial in $a_2, \ldots, a_p, b_2, \ldots, b_p$, hence in $a_2, \ldots, a_p$. (Observe that c does not depend on the further coefficients of α or β by (10).) As in the proof of Lemma 7 it follows that the degree of this polynomial in a_2 is at most $p-2$. We have to show that this polynomial is in fact zero.

Let first $a_2 \ne 1$ and take a positive integer k with $k(1-a_2) = 1$. Then using (12) and (11) we get that the pkth power of α has the form

$$\alpha^{(pk)} = (\alpha^{(p)})^{(k)} = (x + (1-a_2)x^{p+2} + \cdots)^{(k)} = x + k(1-a_2)x^{p+2} + \cdots = x + x^{p+2} + \cdots.$$

Since $\alpha^{(pk)}$ commutes with α, we must have by the uniqueness stated in Lemma 7 that

$$\alpha^{(pk)} = x + x^{p+2} + b_2x^{p+3} + \cdots + b_px^{2p+1} + \cdots.$$

Hence β centralizes α modulo N_{2p+3} in this case. This means that the value of the polynomial c is 0 whenever $a_2 \ne 1$. Since the degree of c in a_2 is at most $p-2$, it implies that $c = 0$ identically. □

Now we can summarize our results on the existence of centralizing elements.

Proposition 9. *Let* $1 \leq u, v \leq 3p+1$ *with* $u \equiv v \pmod{p}$. *Then for every* $\alpha \in U_u$ *there exists a* $\beta \in U_v$ *such that* $[\alpha, \beta] \in N_{3p+2}$.

Proof. Let $u = j + rp, v = j + sp$ with $1 \leq j \leq p, r, s \geq 0$ and set $m = \min(r, s)$. If $u = v$ then we can take $\beta = \alpha$, so assume $u \neq v$.

If $j \neq p$, then Proposition 6 can be applied to obtain a β that commutes with α modulo $N_{(p+2)j+(r+s+m)p}$. Now for $j \geq 2$ we have

$$(p+2)j + (r+s+m)p \geq 2(p+2) + p > 3p+2,$$

so the result follows in this case. If $j = 1$ then

$$(p+2)j + (r+s+m)p = (r+s+m+1)p + 2,$$

hence we get the result unless $r+s+m+1 \leq 2$, that is $m = \min(r, s) = 0$ and $\max(r, s) = 1$. So we have to consider the cases $(u, v) = (1, p+1)$ and $(u, v) = (p+1, 1)$. Let $u = 1, v = p+1$, then $\alpha = x + x^2 + a_2x^3 + \cdots$. Choose $\beta' = x + x^{p+2} + b_2x^{p+3} + \cdots + b_px^{2p+1}$ with $(b_2, \ldots, b_p) = \Psi(a_2, \ldots, a_p)$ (see Lemma 7). Then $[\alpha, \beta'] \in N_{2p+3}$ by Lemma 8. Repeated application of Lemma 5 yields then a $\beta \in U_{p+1}$ such that $[\alpha, \beta] \in N_{3p+2}$. We can proceed similarly for $(u, v) = (p+1, 1)$, $\alpha = x + x^{p+2} + a_2x^{p+3} + \cdots$ by taking $\beta' = x + x^2 + b_2x^3 + \cdots + b_px^{p+1}$ with $(b_2, \ldots, b_p) = \Psi^{-1}(a_2, \ldots, a_p)$ and finishing the proof as above.

Finally consider the case $j = p$. Then Lemma 4 allows us to assume without loss of generality that $\alpha = x + \sum_{\mu=r+1}^{\infty} a_\mu x^{\mu p+1}$. We show that $[\alpha, \beta] \in N_{(r+s+m+3)p}$ for every β of the form $\beta = x + \sum_{\nu=s+1}^{\infty} b_\nu x^{\nu p+1}$. Indeed, by Lemma 1 we have

$$E(\alpha \circ \beta - \beta \circ \alpha) \subseteq \left\{ \left(\sum_{\mu=1}^{M} i_\mu + \sum_{\nu=1}^{N} j_\nu \right) p \mid i_\mu p \in E(\alpha), j_\nu p \in E(\beta), M + N > 2 \right\},$$

where each element is at least

$$(r+1+s+1+m+1)p \geq 4p \geq 3p+2. \qquad \square$$

An obvious "Gaussian elimination" easily yields the following observation.

Lemma 10. *Let* H/N_k *be a subgroup of* G/N_k. *Then* $|H/N_k| = p^\mu$, *where* μ *stands for the number of indices* j, $1 \leq j \leq k-1$, *such that* $H \cap U_j \neq \emptyset$.

Lemma 11. *Let* i *and* n *be natural numbers. Then the number of those integers* j *for which* $j \equiv i \pmod{p}$ *and* $1 \leq j \leq n$ *is*

$$\left[\frac{n-i}{p}\right] - \left[\frac{-i}{p}\right]. \tag{16}$$

Proof. We have to count those j's for which $1-i \le j-i \le n-i$ holds and $j-i$ is divisible by p. Their number is clearly the one given by (16). □

Proposition 12. *Let* $1 \le i < k \le 3p+2$ *and* $\alpha \in N_i \setminus N_{i+1}$. *Then we have*

$$|C_{G/N_k}(\alpha N_k)| = p^{i+[(k-2i-1)/p]-[-i/p]}. \tag{17}$$

Proof. Let $\alpha = x + ax^{i+1} + \cdots$ with $a \neq 0$, and take an integer m with $ma = 1$ in F. Then α and $\alpha^{(m)}$ generate the same cyclic subgroup and (11) yields $\alpha^{(m)} = x + max^{i+1} + \cdots = x + x^{i+1} + \cdots \in U_i$, so we may (and will) assume without loss of generality that $\alpha \in U_i$. In virtue of Lemma 10 we have to count those j's $(1 \le j \le k-1)$ for which there is a $\beta \in U_j$ with $[\alpha, \beta] \in N_k$. Now (6) gives $[\alpha, \beta] = x + (i-j)x^{i+j+1} + \cdots$. Hence if $[\alpha, \beta] \in N_k$ then either $i \equiv j \pmod p$ or $i + j \ge k$ holds. Conversely, if $i \equiv j \pmod p$ then there is a suitable $\beta \in U_j$ by Proposition 9; if $i + j \ge k$ then $[\alpha, \beta] \in N_k$ for every $\beta \in U_j$. Hence the set of the j's in question is

$$\{j \mid 1 \le j \le k-i-1, j \equiv i \pmod p\} \cup \{k-i, \ldots, k-1\}.$$

Lemma 11 then yields (17). □

4. The class number

First we count the number of conjugacy classes in different "layers" of the natural quotients $G_k = G/N_k$, $k \le 3p+2$.

Proposition 13. *Let* $1 \le i < k \le 3p+2$. *Then* $N_i/N_k \setminus N_{i+1}/N_k$ *splits into*

$$(p-1)p^{[(k-2i-1)/p]-[-i/p]}$$

conjugacy classes in $G_k = G/N_k$.

Proof. Let $S = N_i/N_k \setminus N_{i+1}/N_k$, then we have $|S| = (p-1)p^{k-i-1}$. By Proposition 12 each element in S has centralizer of the same order; hence each conjugacy class contained in S has the same size

$$p^{k-1-i-[(k-2i-1)/p]-[-i/p]},$$

from which the statement follows. □

Remark 14. *If* $k \le 3p+2$ *then every conjugacy class of* G_k *contains exactly one element* αN_k, *where* α *has the special form (13).*

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press

Proof. Let $i=j+rp<k$ with $1 \leq j \leq p$, $r \geq 0$. Then the number of special elements (modulo N_k) in $N_i \setminus N_{i+1}$ is

$$(p-1)p^{[(k-2j-1)/p]-r+1}, \tag{18}$$

since we have to choose a nonzero coefficient for x^{i+1} and arbitrary ones for $x^{1+2j+(r+v)p}$ for each v such that $0 \leq v$ and $1+2j+(r+v)p \leq k$. Every conjugacy class contains at least one such element by Lemma 4. On the other hand, the number of conjugacy classes as given by Proposition 13 is

$$(p-1)p^{[(k-2i-1)/p]-[-i/p]}=(p-1)p^{[(k-2j-1)/p]-2r-[-j/p]+r},$$

the same as in (18), since $[-j/p]=-1$ as $-p \leq -j \leq -1$. □

However, the preceding statement is no longer true for $k=3p+3$.

Example 15. *The elements $\alpha=x+x^2$ and $\beta=x+x^2+x^{3p+3}$ (both of the form (13)) are conjugate in G_{3p+3}.*

Proof. We will find an element $\gamma=x+\sum_{i=0}^{p-1} c_i x^{2p+2+i}$ such that $(\gamma^{(-1)} \circ \beta \circ \gamma)N_{3p+3}=\alpha N_{3p+3}$, i.e. $\beta \circ \gamma-\gamma \circ \alpha \in I_{3p+3}$. Calculating modulo I_{3p+3} we obtain

$$\begin{aligned}\beta \circ \gamma-\gamma \circ \alpha &\equiv x+\sum_{i=0}^{p-1} c_i x^{2p+2+i}+x^2+2\sum_{i=0}^{p-1} c_i x^{2p+3+i}+x^{3p+3}\\ &\quad -x-x^2-\sum_{i=0}^{p-1} c_i(x+x^2)^{2p+2+i}\\ &=x^{3p+3}+\sum_{i=0}^{p-1} c_i(x^{2p+2+i}+2x^{2p+3+i}-(x+x^2)^{2p+2+i}).\end{aligned}$$

Here the coefficients of $x,\ldots,x^{2p+3}$ are all zero, and we get a system of linear equations for $c_0,\ldots,c_{p-1}$ by equating the coefficients of $x^{2p+4},\ldots,x^{3p+3}$ with zero. It can be checked that the determinant of the system is nonzero, hence there does exist an appropriate γ. For the sake of simplicity we give the suitable conjugating element only for the case $p=3$, when we obtain $\gamma=x+x^8+2x^9+2x^{10}$. □

Now we can give the proof of our main result.

Proof of the Theorem. We consider the quotient group G_{t+1} of order p^t (see (4)), where $t \leq 3p+1$. Proposition 13 yields that

$$\begin{aligned}k(G_{t+1}) &= 1+\sum_{i=1}^{t}(p-1)p^{[(t-2i)/p]-[-i/p]}\\ &= 1+\sum_{j=1}^{p}(p-1)\sum_{\substack{r\ge 0\\ j+rp\le t}}p^{[(t-2j)/p]-r+1}\\ &= 1+\sum_{j=1}^{p}\left(p^{[(t-2j)/p]+2}-p^{[(t-2j)/p]-[(t-j)/p]+1}\right)\\ &= \sum_{j=1}^{p}p^{[(t-2j)/p]+2}+\left(1-\sum_{j=1}^{p}p^{[(t-2j)/p]-[(t-j)/p]+1}\right).\end{aligned}\tag{19}$$

For odd p the term in parenthesis does not depend on t; its value is always $\frac{1}{2}(1-p^2)$. If $p=2$ then this term is -2 for even t and -1 for odd t.

Let a_t denote the abundance of G_{t+1}. For $t=1,2$ the group G_{t+1} is abelian of order p^t, hence it has abundance 0. Now for $3\le t+2\le 3p+1$ we compare a_{t+2} and a_t. Let $t=2n+e$ with $n\ge 0$, $e\in\{0,1\}$. Then by definition (see (1)) we have

$$\begin{aligned}k(G_{t+3}) &= (p^2-1)(n+1)+p^e+(p^2-1)(p-1)a_{t+2},\\ k(G_{t+1}) &= (p^2-1)n+p^e+(p^2-1)(p-1)a_t,\end{aligned}$$

hence

$$k(G_{t+3})-k(G_{t+1}) = p^2-1+(p^2-1)(p-1)(a_{t+2}-a_t).\tag{20}$$

At the same time we infer from (19) that

$$\begin{aligned}k(G_{t+3})-k(G_{t+1}) &= \sum_{j=1}^{p}p^{[(t+2-2j)/p]+2}-\sum_{j=1}^{p}p^{[(t-2j)/p]+2}\\ &= p^{[t/p]+2}-p^{[t/p]}=(p^2-1)p^{[t/p]}.\end{aligned}\tag{21}$$

Now (20) and (21) together yield

$$a_{t+2}=a_t+\frac{p^{[t/p]}-1}{p-1}=\begin{cases}a_t, & \text{if } t<p;\\ a_t+1, & \text{if } p\le t<2p;\\ a_t+p+1, & \text{if } 2p\le t<3p,\end{cases}$$

in accordance with (2). □

Since the same calculation gives the number of elements of the form (13) for any t, in virtue of Lemma 4 we obtain an upper bound for the number of conjugacy classes.

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press

Corollary 16. *The number of conjugacy classes of G_{t+1} $(t \geq 1)$ satisfies*

$$k(G_{t+1}) \leq \sum_{i=0}^{p-1} p^{\lceil (t+2i)/p \rceil} - \frac{1}{2}(p^2 - 1) \tag{22}$$

for p odd; and

$$k(G_{t+1}) \leq 3 \cdot 2^{\lceil t/2 \rceil} - \begin{cases} 2, & \textit{if } t \textit{ is even;} \\ 1, & \textit{if } t \textit{ is odd,} \end{cases} \tag{23}$$

for $p = 2$. Equality holds if and only if $t \leq 3p + 1$.

For the order of magnitude of this upper bound we have the following.

Corollary 17. *There is a constant C_p such that for all $t \geq 1$ we have*

$$k(G_{t+1}) < C_p \cdot |G_{t+1}|^{1/p}.$$

Proof. Since $|G_{t+1}| = p^t$ we can choose $C_2 = 3$ and $C_p = p^3$ (or an even smaller constant) for $p > 2$ to get an upper estimate of the form $C_p p^{t/p}$ for the right hand sides of (22) and (23). □

Acknowledgements. I am greatly indebted to Andrea Caranti and Levente Lévai for providing me their data which made this work possible. The usefulness of the GAP system is also gratefully acknowledged. I am also thankful for Levente Lévai and László Pyber for their valuable comments.

REFERENCES

1. N. Boston and J. L. Walker, Two-groups with few conjugacy classes, to appear.

2. G. A. Fernández-Alcober and R. Shepherd, *On the order of p-groups of abundance zero*, *J. Algebra*, to appear.

3. B. Huppert, *Endliche Gruppen I*, (Springer-Verlag, Berlin–Heidelberg–New York, 1967).

4. D. L. Johnson, The group of formal power series under substitution, *J. Austral. Math. Soc.* Ser. A **45** (1988), 296–302.

5. J. Poland, Two problems on finite groups with k conjugate classes, *J. Austral. Math. Soc.* Ser. A **8** (1968), 49–55.

6. L. Pyber, Finite groups have many conjugacy classes, *J. London Math. Soc.* (2) **46** (1992), 239–249.

7. B. Rothe, *Konjugiertenklassen in Gruppen von Primzahlpotenzordnung*, (Diplomarbeit, RWTH Aachen, 1993).

8. J. SANGRONIZ, *Conjugacy classes and characters in some quotients of the Nottingham group*, (Universidad del Pais Vasco, Bilbao, 1996), preprint.

9. M. SCHÖNERT et al., *GAP – Groups, Algorithms, and Programming*, (Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, fifth edition, 1995).

10. A. SHALEV, Finite p-groups, in *Finite and Locally Finite Groups* (B. Hartley et al. eds., NATO ASI Series **471**, 1995), 401–450.

11. I. O. YORK, *The group of formal power series under substitution*, (Ph.D. thesis, Nottingham, 1990).

12. I. O. YORK, The exponent of certain finite p-groups, *Proc. Edinburgh Math. Soc.* **33** (1990), 483–490.

MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST, P.O. BOX 127
H-1364, HUNGARY
E-mail address; ppp@math-inst.hu

https://doi.org/10.1017/S0013091500019714 Published online by Cambridge University Press