PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 9, September 1998, Pages 2513–2523
S 0002-9939(98)04440-2

A BOUND FOR THE DERIVED AND FRATTINI SUBGROUPS OF A PRIME-POWER GROUP

GRAHAM ELLIS

(Communicated by Ronald M. Solomon)

ABSTRACT. This paper is based on the seemingly new observation that the Schur multiplier $M(G)$ of a d-generator group of prime-power order p^n has order $|M(G)| \leq p^{d(2n-d-1)/2}$. We prove several related results, including sufficient conditions for a sharper bound on $|M(G)|$ to be an equality.

Let G be a group with centre Z. Schur [13] observed that the commutator subgroup $[G,G]$ is finite whenever the quotient G/Z is finite. Wiegold [17] obtained an estimate for the order of $[G,G]$ in terms of the order of G/Z; in particular he showed that if G/Z has prime-power order p^n, then the order of $[G,G]$ is at most $p^{n(n-1)/2}$. This bound can be attained for all $n \geq 1$, but only if G/Z is elementary abelian. As a corollary, Wiegold re-derived Green's bound [7] on the order of the Schur multiplier of a prime-power group. Gaschütz, Neubüser and Yen [6] subsequently refined Wiegold's methods to obtain a sharper bound on $[G,G]$ (involving the number of generators of the quotient of G by its second centre), and a corresponding sharpening of Green's bound. By a different fine tuning of Wiegold's methods, Jones ([9], [10], [11]) obtained complementary improvements in Green's bound.

In this article we reduce the above bounds on $[G,G]$ by incorporating, in turn: (1) the number of generators of G/Z; (2) the abelian group structure of the quotients of the lower central series of G/Z; (3) the restricted Lie algebra structure of the quotients of the lower p-central series of G/Z; (4) the "breadth in G" of the preimages of the generators of G/Z. The fourth approach (which is the only one to involve more than the structure of G/Z) complements a result of Vaughan-Lee [16]. We obtain corresponding reductions in the above-mentioned bounds on the Schur multiplier. As an application we obtain a rough upper bound on the number of d-generator groups of order p^n. Furthermore, our results are presented in such a way as to yield bounds on the Frattini subgroup of a prime-power group.

Let p be any prime, and let $q \geq 0$ be any nonnegative integer multiple of p. (We are interested mainly in the cases $q = 0$ and $q = p$.) Given a group G we let $Z^q(G)$ denote the subgroup of the centre of G consisting of those elements with order dividing q. Given a normal subgroup N in G, we let $N\#^qG$ denote the subgroup of G generated by the commutators $ngn^{-1}g^{-1}$ and powers n^q for $n \in N$, $g \in G$.

Received by the editors January 27, 1997.
1991 *Mathematics Subject Classification.* Primary 20J05.

We define

$$\begin{aligned}
&\gamma_1^q G = G,\\
&\gamma_{i+1}^q G = (\gamma_i^q G)\#^q G, \qquad i \geq 1,\\
&\Gamma_i^q G = \gamma_i^q G/\gamma_{i+1}^q G, \qquad i \geq 1.
\end{aligned}$$

Furthermore, we set

$$\begin{aligned}
&M^q(G) = H_2(G, \mathbb{Z}_q),\\
&H_n^q(G) = H_n(G, \mathbb{Z}_q),\\
&R(G,q) = \begin{cases} 0 & \text{if } q = 0,\\ |\Gamma_1^0 G|/|\gamma_2^q(M^0(G))| & \text{if } q \geq p, \end{cases}
\end{aligned}$$

where $H_n(G, \mathbb{Z}_q)$ is the n-th homology group of G with coefficients in the abelian group $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$. Thus $Z^0 G$ is the centre of G, $\gamma_1^0 G \leq \gamma_2^0 G \leq \cdots$ is the lower central series of G, and when G is finite $M^0(G)$ is the Schur multiplier of G. If G is a finite p-group, then $\gamma_2^p G$ is its Frattini subgroup, and $\Gamma_i^p G$ is an elementary abelian group for $i \geq 1$. We say that a group is a "d-generator group" if it can be generated by d elements, and by no fewer than d elements.

Theorem 1. *Let G be any group such that $Q = G/Z^q(G)$ is a d-generator group of order p^n. Then*:

(i) $|\gamma_2^q G| \leq p^{(d(2n-d-1)/2)+R(Q,q)}$.

(ii) *There exists a group $\widehat{G}$ with $\widehat{G}/Z^q(\widehat{G}) \cong Q$ and $|\gamma_2^q \widehat{G}| = p^{(d(2n-d-1)/2)+R(Q,q)}$ if and only if the canonical homomorphism $H_3^0(Q) \to H_3^0(Q/\gamma_i^p Q)$ is surjective for each $i \geq 1$.*

(iii) *If $d = n \geq 2$, or if $d = n - 1 = 2$, then there exists a group $\widehat{G}$ with $\widehat{G}/Z^q(\widehat{G})$ a d-generator group of order p^n, and such that $|\gamma_2^q \widehat{G}| = p^{(d(2n-d-1)/2)+R(Q,q)}$.*

Note that $p^{d(2n-d-1)/2} \leq p^{n(n-1)/2}$ for all integers $1 \leq d \leq n$. Thus Wiegold's bound [17, Theorem 2.1] on the commutator subgroup $\gamma_2^0 G$ follows from Theorem 1.

Note that part (iii) of Theorem 1 does not extend to $d = n - 2 = 2$. Consider, for instance, the values $p = 2$, $q = 0$, $n = 4$, $d = 2$ and consider any group G with $G/Z^0(G)$ a 2-generator group of order p^4. Arguments involving the Schur multiplier (see [2]) establish the existence of such a G, and show that the only possibilities for the commutator subgroup are $\gamma_2^0 G \cong C_2 \times C_2$, $\gamma_2^0 G \cong C_2 \times C_4$ and $\gamma_2^0 G \cong C_2 \times C_2 \times C_4$; in all cases $|\gamma_2^0 G|$ is strictly less than $p^{d(2n-d-1)/2} = 32$.

The next result is a variant on Theorem 1 which incorporates the structure of the abelian groups $(Q/Z^0(Q))^{\mathrm{ab}}$ and $\Gamma_i^0(Q)$ for $i \geq 1$.

Theorem 2. *Let G be any group with $|G/Z^q(G)| = p^n$. Set $Q = G/Z^q(G)$ and $\overline{Q} = Q/Z^0(Q)$, and suppose that*

$$\begin{aligned}
&\Gamma_1^0 \overline{Q} \cong C_{p^{m'_{11}}} \times C_{p^{m'_{12}}} \times \cdots \times C_{p^{m'_{1r}}},\\
&\Gamma_i^0 Q \cong C_{p^{m_{i1}}} \times C_{p^{m_{i2}}} \times \cdots \times C_{p^{m_{ir}}}
\end{aligned}$$

for $i \geq 1$. (Here r is independent of i and $m_{ij} \geq 0$.) Set

$$M = \sum_{1 \leq j < k \leq r} \text{minimum}(m_{1j}, m_{1k}) + \sum_{\substack{2 \leq i \leq r\\ 1 \leq j,\, k \leq r}} \text{minimum}(m_{ij}, m'_{1k}).$$

Then

(i) $|\gamma_2^q G| \le p^{M+R(Q,q)}$.

(ii) *There exists a group* $\widehat{G}$ *with* $\widehat{G}/Z^q(\widehat{G}) \cong Q$ *and* $|\gamma_2^q \widehat{G}| = p^{M+R(Q,q)}$ *if the canonical homomorphism* $H_3^0(Q) \to H_3^0(Q/\gamma_i^0 Q)$ *is surjective for each* $i \ge 1$.

This theorem improves slightly on a bound of Gaschütz, Neubüser and Yen [6]. They proved that if $Q = G/Z^0(G)$ is a prime-power group whose central quotient $Q/Z^0(Q)$ is generated by d elements, then

$$|[G,G]| \le |M^0(Q^{\mathrm{ab}})|\,|[Q,Q]|^d.$$

To see the improvement, note that $M^0(Q^{\mathrm{ab}})$ is just the exterior square $Q^{\mathrm{ab}} \wedge Q^{\mathrm{ab}}$ and hence that

$$\log_p |M^0(Q^{\mathrm{ab}})| = \sum_{1\le j<k\le r} \mathrm{minimum}(m_{1j}, m_{1k}).$$

Furthermore, if Q is nilpotent of class c say, then equality (4) below (which involves the tensor product of abelian groups) yields

$$\begin{aligned}\log_p |[Q,Q]|^d &= \log_p |\Gamma_2^0 Q \oplus \cdots \oplus \Gamma_c^0 Q|^d \\ &\ge \log_p |(\Gamma_2^0 Q \oplus \cdots \oplus \Gamma_c^0 Q) \otimes \Gamma_1^0 \overline{Q}| \\ &= \sum_{\substack{2\le i\le r \\ 1\le j,\, k\le r}} \mathrm{minimum}(m_{ij}, m'_{1k}).\end{aligned}$$

The last inequality is strict precisely when the exponent of $\Gamma_2^0 Q \oplus \cdots \oplus \Gamma_c^0 Q$ is greater than the order of at least one of the d generators of $\Gamma_1^0 \overline{Q} = Q/[Q,Q]Z^0(Q)$; in this case the bound in Theorem 2 is lower than the bound of [6].

To illustrate the above results set $p = 2$, $q = 0$, and consider the semi-direct product $Q = \langle x, y | x^8 = y^4 = 1, xy = yx^3 \rangle$ of C_4 with C_8, which has order 2^5. Let G be any group with $Q \cong G/Z^0(G)$. Arguments involving the Schur multiplier of Q (cf. [2]) show that, in this case, such a group G exists and that $\gamma_2^0 G$ must have order 2^3. Wiegold's bound asserts that

$$|\gamma_2^0 G| \le 2^{n(n-1)/2} = 2^{10}.$$

The bound of Gaschütz, Neubüser and Yen asserts that

$$|\gamma_2^0 G| \le |M^0(C_2 \times C_4)|\,|C_2 \times C_2|^2 = 2^5.$$

Since Q is a 2-generator group, Theorem 1(i) asserts that

$$|\gamma_2^0 G| \le 2^{d(2n-d-1)/2} = 2^7.$$

Since $\gamma_2^0 Q/\gamma_3^0 Q \cong C_2$, $\gamma_3^0 Q \cong C_2$, and $\gamma_i^0 Q = 1$ for $i \ge 4$, and since $(Q/Z^0(Q))^{\mathrm{ab}} \cong C_4 \times C_2$, Theorem 2(i) asserts that

$$|\gamma_2^0 G| \le 2^M = 2^5.$$

Let Q be any finite p-group. Then $\gamma_{c+1}^p Q = 1$ for some $c \ge 1$, and the direct sum $\mathfrak{L} = \Gamma_1^p Q \oplus \Gamma_2^p Q \oplus \cdots \oplus \Gamma_c^p Q$ has the structure of a restricted Lie algebra over the field $\mathbb{F} = \mathbb{Z}_p$ (cf. [12]). The Lie bracket $\mathfrak{h}\colon \mathfrak{L} \times \mathfrak{L} \to \mathfrak{L}$ is induced by commutation in Q, and the power map $\mathfrak{p}\colon \mathfrak{L} \to \mathfrak{L}$ is induced by taking p-th powers in Q. For each $i \ge 1$ the bracket $\mathfrak{h}$ restricts to a linear homomorphism $\mathfrak{h}\colon \Gamma_i^p Q \otimes \Gamma_1^p Q \to \Gamma_{i+1}^p Q$ of vector spaces, and repetition of the power map $\mathfrak{p}$ yields a linear homomorphism

$\mathfrak{p}^i\colon \Gamma_1^pQ \to \Gamma_{i+1}^pQ$. The bound of Theorem 1 can be improved by considering the following linear homomorphisms:

$$\begin{aligned}
\mathfrak{j}_2\colon &\Gamma_1^pQ \otimes \Gamma_1^pQ \otimes \Gamma_1^pQ \to \Gamma_2^pQ \otimes \Gamma_1^pQ,\\
&\qquad x\otimes y\otimes z \mapsto \mathfrak{h}(x,y)\otimes z + \mathfrak{h}(y,z)\otimes x + \mathfrak{h}(z,x)\otimes y,\\
\mathfrak{j}_i\colon &\Gamma_1^pQ \otimes \Gamma_1^pQ \otimes \cdots \otimes \Gamma_1^pQ \to \Gamma_i^pQ \otimes \Gamma_1^pQ,\\
&\quad x_1\otimes x_2\otimes\cdots\otimes x_{i+1} \mapsto [x_1,\cdots,x_i]_l \otimes x_{i+1} + [x_{i+1},[x_1,\cdots,x_{i-1}]_l]\\
&\qquad \otimes x_i + [[x_i,x_{i+1}]_r,[x_1,\cdots,x_{i-2}]_l]\\
&\qquad \otimes x_{i-1} + [[x_{i-1},x_i,x_{i+1}]_r,[x_1,\cdots,x_{i-3}]_l]\\
&\qquad \otimes x_{i-2} + \cdots + [x_2,\cdots,x_{i+1}]_r \otimes x_1,\\
\mathfrak{s}_i\colon &\Gamma_1^pQ \to \Gamma_i^pQ \otimes \Gamma_1^pQ, \quad x \mapsto (\mathfrak{p}^{i-1}x)\otimes x, \qquad i\geq 2,\\
\mathfrak{t}_i\colon &\Gamma_1^pQ \otimes \Gamma_1^pQ \to \Gamma_i^pQ \otimes \Gamma_1^pQ, \quad x\otimes y \mapsto (\mathfrak{p}^{i-1}x)\otimes y + (\mathfrak{p}^{i-1}y)\otimes x, \qquad i\geq 2.
\end{aligned}$$

Here $x_i \in \Gamma_1^pQ$ and we have set

$$\begin{aligned}
[x_1,x_2] &= \mathfrak{h}(x_1\otimes x_2),[x_1,\cdots,x_i]_l\\
&= \mathfrak{h}(\cdots\mathfrak{h}(\mathfrak{h}(x_1\otimes x_2)\otimes x_3)\cdots\otimes x_i),[x_1,\cdots,x_i]_r\\
&= \mathfrak{h}(x_1\otimes\cdots\mathfrak{h}(x_{i-2}\otimes\mathfrak{h}(x_{i-1}\otimes x_i))\cdots).
\end{aligned}$$

Note that $\mathfrak{j}_2(x,y,z)=0$ whenever two of x,y,z are equal. Hence $\mathfrak{j}_2$ has trivial image whenever Q is a 2-generator group.

Theorem 3. *Let G be any group such that $Q = G/Z^q(G)$ is a d-generator group of order p^n. Set*

$$a_i = \dim_{\mathbb{F}}(\text{image}(\mathfrak{j}_i) + \text{image}(\mathfrak{s}_i) + \text{image}(\mathfrak{t}_i))$$

for $i\geq 2$, and set $a = a_1 + a_2 + \cdots + a_c$ where $\gamma_{c+1}^pQ = 1$. Then

$$|\gamma_2^qG| \leq p^{(d(2n-d-1)/2)-a+R(Q,q)}.$$

To illustrate Theorem 3 let us return to a group G such that $G/Z^0(G)\cong Q = \langle x,y | x^8 = y^4 = 1,\ xy = yx^3\rangle$. Now $\Gamma_1^2Q \cong \mathbb{Z}_2\oplus\mathbb{Z}_2$ is generated by the cosets of x and y; $\Gamma_2^2Q\cong\mathbb{Z}_2\oplus\mathbb{Z}_2$ is generated by the cosets of x^2 and y^2; $\Gamma_3^2Q\cong Z_2$ is generated by the coset of x^4; $\Gamma_i^2Q = 0$ for $i\geq 4$. Since Q is a 2-generator group, $\mathfrak{j}_2$ has trivial image. One readily verifies that $\mathfrak{j}_3$ also has trivial image. Thus $a_2 = \dim(\text{image}(\mathfrak{s}_2)+\text{image}(\mathfrak{t}_2)) = 3$, $a_3 = \dim(\text{image}(\mathfrak{s}_3)+\text{image}(\mathfrak{t}_3)) = 1$, and $a = 3+1 = 4$. Therefore Theorem 3 asserts that

$$|\gamma_2^0G| \leq 2^{(d(2n-d-1)/2)-a} = 2^3.$$

Vaughan-Lee [16] showed that the commutator subgroup of a finite p-group of "breadth" b has order at most $p^{b(b+1)/2}$. Recall that the *breadth* $b(x)$ of an element x in an arbitrary group G is defined (with respect to the prime p) as the logarithm (to the base p) of the number of elements conjugate to x:

$$b(x) = \log_p|[x]|.$$

Of course, $b(x)$ is infinite when the conjugacy class $[x]$ is infinite. The *breadth* of the group G is defined as the maximum value of $b(x)$ for $x\in G$ if such a maximum exists; otherwise it is defined to be infinite.

Suppose that $Q = G/Z^0(G)$ is a finite p-group. If $C(x)$ denotes the centralizer of x in G, then $p^{b(x)} = |G\colon C(x)|$. Since $|Q| = |G\colon Z^0(G)| = |G\colon C(x)|\times|C(x)\colon$

$Z^0(G)|$ is a power of p, it follows that $b(x)$ is a nonnegative integer for all x in G. For any finite subset $X = \{x_1, \dots, x_d\}$ in G, set

$$b(X) = (b(x_1) + \cdots + b(x_d))/d,$$

and let $\overline{X}$ denote the image of X in Q. It seems reasonable to define the *average breadth* of G to be

$$\overline{b}(G) = \text{minimum}\{b(X)\colon \overline{X} \text{ generates } G/Z^0(G)\}.$$

The following theorem complements Vaughan-Lee's result.

Theorem 4. *Let G be any group such that $Q = G/Z^0(G)$ is a d-generator finite p-group. If G has average breadth $\overline{b} = \overline{b}(G)$, then*

$$|\gamma_2^0 G| \le p^{d\overline{b}}.$$

Our proofs of the above theorems yield the following result of independent interest.

Proposition 5. *Let Q be any d-generator group of order p^n.*

(i) *For a defined as in Theorem 3, we have*

$$|M^q(Q)|\,|\gamma_2^q Q| \le p^{(d(2n-d-1)/2)-a+R(Q,q)}.$$

(ii) *If the abelian groups $(Q/Z^0(Q))^{\mathrm{ab}}$ and $\Gamma_i^0 Q$ have structure as in Theorem 2, then*

$$|M^q(Q)|\,|\gamma_2^q Q| \le p^{M+R(Q,q)}.$$

This bound is attained if the canonical homomorphism $H_3^0(Q) \to H_3^0(Q/\gamma_i^0 Q)$ is surjective for each $i \ge 1$.

Proposition 5(i) (with $q = 0$) sharpens a bound on the Schur multiplier given in [9, Corollary 2.3]. The bound in Proposition 5(ii) (with $q = 0$) is similar to, but lower than, a bound given in [10, Theorem 4.1] (see also [11]); the latter bound uses $\gamma_i^0 G/[\gamma_i^0 G, \gamma_i^0 G]$ in place of our $\gamma_i^0 G/\gamma_{i+1}^0 G$. Proposition 5(ii) also sharpens a bound given in [6].

The proof of Proposition 5 yields analogous bounds on the exponent of $M^q(Q)$ and on the number of generators of $M^q(Q)$. Details of these are left to the reader.

Proposition 5 is relevant to the enumeration of finite p-groups. Let $f(n,p)$ denote the number of groups of order p^n, and set $A(n,p) = \log_p(f(n,p))$. Higman [8] proved that

$$(2/27 - \varepsilon_n)n^3 \le A(n,p) \le (n^3 - n)/6$$

where $\varepsilon_n \to 0$ as $n \to \infty$. Sims [14] subsequently showed that $A(n,p)/n^3 \to 2/27$ as $n \to \infty$. In order to get a feel for the types of p-groups that occur one should investigate, for various group-theoretic properties $\mathcal{P}$, the number $f(n,p,\mathcal{P})$ of groups of order p^n satisfying property $\mathcal{P}$.

Let us consider the number $f(n,p,d)$ of d-generator groups of order p^n, and set

$$A(n,p,d) = \log_p(f(n,p,d)).$$

A lower bound for $A(n,p,d)$ is implicit in [8]. An upper bound can be obtained from Proposition 5. To this effect let us define

$$U(n,d) = \begin{cases} (d-1)(n^2-d^2)/2, & \text{for } d \neq 2, \\ n(n+1)-6, & \text{for } d = 2, \end{cases}$$
$$L(n,d) = (d(d+1)(n-d) - 2(n-d)^2 - 2d^2)/2.$$

The following corollary shows that these two functions give reasonable bounds on $A(n,p,d)$ for "large" values of d.

Corollary 6. *For all integers $n \geq d \geq 1$ we have*

$$L(n,d) \leq A(n,p,d) \leq U(n,d).$$

Furthermore, $A(d,p,d) = U(d,d) = 0$ and for any integer $t \geq 2$ we have

$$\lim_{d\to\infty} \frac{U(td,d)}{L(td,d)} = t+1.$$

Proof. It is implicit in [8] (see also [15]) that $L(n,d)$ is less than $A(n,p,d)$. So we shall concentrate on the upper bound, and on the case $d \neq 2$ (leaving to the reader the case $d = 2$). Certainly $A(n,p,1) = U(n,1)$, so let us suppose that $d \geq 3$. Clearly $A(d,p,d) = U(d,d)$. As an inductive hypothesis assume that $A(k,p,d) \leq U(k,d)$ for some $k \geq d$. For each group G of order p^{k+1} we can choose a central subgroup Z of order p. The group G is determined, up to an extension, by Z and G/Z. In other words G is determined by Z, G/Z, and an element of the second cohomology group $H^2(G/Z, \mathbb{Z}_p)$. The Universal Coefficient Theorem

$$\mathrm{Ext}((G/Z)^{\mathrm{ab}}, \mathbb{Z}_p) \rightarrowtail H^2(G/Z, \mathbb{Z}_p) \twoheadrightarrow \mathrm{Hom}(M^0(G/Z), \mathbb{Z}_p)$$

and Proposition 5(i) imply that

$$|H^2(G/Z, \mathbb{Z}_p)| \leq |M^0(G/Z)| \cdot p^d \leq p^{(d(2k-d+3)-2k)/2}.$$

Therefore

$$\begin{aligned} A(k+1,p,d) &\leq U(k,d) + \log_p |H^2(G/Z, \mathbb{Z}_p)| \\ &\leq ((d-1)(k^2-d^2) + (d(2k-d+3)-2k))/2 \\ &\leq ((d-1)((k+1)^2-d^2) - d^2 + 2d + 1)/2 \\ &\leq ((d-1)((k+1)^2-d^2))/2 \\ &\leq U(k+1,d). \end{aligned}$$

The upper bound of the proposition follows by induction. It is routine to verify the limit in the proposition. □

Our proofs of the above theorems involve the q-exterior product $M \wedge^q N$ of two normal subgroups M and N of some group, a self-contained account of which can be found in [4]. We shall assume a familiarity with the definition of this q-exterior product, and with certain results from [4]. For $q = 0$ the exterior product $M \wedge^0 N$ is that of Brown and Loday [1].

It is shown in [4, p. 247] that $M \wedge^q N$ is finite if both M and N are finite. The following lemma relates the cardinality of the exterior square $Q \wedge^q Q$ to the above theorems.

Lemma 7. *Let G be any group and set $Q = G/Z^q(G)$. Then*:

(i) $|\gamma_2^q G| \leq |Q \wedge^q Q|$.

Moreover, there is a group $\widehat{G}$ such that $\widehat{G}/Z^q(\widehat{G}) \cong Q$ and $\gamma_2^q \widehat{G} \cong Q \wedge^q Q$.

(ii) $|M^q(G)|\,|\gamma_2^q G| = |G \wedge^q G|$.

Proof. Theorem 6 and Proposition 7 in [4] (the first of these results being due to [3]) yield the following diagram of solid homomorphisms:

$$\begin{array}{ccccccc} Z^q(G)\wedge^q G & \xrightarrow{\iota} & G\wedge^q G & \xrightarrow{\pi} & Q\wedge^q Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \partial} & \swarrow & & & \\ & & G & & & & \\ & & \downarrow & & & & \\ & & \Gamma_1^q G & & & & \\ & & \downarrow & & & & \\ & & 1 & & & & \end{array}$$

in which the row and column are exact, and in which $\mathrm{im}(\iota) \subseteq \ker(\partial)$. There is thus a surjection $Q \wedge^q Q \twoheadrightarrow \gamma_2^q G$ from which we deduce that $|\gamma_2^q G| \leq |Q \wedge^q Q|$.

Let $\mu\colon \widehat{G} \to Q$ be any projective q-crossed module with $\mathrm{im}(\mu) = Q$; the definition and existence of such an object is given in [4, p. 245]. Proposition 5 in [4] implies that $\gamma_2^q \widehat{G} \cong Q \wedge^q Q$. The proof of Proposition 16(vii) in [4] implies that $\widehat{G}/Z^q(\widehat{G}) \cong Q$.

Propositions 1 and 5 in [4] imply an exact sequence (which is also to be found in [5])

$$1 \to M^q(G) \to G \wedge^q G \to G \to \Gamma_1^q G \to 1.$$

The equality $|M^q(G)|\,|\gamma_2^q G| = |G \wedge^q G|$ follows from the exactness of this sequence. □

In the following lemma (and throughout the article) we use the symbol $\otimes$ to denote the usual tensor product of abelian groups considered as $\mathbb{Z}$-modules.

Lemma 8. (i) [1] *Any normal inclusion $N \leq G$ gives rise to a natural exact sequence*

$$H_3^0(G) \to H_3^0(G/N) \to N\wedge^0 G \to G\wedge^0 G \to (G/N)\wedge^0(G/N) \to 1.$$

(ii) [4] *Any pair of normal inclusions $N \leq G$ and $M \leq G$ with $M \subseteq N$ give rise to a natural exact sequence*

$$M\wedge^0 G \to N\wedge^0 G \to (N/M)\wedge^0(G/M) \to 1.$$

(iii) *There is an isomorphism*

$$(\Gamma_i^p G)\wedge^0(G/\gamma_{i+1}^p G) \cong (\Gamma_i^p G) \otimes (\Gamma_1^p G)$$

for $i \geq 2$.

(iv) *For $q \geq p$ there is an exact sequence*

$$0 \to \gamma_2^q(M^0(G)) \to G\wedge^0 G \to G\wedge^q G \to \Gamma_1^0 G \to 0.$$

Proof. Part (i) can be found, for instance, in [1], and part (ii) is an easy modification of Proposition 7 in [4]. To prove (iii) note that $\Gamma_i^p G$ lies in the centre of $G/\gamma_{i+1}^p G$. As explained in [1], in this case the defining relations of the exterior product yield an isomorphism

$$\Gamma_i^p G \wedge^0 (G/\gamma_{i+1}^p G) \cong \Gamma_i^p G \otimes (G/\gamma_{i+1}^p G)^{\mathrm{ab}} / \langle x \otimes \overline{x} \mid x \in \Gamma_i^p G \rangle$$

where $\overline{x}$ denotes the image of x in the abelianization of $G/\gamma_{i+1}^p G$. The isomorphism of (iii) follows. The exact sequence of (iv) follows from Proposition 14 in [4]. □

Set $\varepsilon = 0$ or $\varepsilon = p$. Let Q be a p-group of order p^n. Let c be the first integer such that then $\gamma_{c+1}^\varepsilon Q = 1$.

Lemma 8(i) applied to the normal inclusion $\gamma_2^\varepsilon Q \leq Q$ yields the exact sequence

$$\gamma_2^\varepsilon Q \wedge^0 Q \xrightarrow{\alpha_2} Q \wedge^0 Q \longrightarrow \Gamma_1^\varepsilon Q \wedge^0 \Gamma_1^\varepsilon Q \longrightarrow 1. \tag{1}$$

For $i \geq 2$ the normal inclusion $\gamma_{i+1}^\varepsilon Q \leq \gamma_i^\varepsilon Q$ in conjunction with Lemma 8(ii) yields the exact sequence

$$\gamma_{i+1}^\varepsilon Q \wedge^0 Q \xrightarrow{\alpha_{i+1}} \gamma_i^\varepsilon Q \wedge^0 Q \longrightarrow (\gamma_i^\varepsilon Q/\gamma_{i+1}^\varepsilon Q) \wedge^0 (Q/\gamma_{i+1}^\varepsilon Q) \longrightarrow 1. \tag{2}$$

Sequences (1) and (2) in conjunction with Lemma 8(iii) imply

$$|Q \wedge^0 Q| = \frac{|\Gamma_1^\varepsilon Q \wedge^0 \Gamma_1^\varepsilon Q|\, |\Gamma_2^\varepsilon Q \otimes \Gamma_1^\varepsilon Q| \cdots |\Gamma_{c-1}^\varepsilon Q \otimes \Gamma_1^\varepsilon Q|\, |\gamma_c^\varepsilon Q \otimes \Gamma_1^\varepsilon Q|}{|\ker \alpha_2|\, |\ker \alpha_3| \cdots |\ker \alpha_c|}. \tag{3}$$

Recall that the tensor product of any two abelian groups can be computed from the following isomorphisms: $A \otimes (B \times C) \cong (A \otimes B) \times (A \otimes C)$, $A \otimes B \cong B \otimes A$, and $C_m \otimes C_n \cong C_{hcf(m,n)}$ where A, B, C are arbitrary abelian groups, and C_m is the cyclic group of order m. Recall from [1] that for any abelian group A there is an isomorphism $A \wedge^0 A \cong A \otimes A / \langle a \otimes a : a \in A \rangle$. Thus, if

$$\Gamma_i^\varepsilon Q \cong C_{p^{m_{i1}}} \times C_{p^{m_{i2}}} \times \cdots \times C_{p^{m_{ir}}}$$

and if $M_{ijk} = \text{minimum}(m_{ij}, m_{1k})$, then

$$\begin{aligned} \log_p |\Gamma_1^\varepsilon Q \wedge^0 \Gamma_1^\varepsilon Q| &= \sum_{1 \leq j < k \leq r} M_{1jk}, \\ \log_p |\Gamma_i^\varepsilon Q \otimes \Gamma_1^\varepsilon Q| &= \sum_{1 \leq j,\, k \leq r} M_{ijk},\ i \geq 2. \end{aligned} \tag{4}$$

Note that each $|\Gamma_i^\varepsilon Q \otimes \Gamma_1^\varepsilon Q|$ is a maximum, for any given $|\Gamma_i^\varepsilon Q| = p^{m_i}$ and $|\Gamma_1^\varepsilon Q| = p^{m_1}$, if and only if $\Gamma_i^\varepsilon Q$ and $\Gamma_1^\varepsilon Q$ are elementary abelian; in other words

$$\begin{aligned} |\Gamma_1^\varepsilon Q \wedge^0 \Gamma_1^\varepsilon Q| &\leq p^{m_1(m_1-1)/2}, \\ |\Gamma_i^\varepsilon Q \otimes \Gamma_1^\varepsilon Q| &\leq p^{m_1 m_i},\ i \geq 2. \end{aligned} \tag{5}$$

Now (3) and (5) imply that

$$\begin{aligned} |Q \wedge^0 Q| &\leq p^{m_1(m_1-1)/2 + m_1 m_2 + m_1 m_3 + \cdots m_1 m_c} \\ &= p^{m_1(m_1 - 1 + 2m_2 + 2m_3 + \cdots + 2m_c)/2} \\ &= p^{m_1(2n - m_1 - 1)/2}. \end{aligned} \tag{6}$$

Note that if $\varepsilon = p$, then $m_1 = d$ is the minimum number of generators needed for Q. Thus Theorem 1(i) follows from (6), the inequality of Lemma 7(i), and the exact sequence of Lemma 8(iv). For $i \geq 2$ Lemma 8(i) yields an exact sequence

$$H_3^0(Q) \longrightarrow H_3^0(Q/\gamma_i^\varepsilon Q) \longrightarrow \gamma_i^\varepsilon Q \wedge^0 Q \xrightarrow{\beta_i} Q \wedge^0 Q$$
$$\longrightarrow (Q/\gamma_i^\varepsilon Q) \wedge^0 (Q/\gamma_i^\varepsilon Q) \longrightarrow 1.$$

Now β_i factors as

$$\beta_i \colon \gamma_i^\varepsilon Q \wedge^0 Q \xrightarrow{\alpha_i} \gamma_{i-1}^\varepsilon Q \wedge^0 Q \longrightarrow \cdots \xrightarrow{\alpha_2} Q \wedge^0 Q.$$

So $\ker \beta_i = 0$ for all $i \geq 2$ if and only if $\ker \alpha_i = 0$ for all $i \geq 2$. This equivalence, together with Lemma 7(i) and our derivation of Theorem 1(i), imply Theorem 1(ii).

In order to prove Theorem 2 note that when $\varepsilon = 0$ and $i \geq 2$ the homomorphism β_i factors as

$$\begin{array}{ccc} \gamma_i^0 Q \wedge^0 Q & \xrightarrow{\quad\beta_i\quad} & Q \wedge^0 Q \\ & \searrow \quad \nearrow & \\ & \gamma_i^0 Q \wedge^0 (Q/Z^0 Q) & \end{array}$$

since the kernel of the canonical homomorphism $\gamma_i^0 Q \wedge^0 Q \to \gamma_i^0 Q \wedge^0 (Q/Z^0 Q)$ is generated by the elements $x \wedge z$ with $x \in \gamma_i^0 Q$ and $z \in Z^0(Q)$, and since $\beta_i(x \wedge z) = 1$ for each such generator. (To prove the triviality of $\beta_i(x \wedge z)$, note that we can find an element $\tilde{x} \in Q \wedge^0 Q$ which maps canonically onto x. We have $\beta_i(x \wedge z) = x \wedge z = \tilde{x}^z \tilde{x}^{-1}$ by [1]. But z is central and thus acts trivially on $Q \wedge^0 Q$. Therefore $\beta_i(x \wedge z) = \tilde{x}^z \tilde{x}^{-1} = 1$.) This factorization, together with the arguments behind (3), yield the inequality

$$|Q \wedge^0 Q| \leq |\Gamma_1^0 Q \wedge^0 \Gamma_1^0 Q| \, |\Gamma_2^0 Q \otimes \Gamma_1^0 \overline{Q}| \cdots |\Gamma_{c-1}^0 Q \otimes \Gamma_1^0 \overline{Q}| \, |\gamma_c^\varepsilon Q \otimes \Gamma_1^0 \overline{Q}| \tag{7}$$

where $\overline{Q} = Q/Z^0(Q)$.

The proof of Theorem 2 is similar to that of Theorem 1; the differences are that now $\varepsilon = 0$, and that (7) can be used in place of (3).

Theorem 3 is an improvement on parts (i) and (ii) of Theorem 1 obtained by using Theorem 9 in [4] to identify certain non-trivial elements in $\ker \alpha_i$, and thus to estimate $|\ker \alpha_i|$ in (3).

Proposition 5 follows in the same fashion from (3), (7) and Lemma 7(ii).

To prove Theorem 4 suppose that $Q = G/Z^0(G)$ is of order p^n, and that $X = \{x_1, \ldots, x_d\}$ is a subset of G whose image in Q generates Q, and which satisfies $\overline{b}(G) = b(X)$. Denote by C_i the image in Q of the centraliser $C(x_i)$ of x_i in G. Denote by U_i the cyclic subgroup of Q generated by the image of x_i. The image of the canonical homomorphism $C_i \wedge^0 U_i \to Q \wedge^0 Q$ clearly lies in the kernel of the surjection $Q \wedge^0 Q \twoheadrightarrow \gamma_2^0 G$, and this observation is the basis of the proof. Set $\varepsilon = p$, let V_i denote the cyclic summand of $Q/\gamma_2^\varepsilon(Q)$ generated by the image of x_i, and set $D_{ij} = C_i \cap \gamma_j^\varepsilon(Q)$. Note that the canonical homomorphisms

$$(D_{ij}/D_{ij+1}) \otimes V_i \rightarrowtail \Gamma_j^\varepsilon Q \otimes \Gamma_1^\varepsilon Q$$

are injective, and that

$$|(D_{i1}/D_{i2}) \otimes V_i| \, |(D_{i2}/D_{i3}) \otimes V_i| \cdots |D_{ic} \otimes V_i| = |C_i| = p^{n - b(x_i)}.$$

Combining these three observations with (3) yields

$$\begin{aligned}|\gamma_2^0(G)| &\leq \frac{|\Gamma_1^\varepsilon Q \otimes \Gamma_1^\varepsilon Q|\,|\Gamma_2^\varepsilon Q \otimes \Gamma_1^\varepsilon Q| \cdots |\Gamma_{c-1}^\varepsilon Q \otimes \Gamma_1^\varepsilon Q|\,|\gamma_c^\varepsilon Q \otimes \Gamma_1^\varepsilon Q|}{\prod_{1\leq i\leq d} |(D_{i1}/D_{i2}) \otimes V_i|\,|(D_{i2}/D_{i3}) \otimes V_i| \cdots |(D_{ic} \otimes V_i)|} \\ &\leq p^{nd}/p^{n-b(x_1)+\cdots+n-b(x_d)} \\ &= p^{d\bar{b}(G)}\end{aligned}$$

as required.

To prove Theorem 1(iii) for $d = n \geq 2$ set Q equal to the elementary abelian p-group on n generators. Then $|Q| = |\Gamma_1^q Q| = p^n$, $R(Q,q) = 0$, and $|Q \wedge^q Q| = p^{(n(n-1)/2)}$. Moreover, $Q \cong G/Z^q(G)$ for some G by Proposition 16(vii) in [4]. Thus the second assertion of Lemma 7(i) establishes the existence of a group $\widehat{G}$ with $\widehat{G}/Z^q(\widehat{G}) \cong Q$ and $|\gamma_2^q \widehat{G}| = p^{(n(n-1)/2)+R(Q,q)}$.

To prove Theorem 1(iii) for $d = n - 1 = 2$ let us first note that for any abelian groups A, B we can construct a semi-direct product

$$A \square B = ((A \otimes B) \times B) \rtimes Z$$

in which the action of an element a in A on the action of an element (τ, b) in the direct product $(A \otimes B) \times B$ is given by

$${}^a(\tau, b) = (\tau(a \otimes b), b).$$

If the elements of A and B all have order dividing q, then

$$\gamma_2^q(A \square B) \cong A \otimes B.$$

To prove Theorem 1(iii) for $d = n - 1 = 2$ set $Q = C_p \square C_p$. Then $|Q| = p^3$, $|\Gamma_1^q Q| = p^2$, and one can readily verify that $|Q \wedge^q Q| = p^{3+R(Q,q)} = p^{(d(2n-d-1)/2)+R(Q,q)}$. Now $Q \cong G/Z^q(G)$ for some G by Proposition 16(vii) in [4]. Thus the second assertion of Lemma 7(i) establishes the existence of a group $\widehat{G}$ with $\widehat{G}/Z^q(\widehat{G}) \cong Q$ and $|\gamma_2^q \widehat{G}| = p^{(d(2n-d-1)/2)+R(Q,q)}$.

References

[1] R. Brown and J.-L. Loday, *Van Kampen theorems for diagrams of spaces*, Topology **26** (1987), 311–335. MR **88m:**55008

[2] J. Burns, G. Ellis, D. MacHale, P. Ó'Murchú, R. Sheehy, and J. Wiegold, *Lower central series of groups with small upper central factors*, Proc. Royal Irish Acad. (to appear).

[3] D. Conduché and C. Rodríguez-Fernádez, *Nonabelian tensor and exterior products modulo q and universal q-central relative extensions*, J. Pure Applied Algebra **78**, 139–160 (1992). MR **93b:**20085

[4] G. Ellis, *Tensor products and q-crossed modules*, J. London Math. Soc. (2) **51** (1955), 243–258. MR **96c:**20096

[5] G. Ellis and C. Rodríguez-Fernádez, *An exterior product for the homology of groups with integral coefficients modulo q*, Cahiers Topologie Géom. Differentielle Catégoriques **30** (1989), 339–343. MR **90k:**20087

[6] W. Gaschütz, J. Neubüser and Ti Yen, *Über den Multiplikator von p-Gruppen*, Math. Z. **100** (1967), 93–96. MR **36:**272

[7] J. A. Green, *On the number of automorphisms of a finite group*, Proc. Royal Soc. A **237** (1956), 574–581. MR **18:**464c

[8] G. Higman, *Enumerating p-groups*, I. *Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30. MR **22:**4779

[9] M. R. Jones, *Multiplicators of p-groups*, Math. Z. **127** (1972), 165–166. MR **47:**6851

[10] ———, *Some inequalities for the multiplicator of finite group*, Proc. Amer. Math. Soc. **39** (1973), 450-456. MR **47:**3524

[11] ———, *Some inequalities for the multiplicator of a finite group* II, Proc. Amer. Math. Soc. **45** (1974), 167–172. MR **50:**4741
[12] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory*, Dover Publications, New York (1976). MR **54:**10423
[13] I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine angew. Math. **127** (1904), 20–50.
[14] C. C. Sims, *Enumerating p-groups*, Proc. London Math. Soc. (3) **15** (1965), 151–166. MR **30:**164
[15] M. Suzuki, *Group Theory* II, Grundlehren der mathematischen Wissenschaften 248, Springer-Verlag, 1986. MR **87e:**20001
[16] M. R. Vaughan-Lee, *Breadth and commutator subgroups of p-groups*, J. Algebra **32** (1974), 278–285. MR **51:**690
[17] J. Wiegold, *Multiplicators and groups with finite central factor-groups*, Math. Z. **89** (1965), 345–347. MR **31:**3510

Department of Mathematics, University College, Galway, Ireland
E-mail address: graham.ellis@ucg.ie
Current address, September 1998 to June 1999: Max-Planck-Institut für Mathematik, Gottfried-Claren-Straße 26, Bonn, Germany