J. Austral. Math. Soc. (*Series A*) **67** (1999), 191–205

ENUMERATING p-GROUPS

BETTINA EICK and E. A. O'BRIEN

Dedicated to M. F. (Mike) Newman on the occasion of his 65th birthday

(Received 15 September 1998; revised 19 May 1999)

Communicated by C. F. Miller

Abstract

We present a new algorithm which uses a cohomological approach to determine the groups of order p^n, where p is a prime. We develop two methods to enumerate p-groups using the Cauchy-Frobenius Lemma. As an application we show that there are 10 494 213 groups of order 2^9.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 20D15.
Keywords and phrases: p-groups, enumeration, cohomology, Cauchy-Frobenius lemma.

1. Introduction

A central problem in attempting to determine the groups of order p^n, where p is a prime, is that the number of such groups grows exponentially with increasing n. Higman [6] and Sims [15] provide asymptotic estimates which show that the number of groups of order p^n is $p^{2n^3/27+O(n^{8/3})}$.

The p-group generation algorithm ([9, 10]) is a practical algorithm to generate descriptions of the groups of order p^n. Here we present an alternative which uses cohomological techniques to do this task. Both algorithms produce a complete and irredundant list of descriptions of the p-groups of a given order — that is, a representative of each isomorphism type is present and no two elements in the list have the same isomorphism type. A central feature of both algorithms is that the isomorphism problem is solved by explicitly computing certain orbits.

If we want simply to *enumerate* the groups of order p^n, we no longer need explicit descriptions of the groups, but instead need only to determine the number of groups or

equivalently of orbits. We modify the cohomology algorithm to exploit the Cauchy-Frobenius Lemma to count the number of orbits, and hence obtain a practical method to enumerate p-groups. We also develop a variant of the p-group generation algorithm to enumerate the groups of exponent-p class 2.

In a 1967 lecture, Sims outlined a method for enumerating p-groups, by stepping down the lower exponent-p central series and finding orbits of a second cohomology group under the action of automorphisms. (We thank J. Neubüser for drawing our attention to a report of his lecture in [8].)

The problem of determining all groups of a given order was initiated by Cayley in 1854. A bibliography on group enumerations, determinations, and classifications is provided by O'Brien in [13].

The p-group generation algorithm was used to determine the 2328 groups of order 128 (see [7]), the 56 092 groups of order 256 ([11]), and the groups of order dividing 3^6. Besche and Eick [1] developed algorithms to determine the groups of order m, for a given integer m. Besche and Eick [2, 3] determined the non-nilpotent groups of order at most 1000. Combining these results, we now have explicit descriptions for the groups of order at most 1000 with one exception: those of order 512. O'Brien in [11] showed that there are at least 8 445 538 such groups. Since existing computational resources did not readily permit the determination of all of these groups, our initial motivation was the development of methods to enumerate these.

The organisation of this paper is as follows. In Section 2 we consider computationally useful descriptions of p-groups. In Section 3 we introduce the cohomology method to determine up to isomorphism the p-groups of a given order; we also outline the p-group generation method and compare the two algorithms. In Section 4 we present enumeration variants of these algorithms. In Section 5 we discuss implementations of the algorithms. Finally, we report on an application which shows that there are 10 494 213 groups of order 512.

2. Describing p-groups

A group G of order p^n has a composition series with factors of order p, say $G = C_1 \rhd C_2 \rhd \cdots \rhd C_n \rhd C_{n+1} = \{1\}$. If we choose $g_i \in C_i \setminus C_{i+1}$, then we obtain a *polycyclic generating sequence* $(g_1, \ldots, g_n)$ of G. A central feature of a polycyclic generating sequence is that every element of G may be written as a *normal word* $g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_n^{\alpha_n}$ where $0 \leq \alpha_i < p$. Further, $(g_i, \ldots, g_n)$ is a polycyclic generating sequence of C_i. Thus each polycyclic generating sequence determines a composition series of G.

A polycyclic generating sequence $(g_1, \ldots, g_n)$ of G determines a (finite) *power-*

commutator presentation of G with defining relations of the form

$$g_i^p = g_{i+1}^{\beta(i,i,i+1)} \cdots g_n^{\beta(i,i,n)} \text{ and } [g_j, g_i] = g_{j+1}^{\beta(i,j,j+1)} \cdots g_n^{\beta(i,j,n)},$$

where all exponents $\beta(i, j, k) \in \{0, \ldots, p-1\}$. The given polycyclic generating sequence determines the presentation uniquely. These presentations are important in effective computation with p-groups (see [16, Chapter 9]).

The *lower exponent-p central series* of G is the descending sequence of subgroups $G = \mathscr{P}_1(G) \rhd \mathscr{P}_2(G) \rhd \cdots \rhd \mathscr{P}_c(G) \rhd \mathscr{P}_{c+1}(G) = \{1\}$, where $\mathscr{P}_i(G) = [\mathscr{P}_{i-1}(G), G]\mathscr{P}_{i-1}(G)^p$ for $i > 1$. If c is the smallest integer such that $\mathscr{P}_{c+1}(G) = 1$, then G has *exponent-p class* c. A group with exponent-p class c has nilpotency class at most c.

Let $\mathscr{G} = (g_1, \ldots, g_n)$ be a polycyclic generating sequence of G. If the composition series determined by $\mathscr{G}$ refines the lower exponent-p central series of G, then we assign a *weight* w_i to each generator g_i; that is, w_i is the largest integer such that $\mathscr{P}_{w_i}(G)$ contains g_i. The corresponding power-commutator presentation is now weighted, a useful feature for many applications; such a presentation can be constructed for a p-group described in various ways.

3. Generating p-groups

Let G be a finite p-group of exponent-p class c. A group H is a *descendant* of G if $H/\mathscr{P}_{c+1}(H)$ is isomorphic to G. We say that H is an *immediate descendant* of G if it is a descendant of G and has exponent-p class $c+1$.

Note that $\mathscr{P}_2(G) = \Phi(G)$. The rank d of the elementary Abelian p-group $G/\Phi(G)$ is the cardinality of a minimal generating set of G and hence G is a *d-generator* group. Since $\mathscr{P}_{c+1}(H) \leq \mathscr{P}_2(H) = \Phi(H)$, every descendant of G is also a d-generator group. Thus, by induction, every d-generator p-group is a descendant of the elementary Abelian p-group of rank d.

In this section we present two methods to construct p-groups: the cohomology algorithm and the well-known p-group generation algorithm. In summary, both compute power-commutator presentations for the immediate descendants of a finite p-group.

3.1. The cohomology algorithm Let G be a group of order p^n and exponent-p class c, and let h be a positive integer. We present a method to construct up to isomorphism the immediate descendants H of G where $|H| = p^{n+h}$. A standard reference for background material assumed here is Robinson ([14, page 315]).

3.1.1. *Notation and background* Let M be an elementary Abelian p-group acted on by G. Let $Z^2(G, M)$ be the set of all 2-cocycles of G with coefficients in M

and let $B^2(G, M)$ be the subset of $Z^2(G, M)$ consisting of all 2-coboundaries. More precisely:

$$\begin{aligned} Z^2(G, M) =& \{\phi : G \times G \to M \mid \\ & \phi(b, c)\phi(a, bc) = \phi(ab, c)\phi(a, b)^c \text{ for all } a, b, c \in G\}, \\ B^2(G, M) =& \{\phi : G \times G \to M \mid \phi \in Z^2(G, M) \text{ and there} \\ & \text{exists a map } G \to M : g \mapsto m_g \text{ with } \phi(a, b) = m_{ab}m_a^{-b}m_b^{-1}\}. \end{aligned}$$

Setting $(\phi_1\phi_2)(a, b) = \phi_1(a, b)\phi_2(a, b)$, we obtain that $Z^2(G, M)$ is an Abelian group. Since M is an elementary Abelian p-group, $Z^2(G, M)$ is also elementary Abelian. Then the second cohomology group $H^2(G, M)$ is $Z^2(G, M)/B^2(G, M)$.

Each 2-cocycle $\phi \in Z^2(G, M)$ defines an extension $E(\phi)$ of G by M. This extension can be viewed as the Cartesian product $E(\phi) = G \times M$ on which a multiplication is defined by the rule:

$$(g_1, m_1)(g_2, m_2) = (g_1g_2, \phi(g_1, g_2)m_1^{g_2}m_2).$$

Observe that $M(\phi) = \{(1, m) \mid m \in M\}$ is a normal subgroup of $E(\phi)$ isomorphic to M. Note that $(1, m)^{(g,n)} = (1, m^g)$ for $m, n \in M$ and $g \in G$; that is, the conjugation action of $E(\phi)$ on $M(\phi)$ coincides with the action of G on M. Further, for each such extension $E(\phi)$ we have an epimorphism $\psi : E(\phi) \to G : (g, m) \mapsto g$ with kernel $M(\phi)$.

Two 2-cocycles are *equivalent* if they are in the same coset of $B^2(G, M)$. Two extensions $E(\phi_1)$ and $E(\phi_2)$ are equivalent if ϕ_1 and ϕ_2 are equivalent. It is well-known that equivalent extensions are isomorphic; the converse is not necessarily true.

Clearly, the trivial 2-cocycle $1 : G \times G \to M : (g, h) \mapsto 1$ defines the split extension $E(1)$ of G by M and thus each $\phi \in B^2(G, M)$ defines an extension $E(\phi)$ isomorphic to the split extension. Here, the converse is true – each split extension is defined by a 2-cocycle in $B^2(G, M)$.

3.1.2. *A computationally useful view of $H^2(G, M)$* We now restrict our attention to elementary Abelian p-groups M with trivial G-action, although most of the ideas presented below work for arbitrary G-modules M.

Let $(g_1, \ldots, g_n)$ be a polycyclic generating sequence of G; we use the notation of Section 2 for the corresponding power-commutator presentation. Let $(m_1, \ldots, m_h)$ be a polycyclic generating sequence of M and let $\phi \in Z^2(G, M)$. Then $((g_1, 1), \ldots, (g_n, 1), (1, m_1), \ldots, (1, m_h))$ is a polycyclic generating sequence of $E(\phi)$ and determines a unique power-commutator presentation of $E(\phi)$ on these generators.

We now determine relations for this presentation. Clearly, $[(1, m_j), (1, m_i)] = (1, 1)$ and $(1, m_k)^p = (1, 1)$ for $1 \leq i < j \leq h$ and $1 \leq k \leq h$, since $M(\phi)$ is an elementary Abelian p-group; also $[(1, m_j), (g_i, 1)] = (1, 1)$ for $1 \leq j \leq h$ and

$1 \leq i \leq n$, since $E(\phi)$ acts trivially on $M(\phi)$. These relations are independent of the 2-cocycle ϕ. It remains to determine the relations corresponding to the powers $(g_i, 1)^p$ and commutators $[(g_j, 1), (g_i, 1)]$.

LEMMA 3.1. *Let $E(\phi)$ be an extension of G by M, let $\mathcal{G} = (g_1, \dots, g_n)$ be a polycyclic generating set of G and let $w(g_1, \dots, g_n) = w_1 \cdots w_s$ be a word in $\mathcal{G} \cup \mathcal{G}^{-1}$. Then $w((g_1, 1), \dots, (g_n, 1)) = (w(g_1, \dots, g_n), m_w)$ where*

$$m_w = \prod_{k=1}^{s-1} \phi(w_k, w_{k+1} \cdots w_s)\phi_k \in M,$$

and $\phi_k := \phi(w_k, w_k^{-1})^{-1}$ if $w_k \in \mathcal{G}^{-1}$, and $\phi_k := 1$ if $w_k \in \mathcal{G}$.

PROOF. We use induction on the length s of the given word. Clearly, the lemma is true for the empty word. Assume it is true for the subword $v(g_1, \dots, g_n) := w_2 \cdots w_s$.

If $w_1 = g_i$, a generator in $\mathcal{G}$, then

$$\begin{aligned} w((g_1, 1), \dots, (g_n, 1)) &= (g_i, 1)v((g_1, 1), \dots, (g_n, 1)) \\ &= (g_i, 1)(v(g_1, \dots, g_n), m_v) \\ &= (g_i v(g_1, \dots, g_n), \phi(g_i, v)m_v) \\ &= (w(g_1, \dots, g_n), m_w) \end{aligned}$$

as required, since $\phi(g_i, v)m_v = \phi(w_1, w_2 \cdots w_s)m_v = m_w$.

If $w_1 = g_i^{-1}$, the inverse of a generator in $\mathcal{G}$, then

$$\begin{aligned} w((g_1, 1), \dots, (g_n, 1)) &= (g_i, 1)^{-1}v((g_1, 1), \dots, (g_n, 1)) \\ &= (g_i^{-1}, \phi(g_i, g_i^{-1})^{-1})(v(g_1, \dots, g_n), m_v) \\ &= (g_i^{-1}v(g_1, \dots, g_n), \phi(g_i^{-1}, v)\phi(g_i, g_i^{-1})^{-1}m_v) \\ &= (w(g_1, \dots, g_n), m_w) \end{aligned}$$

as required, since $\phi(g_i^{-1}, v)\phi(g_i, g_i^{-1})^{-1}m_v = \phi(w_1, w_2 \cdots w_s)\phi(w_1, w_1^{-1})^{-1}m_v = m_w$. The result follows. □

For example, consider $w(g_1, \dots, g_n) := ([g_j, g_i])^{-1} g_{j+1}^{\beta(i,j,j+1)} \cdots g_n^{\beta(i,j,n)}$ corresponding to a relator in the power-commutator presentation of G. By Lemma 3.1, there exists an element $x_{i,j}(\phi) := m_w \in M$ such that

$$w((g_1, 1), \dots, (g_n, 1)) = (w(g_1, \dots, g_n), x_{i,j}(\phi)) = (1, x_{i,j}(\phi)).$$

We now compute the normal form of $x_{i,j}(\phi)$ in the generators $(m_1, \dots, m_h)$ of M, say $x_{i,j}(\phi) = m_1^{\beta(i,j,n+1)} \cdots m_h^{\beta(i,j,n+h)}$. Then

$$[(g_j, 1), (g_i, 1)] = \prod_{k=j+1}^{n} (g_k, 1)^{\beta(i,j,k)} \prod_{k=1}^{h} (1, m_k)^{\beta(i,j,n+k)}$$

is the relation of $E(\phi)$ of the desired type. Similarly, we compute elements $x_{i,i}(\phi)$ for the power relations $(g_i, 1)^p$ and thus determine that

$$(g_i, 1)^p = \prod_{k=i+1}^{n} (g_k, 1)^{\beta(i,i,k)} \prod_{k=1}^{h} (1, m_k)^{\beta(i,i,n+k)}.$$

The exponents $\beta(i, j, l)$ of these relations depend on the corresponding relations of G for $l \leq n$ and on the elements $x_{i,j}(\phi)$ for $l > n$. Therefore, if the presentation of G and the generating set of M are fixed, then the tuple $X(\phi) := (x_{1,1}(\phi), x_{1,2}(\phi), \ldots, x_{n,n}(\phi))$ defines the power-commutator presentation of $E(\phi)$ determined by $((g_1, 1), \ldots, (g_n, 1), (1, m_1), \ldots, (1, m_h))$.

By Lemma 3.1, the elements $x_{i,j}(\phi)$ are words in the images of ϕ. Thus $E(\phi_1\phi_2)$ has a power-commutator presentation defined by the tuple

$$X(\phi_1)X(\phi_2) = (x_{1,1}(\phi_1)x_{1,1}(\phi_2), \ldots, x_{n,n}(\phi_1)x_{n,n}(\phi_2)).$$

Hence, we obtain a group homomorphism $X : Z^2(G, M) \to M \times \cdots \times M : \phi \mapsto X(\phi)$.

LEMMA 3.2. *Let Z and B be the images under X of $Z^2(G, M)$ and $B^2(G, M)$, respectively. Then $H^2(G, M) \cong Z/B$.*

PROOF. The kernel of X consists of those $\phi \in Z^2(G, M)$ with $x_{i,j}(\phi) = 1$ for all i, j. Thus $X(\phi)$ defines a power-commutator presentation of the split extension of G by M. Therefore $E(\phi)$ is equivalent to $E(1)$, the extension of the trivial cocycle. Thus $\phi \in B^2(G, M)$ and so $\ker(X) \leq B^2(G, M)$. Hence, $Z/B \cong H^2(G, M)$. □

Since, for computational efficiency, we represent p-groups by power-commutator presentations, it is most sensible to represent $H^2(G, M)$ explicitly as Z/B. Moreover, we can view the elementary Abelian p-group M as a vector space over GF(p) and this induces in turn an explicit description of Z and B as vector spaces over GF(p).

3.1.3. *Computing Z and B* Wegner in [19] describes a practical algorithm to compute Z/B, following a suggestion of Leedham-Green and Plesken. We include a brief outline of this method for completeness.

To compute Z we must determine which tuples $(x_{1,1}, x_{1,2}, \ldots, x_{n,n}) \in M \times \cdots \times M$ are in the image of X. Clearly, each such tuple defines a power-commutator presentation of some extension H of G by M, but the order of H may be smaller than $|G||M|$. We want to find the *consistent* presentations of this type – namely, those for extensions of order $|G||M|$.

The *consistency-enforcement* algorithm of Vaughan-Lee [18] exploits the fact that certain equations on products of elements are satisfied in a consistent power-commutator presentation. We adapt his method by viewing the elements $x_{1,1}, \ldots, x_{n,n}$ as

unknowns and write down a power-commutator presentation for a 'generic' extension of G by M containing these unknowns. Then we evaluate these equations and obtain a system of homogeneous linear equations in $x_{1,1}, \ldots, x_{n,n}$. Since $x_{i,j} \in M$, we can treat this system as one of homogeneous linear equations over GF(p) and determine Z as the null space of the system.

To compute B, we consider the definition of $B^2(G, M)$. A 2-cocycle ϕ is in $B^2(G, M)$ if there exists a mapping $\delta : G \to M : g \mapsto m_g$ such that $\phi(x, y) = m_{xy} m_x^{-1} m_y^{-1}$. But each mapping $\delta : G \to M : g \mapsto m_g$ defines a 2-coboundary via this formula. Thus we consider all such mappings δ and compute $X(\phi)$ for the 2-cocycle ϕ defined by δ.

For each δ there is a monomorphism $G \to E(\phi) : g \mapsto (g, m_g)$. In particular, the elements $(g_1, m_{g_1}), \ldots, (g_n, m_{g_n})$ satisfy the relations of G. Thus we may insert these elements $(g_i, m_{g_i}) = (g_i, 1)(1, m_{g_i})$ in the relations of a power-commutator presentation of G and then 'collect' the elements $(1, m_{g_i})$ to the left. By this process we obtain the elements $x_{i,j}(\phi)$ as words in the elements $(1, m_{g_i})$.

To obtain a basis of B, we must compute the tuples $(x_{1,1}, \ldots, x_{n,n})$ for all mappings $\delta : G \to M$. For this purpose, we consider the elements m_{g_i} to be arbitrary elements of M. Thus, instead of fixed elements m_{g_i}, we insert a basis of M in the relations of G and so obtain a basis of B.

3.1.4. *The subset of $H^2(G, M)$ corresponding to descendants* An extension $E(\phi)$ of G by M is an immediate descendant of G if $E(\phi)/\mathscr{P}_{c+1}(E(\phi)) \cong G$. Observe that $E(\phi)/M(\phi) \cong G$. Since G has exponent-p class c, we have $\{1\} = \mathscr{P}_{c+1}(G) \simeq \mathscr{P}_{c+1}(E(\phi)/M(\phi)) = \mathscr{P}_{c+1}(E(\phi))M(\phi)/M(\phi)$. Hence, $\mathscr{P}_{c+1}(E(\phi)) \leq M(\phi)$. Thus $E(\phi)$ is an immediate descendant of G if and only if $M(\phi) = \mathscr{P}_{c+1}(E(\phi))$.

Our aim is to find a description of those equivalence classes of 2-cocycles which correspond to immediate descendants. To facilitate this, we assume that the given power-commutator presentation of G is weighted. Let $g_{r+1}, \ldots, g_n$ be the generators of G of highest weight c and so $\mathscr{P}_c(G) = \langle g_{r+1}, \ldots, g_n \rangle$. Then $g_j^p = 1$ and $[g_j, g_i] = 1$ for $r + 1 \leq j \leq n$ and $1 \leq i \leq n$.

LEMMA 3.3. *Let $E(\phi)$ be an extension of G by M and let the power-commutator presentation of G be weighted. Then $E(\phi)$ is an immediate descendant of G if and only if $\langle x_{i,j}(\phi) \mid r + 1 \leq i \leq n$ and $1 \leq j \leq i \rangle = M$.*

PROOF.

$$\begin{aligned}
\mathscr{P}_{c+1}(E(\phi)) &= [\mathscr{P}_c(E(\phi)), E(\phi)]\mathscr{P}_c(E(\phi))^p \\
&= \langle [(g_i, 1), (g_j, 1)], (g_i, 1)^p \mid r + 1 \leq i \leq n \text{ and } 1 \leq j < i \rangle \\
&= \langle ((1, x_{i,j}(\phi)), (1, x_{i,i}(\phi)) \mid r + 1 \leq i \leq n \text{ and } 1 \leq j < i \rangle \\
&= \langle (1, x_{i,j}(\phi)) \mid r + 1 \leq i \leq n \text{ and } 1 \leq j \leq i \rangle.
\end{aligned}$$

Since $E(\phi)$ is an immediate descendant of G if and only if $\mathscr{P}_{c+1}(E(\phi)) = M(\phi)$, the result follows. □

Hence, we can decide readily from $X(\phi)$ whether or not $E(\phi)$ is an immediate descendant of G. By Lemma 3.3, we are interested only in extensions $E(\phi)$ of G by M where no maximal subgroup of M contains all of the elements $x_{i,j}(\phi)$ for $r+1 \leq i \leq n$ and $1 \leq j \leq i$. Let $C = Z/B$. We introduce the following notation for maximal subgroups U of M.

$$Z(U) := \{X(\phi) \in Z \mid x_{i,j}(\phi) \in U \text{ for } r+1 \leq i \leq n \text{ and } 1 \leq j \leq i\},$$
$$C(U) := Z(U)B/B.$$

Then the subset of C containing equivalence classes of 2-cocycles which correspond to immediate descendants of G is given by

$$D := C \setminus \bigcup_{U \lhd M} C(U).$$

3.1.5. *Isomorphism classes of immediate descendants* Two non-equivalent 2-cocycles in D may lead to isomorphic extensions. Hence, we determine the subsets of D that correspond to distinct isomorphism types of immediate descendants. This is a special case of the method described in Besche and Eick [1, Section 3.3]; we give only an outline here.

First, we define an action of $A := \mathrm{Aut}\ G \times \mathrm{Aut}\ M$ on C. Let $(\alpha, \nu) \in A$ and let $\phi : G \times G \to M$ be an element of $Z^2(G, M)$. Then we define

$$\phi^{(\alpha,\nu)} : G \times G \to M : (x, y) \mapsto (x^{\alpha^{-1}}, y^{\alpha^{-1}})^{\nu}.$$

This yields an action of A on $Z^2(G, M)$ which leaves $B^2(G, M)$ setwise invariant. We obtain an induced action of A on $H^2(G, M)$ and thus on C.

Next, we define an equivalence relation between extensions. Two extensions $E(\phi_1)$ and $E(\phi_2)$ of G by M are *strongly isomorphic* if there exists an isomorphism $\iota : E(\phi_1) \to E(\phi_2)$ with $M(\phi_1)^{\iota} = M(\phi_2)$. We are interested in this equivalence because of the following result of Besche and Eick [1, Theorem 3.6].

THEOREM 3.4. *The orbits of A on $H^2(G, M)$ are in one-to-one correspondence to the strong isomorphism types of extensions of G by M.*

Let $E(\phi_1)$ and $E(\phi_2)$ be two extensions of G by M which are immediate descendants of G. Then $M(\phi_i) = \mathscr{P}_{c+1}(E(\phi_i))$ for $i = 1, 2$. Thus the embedding of M in each of these extensions is a subgroup which is invariant under isomorphisms; that is, for each isomorphism $\iota : E(\phi_1) \to E(\phi_2)$ we have that $M(\phi_1)^{\iota} = \mathscr{P}_{c+1}(E(\phi_1))^{\iota} = \mathscr{P}_{c+1}(E(\phi_1)^{\iota}) = \mathscr{P}_{c+1}(E(\phi_2)) = M(\phi_2)$. Hence, strong isomorphism is equivalent to isomorphism for immediate descendants. We obtain the following corollary to Theorem 3.4.

COROLLARY 3.5. *Two immediate descendants $E(\phi_1)$ and $E(\phi_2)$ are isomorphic if and only if the cosets $\phi_1 B^2(G, M)$ and $\phi_2 B^2(G, M)$ are contained in the same orbit under the action of A on $H^2(G, M)$.*

3.1.6. *Listing the distinct isomorphism types* We obtain the list of isomorphism types of immediate descendants of G having order p^{n+h} as the extensions of G by M defined by orbit representatives in $D \subseteq C \cong H^2(G, M)$ under the action of $A \cong \text{Aut } G \times \text{Aut } M$.

Since C is a subgroup of the l-fold Cartesian product of M, we may view C as a subspace of the (lh)-dimensional vector space over GF(p). The action of A on $Z^2(G, M)$ and thus on C is linear. Therefore we can represent A as a matrix group acting on C. To apply Lemma 3.4, we compute orbits of the vectors in D under the action of a matrix group.

3.1.7. *A reduction of the orbit computation* Consider the elements of C as $l \times h$ matrices. Then the action of Aut M on C is the natural action of GL(h, p) by matrix multiplication from the right. Hence, for each element in C we can compute a 'standard representative' of its Aut M orbit by Gaussian elimination, and so we do not need to list explicitly the Aut M orbits of C. To determine the Aut $G \times$ Aut M orbits on C, we now compute the Aut G orbits of the Aut M orbits on C.

3.2. The p-group generation algorithm We now briefly outline the p-group generation algorithm of O'Brien [10]. Let G be a d-generator p-group of order p^n and exponent-p class c and let F be the free group on d generators. Then $G = F/R$ for some R. Assume we wish to construct the immediate descendants of G having order p^{n+h} for fixed $h > 0$. First, we compute a power-commutator presentation for the maximal central, elementary Abelian Frattini extension of G. This extension G^* is the *p-covering group* of G and is defined by $G^* = F/[R, F]R^p$. Thus, G^* has a normal subgroup M where $G^*/M \cong G$ and M is elementary Abelian, central and contained in the Frattini subgroup of G^*. The subgroup M is the *p-multiplicator* of G. Further, G^* has exponent-p class at most $c+1$ and $N := \lambda_{c+1}(G^*) \leq M$ is the *nucleus* of G. Now, G^* has the property that every immediate descendant of G is a factor group G^*/U, where U is a supplement of N in M. Also, Aut G, the automorphism group of G, induces a linear action on M and the orbits of Aut G on supplements of index p^h in M to N are in one-to-one correspondence with isomorphism class representatives of immediate descendants of G having order p^{n+h}.

3.3. A comparison of the two algorithms In both cases, isomorphism classes of immediate descendants are obtained by computing certain orbits and taking a representative of each orbit. The central difference between the methods lies in the objects permuted.

Using the cohomology method, we determine orbits of vectors under the action of Aut $G \times$ Aut M or orbits of Aut M orbits under the action of Aut G; using p-group generation, we determine orbits of subspaces under the action of Aut G.

This suggests that the cohomology algorithm will not yield a significantly better approach to the determination of p-groups than the p-group generation algorithm.

One important advantage of the cohomology algorithm is that it may be modified easily to a general enumeration method; such a modification for the p-group generation algorithm is more complex and has been developed only for exponent-p class 2 groups.

4. Enumeration variants of the algorithms

Recall that isomorphism classes of immediate descendants are obtained by computing certain orbits and taking a representative of each orbit. Their explicit computation is the *practical* limitation in applying these algorithms.

Consider the task of *enumerating* the groups of order p^n. We no longer need explicit descriptions of the groups, but instead need only to determine the number of orbits. Hence, we can use the Cauchy-Frobenius Lemma (see, for example, Robinson [14, page 42]) to count the number of orbits.

LEMMA 4.1. *Let G be a finite group acting on a finite set Ω. Let $\mathscr{C}$ be a set of conjugacy class representatives of G and let $cl(g)$ be the conjugacy class of $g \in G$. Let* $\mathrm{Fix}_g(\Omega) = \{\alpha \in \Omega \mid \alpha g = \alpha\}$. *The number k of orbits of G on Ω is given by*

$$k = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_g(\Omega)| = \frac{1}{|G|} \sum_{g \in \mathscr{C}} |cl(g)||\mathrm{Fix}_g(\Omega)|.$$

4.1. Using the cohomology method to enumerate p-groups It is easy to incorporate this observation into the cohomology algorithm of Section 3.1. Recall that C is a vector space defined over GF(p) and D is a subset of C. We want to compute the number of orbits of $A =$ Aut $G \times$ Aut M in its action on D. Computing the conjugacy classes of A reduces to the separate computation of conjugacy classes of Aut G and Aut $M \cong GL(h, p)$. Let $a \in A$ and define $F_a := \mathrm{Fix}_a(C)$. Then $|\mathrm{Fix}_a(D)|$ can be computed using the following formula.

$$\begin{aligned} |\mathrm{Fix}_a(D)| &= |F_a \setminus \mathrm{Fix}_a(\cup_{U<M} C(U))| \\ &= |F_a| - |\mathrm{Fix}_a(\cup_{U<M} C(U))| \\ &= |F_a| - |F_a \cap (\cup_{U<M} C(U))| \\ &= |F_a| - |\cup_{U<M} F_a \cap C(U)|. \end{aligned}$$

Since A acts as a matrix group on D, the subspace F_a of C can be computed as the nullspace of $M_a - I$, where M_a is the matrix representation of a on C. Variants of

Gaussian elimination can be used to compute intersections of the subspaces $F_a \cap C(U)$. It is more difficult to compute the cardinality of the union of subspaces of the form $F_a \cap C(U)$, since this is not usually a subspace; we use a recursive procedure and the formula $|W \cup V| = |W| + |V| - |W \cap V|$.

4.2. Enumerating exponent-p class 2 groups If our goal is only to enumerate the groups of exponent-p class 2, we can simplify details of the calculations. In practice, if our motivation is to obtain a *good estimate* for the number of groups of order p^n, then this limitation is not significant, since 'almost all' p-groups have class 2 [6, 15].

Since the conjugacy class of an element of $\mathrm{GL}(m, p)$ is determined by its (primary) rational canonical form, it is an easy task to write down representatives and lengths for the conjugacy classes of $\mathrm{GL}(m, p)$. Hence, we can readily compute the conjugacy class information required for the relevant automorphism group.

4.2.1. *Using p-group generation to enumerate class 2 groups* If G is a d-generator elementary Abelian p-group, then its p-multiplicator M has rank $d + \binom{d}{2}$ and coincides with the nucleus, N.

To apply the Cauchy-Frobenius Lemma to count the number of immediate descendants of G, we must now determine the number of subspaces of a particular dimension of M which are fixed under the action of an element of Aut G on M. How do we calculate this?

We first consider the following problem. Let A be an Abelian p-group of order p^n. How many subgroups of A have order p^k?

Let A be isomorphic to $\prod_{i\geq 1} C(p^i)^{a_i}$. Define $\alpha_i = a_i + a_{i+1} + \cdots$. Then the partition $(\alpha_1 \geq \alpha_2 \geq \cdots)$ of n specifies the isomorphism *type* of A. Observe that $|\Omega_i A / \Omega_{i-1} A| = p^{\alpha(i)}$. If $B \leq A$, then the type β of B is $(\beta_1 \geq \beta_2 \geq \cdots)$, where $\beta_i \leq \alpha_i$ for all i.

Let $\binom{n}{k}_p$ be the number of k-dimensional subgroups of an n-dimensional vector space over $\mathrm{GF}(p)$.

LEMMA 4.2 (Birkhoff [4]). *Let $f(\alpha, \beta, p)$ denote the number of subgroups of type β in the finite Abelian p-group of type α. Then*

$$f(\alpha, \beta, p) = \prod_{i\geq 1} p^{\beta_{i+1}(\alpha_i - \beta_i)} \binom{\alpha_i - \beta_{i+1}}{\beta_i - \beta_{i+1}}_p .$$

Hence, the number of subgroups of A having order p^k is $\sum_\beta f(\alpha, \beta, p)$ where β runs over the dual of each restricted partition of k.

Clearly, this enables one to count the number of subgroups of a given order in any finite Abelian group, or the number of submodules of a given order in a finite module over any principal ideal domain. When the principal ideal domain is the polynomial algebra $\mathrm{GF}(q)[x]$, where $q = p^e$, the question may be paraphrased as follows.

Let g be an element of $\mathrm{GL}(n, q)$ and let V denote the vector space on which this group naturally acts. How many g-invariant subspaces of dimension k does V have?

Of course, the answer depends on g and, more precisely, on the conjugacy class of g in $\mathrm{GL}(n, q)$, which may be identified by giving the distinct irreducible factors $f_1, \ldots, f_r$ of the characteristic polynomial of g and the numbers $n_{i,j}$ of the indecomposable blocks with characteristic polynomial f_i^j in the (primary) rational normal form of g.

Write $v_{i,j} = n_{i,j} + n_{i,j+1} + \cdots$; then $n_i = \sum_j v_{i,j} = \sum_j j n_{i,j}$. Let v_i be the partition of n_i so defined: namely,

$$v_i = (v_{i,1} \geq v_{i,2} \geq \cdots).$$

Then V is a direct sum of subspaces V_i where

$$V_i = \{v \in V \mid v f_i(g)^{n_i} = 0\}.$$

How do we count the g-invariant subspaces of dimension k? Let $\delta = (\delta_1, \ldots, \delta_r)$ range over all sequences of non-negative integers such that $k = \sum_i \delta_i \deg(f_i)$ and $\delta_i \leq n_i$ for $i = 1, \ldots, r$. For each such $\delta = (\delta_1, \ldots, \delta_r)$, we first count the number of $\langle g \rangle$-submodules of V_i having composition length δ_i. We next form the product of these values over i, and finally we sum the products over each δ.

How do we compute the number of $\langle g \rangle$-submodules of V_i with composition length δ_i? Let $\gamma = (\gamma_1 \geq \gamma_2 \geq \cdots)$ be a partition of δ_i such that $\gamma_j \leq v_{i,j}$ for all j. Then the number of $\langle g \rangle$-submodules of V_i of isomorphism type γ is $f(v_i, \gamma, p^{\deg(f_i)})$.

In summary, the number of g-invariant subspaces of dimension k is

$$\sum_{\delta} \prod_{i} \sum_{\gamma} f(v_i, \gamma, p^{\deg(f_i)}).$$

5. Implementations

GAP 4 [17] provides most of the underlying machinery needed to implement the cohomology algorithm and its enumeration variant. In particular, GAP 4 can compute the explicit descriptions of C and D and the matrix action of A on C. Using GAP 4b3 on a 400Mhz Pentium Pro machine under Linux, it takes approximately 20 minutes of CPU time to compute the information of Table 1.

We also implemented the enumeration variant of p-group generation in MAGMA [5]. Our implementation counts: the subgroups of an Abelian p-group; given $g \in \mathrm{GL}(d, q)$, the number of g-invariant subspaces of a given dimension; the number of d-generator p-groups of exponent-p class 2. Using MAGMA V2.4 on a Sun UltraSPARC Enterprise 4000 server, it takes approximately 2 minutes of CPU time to compute the

TABLE 1. Number of d-generator groups of order 2^n and exponent-p class 2

	n								
d	2	3	4	5	6	7	8	9	10
1	1								
2		3	3	1					
3			4	15	28	15	4	1	
4				6	54	604	3 566	6 709	3 566
5					7	151	26 065	5 829 109	378 628 831
6						9	433	2 948 829	47 698 016 406
7							10	1 112	726 843 973
8								12	2 933
9									13
Total	1	3	7	22	89	779	30 078	8 785 772	48 803 495 722

TABLE 2. Number of groups of order 512 having exponent-p class at least 3

Order	k	t
2^5	2	9
2^6	27	30 759
2^7	263	218 225
2^8	12 105	1 459 447
Total		1 708 440

information of Table 1. It is particularly easy to extend these results. For example, we counted the number of exponent-p class 2 groups of order at most p^{10} for primes p at most 7; see [13] for results.

6. An application

Our primary application is the enumeration of the 2-groups of exponent-p class 2 and order dividing 1024. The results are recorded in Table 1.

We used the variant of the cohomology algorithm to enumerate the remaining groups of order 512: those having exponent-p class *at least* 3. The algorithm takes as input both a power-commutator presentation for the given p-group and a description of its automorphism group. For each relevant group of order dividing 256, its automorphism group was computed using an extension developed by the authors of O'Brien's algorithm [12].

For each relevant order 2^n, we record in Table 2 the number k of groups of this

order having immediate descendants of order 512 and the total number t of immediate descendants of these k groups. Hence, the number of groups of order 512 is 10 494 213.

Since the figures obtained agree with those already known for the groups of order dividing 256, it provides some assurance that our implementations are correct. Ours is the first enumeration, independent of p-group generation, of the groups of order 256 and so it is a cross-check for the results of [11].

Acknowledgements

We thank L. G. Kovács, C. R. Leedham-Green, J. Neubüser, and M. F. Newman for invaluable discussion and comment. O'Brien acknowledges the financial support of the Alexander von Humboldt Foundation, Bonn.

References

[1] H. U. Besche and B. Eick, 'Construction of finite groups', *J. Symbolic Comput.* **27** (1999), 387–404.
[2] ———, 'The groups of order at most 1000 except 512 and 768', *J. Symbolic Comput.* **27** (1999), 405–413.
[3] ———, 'The groups of order $q^n \cdot p$', Technical Report.
[4] G. Birkhoff, 'Subgroups of Abelian groups', *Proc. London Math. Soc.* **38** (1934), 385–401.
[5] W. Bosma, J. Cannon and C. Playoust, 'The MAGMA algebra system I: The user language', *J. Symbolic Comput.* **24** (1997), 235–265.
[6] G. Higman, 'Enumerating p-groups. I: Inequalities', *Proc. London Math. Soc.* **10** (1960), 24–30.
[7] R. James, M. F. Newman and E. A. O'Brien, 'The groups of order 128', *J. Algebra* **129** (1990), 136–158.
[8] J. Neubüser, 'Investigations of groups on computers', in: *Computational problems in abstract algebra* (Pergamon Press, Oxford, 1967) pp. 1–19.
[9] M. F. Newman, 'Determination of groups of prime-power order', in: *Group theory (Canberra 1975)*, Lecture Notes in Math. 573 (Springer, Berlin, 1977) pp. 73–84.
[10] E. A. O'Brien, 'The p-group generation algorithm', *J. Symbolic Comput.* **9** (1990), 677–698.
[11] ———, 'The groups of order 256', *J. Algebra* **143** (1991), 219–235.
[12] ———, 'Computing automorphism groups of p-groups', in: *Computational algebra and number theory (Sydney, 1992)* (Kluwer Academic Publ., Dordrecht, 1995) pp. 83–90.
[13] ———, 'Bibliography on the determination of finite groups', Available from `http://www.math.auckland.ac.nz/~obrien`.
[14] D. J. Robinson, *A course in the theory of groups*, Graduate Texts in Math. 80, 2nd Edition (Springer, New York, 1996).
[15] C. C. Sims, 'Enumerating p-groups', *Proc. London Math. Soc.* **15** (1965), 151–166.
[16] ———, *Computation with finitely presented groups* (Cambridge University Press, New York, 1994).
[17] The GAP Team, GAP – *Groups, algorithms, and programming, version* 4, Lehrstuhl D für Mathematik, RWTH Aachen, and School of Mathematical and Computational Sciences, University of St Andrews, 1999.
[18] M. R. Vaughan-Lee, 'An aspect of the nilpotent quotient algorithm', in: *Computational group theory (Durham, 1982)* (Academic Press, London, 1984) pp. 76–83.

[19] A. Wegner, *The construction of finite soluble factor groups of finitely presented groups and its applications* (Ph.D. Thesis, University of St Andrews, 1992).

Fachbereich Mathematik
Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel
Germany
e-mail: eick@mathematik.uni-kassel.de

Department of Mathematics
University of Auckland
Private Bag 92019
Auckland
New Zealand
e-mail: obrien@math.auckland.ac.nz