The groups of order 256

Abstract

Building on earlier work, a new method for generating descriptions of p-groups is developed. The theory and implementation of this method are described and its application in determining the 56 092 groups of order 256 is outlined.

1 Introduction

In 1951, a detailed proposal for the use of computers in mathematics was made in a lecture by M.H.A. Newman, delivered at the Inaugural Conference of the Manchester University Computer. In his address, he discussed the use of probability testing in determining the groups of order 256. In this paper, an algorithm used in the determination of the 56 092 groups of this order by computer is described.

In a 1977 paper, M.F. Newman gave a theoretical description of an algorithm that can be used to generate descriptions of finite p-groups. The theory and implementation of this algorithm, now known as the p-group generation algorithm, are described in detail in O'Brien (1990). In practice, there are space and time limitations on the performance of the algorithm implementation. The algorithm extensions described here and in O'Brien (1990) significantly increase the range of applicability of the algorithm.

The determination of the groups of order 256 is used to motivate the development of the extension. A detailed description of earlier work in using the algorithm to determine the groups of order 128 is provided in James, Newman & O'Brien (1990). However, the algorithm extension is described in a general context. An application of the extension is given and a summary of the results of the determination of the groups of order dividing 256 is given.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20-04, 20D15.

2 An extended p-group generation algorithm

In this paper, it is not intended to provide background on either the theory or implementation of the p-group generation algorithm. The interested reader is referred to Newman (1977) and O'Brien (1990). The notation used in the latter paper will be used here and the implementation described there will be known as the standard implementation.

The standard implementation was used to determine all of the groups of order 256 except for the immediate descendants of the elementary abelian groups of order 32 and 64. These groups are denoted by (1^5) and (1^6), respectively. In these cases, difficulties arise in computing the orbits of the allowable subgroups since the permutation group degrees are $6\ 347\ 715$ and $178\ 940\ 587$, respectively. The direct computation of the orbits of such permutation groups requires "large" resources. (However, such a calculation is possible for (1^5); in fact, it was carried out in order to verify the results obtained in applying the extension described below.)

As a consequence, an extended algorithm was developed. The idea of the algorithm is to use available information on the orbits of the s-step relative allowable subgroups together with some additional information to obtain a representative of each orbit of the (s+1)-step relative allowable subgroups. The additional information - essentially, automorphisms that map certain elements to their orbit representatives - can be obtained easily. The representative obtained for each orbit is not necessarily the representative obtained by using the standard implementation. The extended algorithm can also be used to obtain a stabiliser of each representative.

Some of the notation established in O'Brien (1990) is summarised here. Let $G = F/R$ be a p-group where F is a free group; its automorphism group is $\mathrm{Aut}\, G$, its p-covering group, G^*, is F/R^*, and its p-multiplicator, R/R^*, has rank q. Let C/R^* be a characteristic, initial segment subgroup of rank t, where $1 \leq t \leq q$, in the p-multiplicator of G. The orbits of the s-step allowable subgroups are known as s-step orbits.

Information is required on the orbits of the (s+1)-step allowable subgroups relative to C/R^*. In applying the extended algorithm, it is assumed that the orbits of the s-step allowable subgroups relative to C/R^* have been computed and that the stabiliser of each orbit representative has been calculated.

Note that each s-step orbit representative is a subgroup of rank $t - s$. The initial step of the extended algorithm is the following:

1. For each s-step orbit representative in turn, compute the orbits of its maximal subgroups under the action of its stabiliser. These orbits are called *suborbits.*

The representative of each suborbit is a subgroup of rank $t - s - 1$. If C/R^* is properly contained in the nucleus, N/R^*, then the relative nucleus is C/R^*; it follows that each suborbit representative is an (s+1)-step allowable subgroup relative to C/R^*.

The remaining case where the characteristic subgroup, C/R^*, contains N/R^* is illustrated in Figure 1.

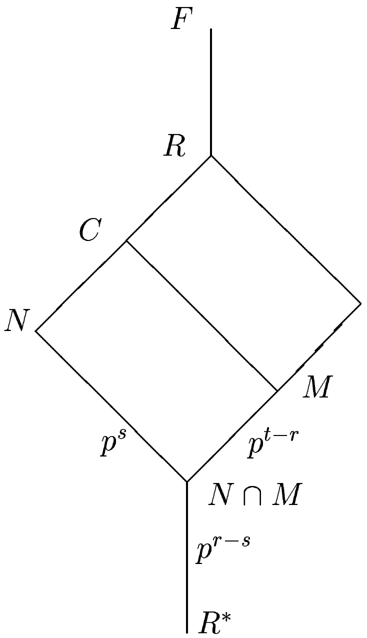

Figure 1: The characteristic subgroup contains the nucleus

The s-step relative allowable subgroup M/R^* intersects the relative nucleus, N/R^*, in a subgroup of rank $r - s$. Since G has (s+1)-step immediate descendants, this intersection is non-trivial. Let U/R^* be a maximal subgroup of M/R^*. If U contains $M \cap N$, then U/R^* is not an (s+1)-step allowable subgroup since it does not supplement the relative nucleus. If U does not contain $M \cap N$, then U/R^* intersects the nucleus in a subgroup of smaller rank; therefore, it supplements N/R^* in C/R^* and it is an (s+1)-step allowable subgroup. The nucleus is a characteristic subgroup and M/R^* is fixed under the action of its stabiliser. Hence, the intersection of N/R^* with M/R^* is fixed under the action of the stabiliser of M/R^*. Thus, the suborbits are of two types: either all elements of a suborbit are (s+1)-step allowable subgroups or all elements are not. The latter suborbits are not required for the present calculation.

For the remainder of this section, relative allowable subgroups are simply described as allowable subgroups. In order to assist the discussion, let the s-step orbits of G be denoted by $O_1, \ldots, O_u$ and let these orbits have representatives $R_1, \ldots, R_u$, respectively. An arbitrary s-step allowable subgroup is denoted by M rather than M/R^* and, similarly, an arbitrary (s+1)-step allowable subgroup is denoted by U.

Let $\mathcal{L}$ be the list obtained by choosing a representative of each suborbit consisting of (s+1)-step allowable subgroups.

Lemma 2.1 *The list $\mathcal{L}$ contains an element of each orbit of the (s+1)-step allowable subgroups.*

Proof Let U be an arbitrary (s+1)-step allowable subgroup, let M be an s-step allowable subgroup containing U, and let the representative of the s-step orbit containing M be R_k. Then there exists an extended automorphism, α^*, of G that maps M to R_k. The (s+1)-step allowable subgroup $U\alpha^*$ is in some suborbit of R_k and the representative of this suborbit is in $\mathcal{L}$. The suborbit representative and U are in the same (s+1)-step orbit. □

Two members of the list may be in the same (s+1)-step orbit, so this lemma gives an upper bound on the number of (s+1)-step orbits.

As a first step to reducing $\mathcal{L}$ to a list of orbit representatives, certain orbit invariants are computed. Each $(s{+}1)$-step allowable subgroup has rank $t-s-1$ and is a maximal subgroup of $v=(p^{s+1}-1)/(p-1)$ s-step allowable subgroups. The *cycle structure* of an $(s{+}1)$-step allowable subgroup, U, is the symbol $(i_1^{m_1}\dots i_\eta^{m_\eta})$, where $\sum_{j=1}^{\eta} m_j = v$ and, for each $j\in\{1,\dots,\eta\}$, m_j is the number of s-step allowable subgroups in O_{i_j} which contain U. The number of occurrences of each i_j is its *multiplicity.*

Lemma 2.2 *Any two elements of the same* $(s{+}1)$*-step orbit have the same cycle structure.*

Proof Let U be an $(s{+}1)$-step allowable subgroup and let $U\alpha^*$ be its image under an extended automorphism, α^*, of G. Let M be one of the s-step allowable subgroups that contain U. Then M and $M\alpha^*$ are elements of the same s-step orbit. Therefore, U and $U\alpha^*$ have the same cycle structure. □

Thus, only suborbit representatives having the same cycle structure can be elements of the same $(s{+}1)$-step orbit and the number of different cycle structures is a lower bound on the number of $(s{+}1)$-step orbits.

Lemma 2.3 *Let* U *be a representative of a suborbit of* R_k. *If its cycle structure contains an occurrence of some* j *where* $j\neq k$, *then there is another member of* $\mathcal{L}$ *that is in the same* $(s{+}1)$*-step orbit as* U.

Proof Since the cycle structure of U contains an occurrence of some j where $j\neq k$, one of the s-step allowable subgroups containing U is an element of the s-step orbit O_j. Therefore, there exists an extended automorphism, α^*, of G that maps this subgroup to the representative, R_j, of the orbit O_j. Applying α^* to the suborbit representative U, a new element is obtained which is a maximal subgroup of R_j. Representatives of the suborbits of R_j are in $\mathcal{L}$ and U is in the same $(s{+}1)$-step orbit as one of these representatives. □

The s-step orbit representatives are organised as a list in which they are ordered by increasing label. In computing the suborbits, the s-step orbit representatives are processed in this order. This provides an ordering on the members of $\mathcal{L}$.

When the cycle structures of the members of $\mathcal{L}$ have been computed, Lemma 2.3 may show that there are certain duplications in $\mathcal{L}$. This lemma is applied by deleting those members of the list that are representatives of suborbits of R_k and have cycle structures containing an occurrence of some j, where $j < k$. In this way, a new list, $\mathcal{L}$, is obtained.

In this new list, duplications can occur only in the following case: let R_k be the representative of a particular s-step orbit O_k and let $U_1, \ldots, U_y$ be suborbit representatives of R_k which have the same cycle structure. Each element of this cycle structure is at least k and the multiplicity of k is at least 1 since one of the s-step allowable subgroups containing each of these subgroups is R_k.

The following lemma deals with the case where the multiplicity of k in the cycle structure of these suborbit representatives is exactly 1.

Lemma 2.4 *Let U be both an element of $\mathcal{L}$ and a suborbit representative of R_k. If the multiplicity of k in the cycle structure of U is exactly 1, then there is no other member of the list which is an element of the same $(s{+}1)$-step orbit as U.*

Proof The multiplicity of k in the cycle structure of U is 1; therefore, R_k is the only element of O_k that contains U as a maximal subgroup. Assume that $U\alpha^*$ is in the list, where α^* is an extended automorphism of G. Lemma 2.2 shows that U and $U\alpha^*$ have the same cycle structure. Therefore, $U\alpha^*$ is a maximal subgroup of R_k and $R_k\alpha^*$. But the multiplicity of k in the cycle structure of $U\alpha^*$ is exactly 1 showing that $R_k = R_k\alpha^*$. Hence, α is an element of the stabiliser of R_k and it follows that U and $U\alpha^*$ are elements of the same suborbit of R_k. Thus, $U\alpha^* = U$. □

The above lemma shows that possible duplications can occur only when there are $(s{+}1)$-step allowable subgroups, $U_1, \ldots, U_y$, in the list that satisfy the following conditions:

(i) all are representatives of suborbits of some R_k;

(ii) each has the same cycle structure;

(iii) each is contained in exactly m allowable subgroups from O_k where $m > 1$.

Possible duplications that arise in this case can be removed by calculating automorphisms of G whose extensions to G^* map these m allowable subgroups to the representative, R_k, of O_k.

Let U_i be an element of $\{U_1, \ldots, U_y\}$ and let $M_1, \ldots, M_m$ be the s-step allowable subgroups from O_k that contain U_i. Note that one of these m subgroups, say M_1, is R_k. Since M_j and R_k are elements of the same orbit, for each j there exists an automorphism, γ_{ij}, of G whose extension, γ_{ij}^*, maps M_j to R_k.

The image of U_i under the action of each of the $m-1$ automorphisms, γ_{ij}^* where $j \neq 1$, is now calculated. If U_i is mapped to the suborbit having representative U_l under the action of any of these automorphisms, then U_i and U_l are elements of the same (s+1)-step orbit and their suborbits lie in the same (s+1)-step orbit.

A maximum of $(m-1) \times y$ automorphisms are calculated and the images of the U_is determined. When these calculations have been completed, all of the suborbits that were found to lie in the same (s+1)-step orbit are fused together to form a set of maximal subgroups; this set is called a *fused suborbit.* One of the U_is in the fused suborbit is chosen as its representative. In order to simplify the notation of Lemma 2.5, if the suborbit having representative U_i for $i \in \{1, \ldots, y\}$ does not fuse with any other suborbit, then the suborbit of U_i is regarded as its fused suborbit.

Representatives of the fused suborbits are now selected to give, after suitable renumbering of the elements, a set $\{U_1, \ldots, U_x\}$ where $1 \leq x \leq y$.

Let U_i be an element of $\{U_1, \ldots, U_x\}$ and let M_j be an s-step allowable subgroup from O_k that contains U_i. A particular automorphism γ_{ij} has been calculated which satisfies the following conditions: the representative of the fused suborbit containing $U_i\gamma_{ij}^*$ is U_i and $M_j\gamma_{ij}^* = R_k$.

Lemma 2.5 *No two of* $U_1, \ldots, U_x$ *are elements of the same* (s+1)*-step orbit.*

Proof Assume that U_i and U_l are elements of the same (s+1)-step orbit. Then there exists an extended automorphism α^* of G such that $U_i\alpha^* = U_l$. Under the action of

α^*, R_k is mapped onto an s-step allowable subgroup M that contains U_l. From the previous calculations, a particular automorphism γ has been obtained whose extension γ^* maps M to R_k and γ^* also maps U_l to an element of its fused suborbit. It follows that $R_k\alpha^*\gamma^* = R_k$ and, therefore, $\alpha\gamma$ is in the stabiliser of R_k. The suborbits of R_k were computed under the action of the stabiliser of R_k. Hence, $U_i\alpha^*\gamma^*$ is an element of the same suborbit as U_i. But $U_i\alpha^*\gamma^* = U_l\gamma^*$ is in the same fused suborbit as U_l. Therefore, U_i and U_l are elements of the same fused suborbit. Hence, by the choice of $\{U_1, \ldots, U_x\}$, $U_l = U_i$. □

If there are other suborbit representatives that satisfy conditions (i) to (iii) given above, they must be processed similarly. When all of these cases have been processed, the resulting list contains one representative of each (s+1)-step orbit.

Let U be both a member of this list and a representative of a suborbit of some R_k. The calculation of the stabiliser of U, viewed as an (s+1)-step allowable subgroup, is now discussed. As a first step, the subgroup of the stabiliser of R_k that stabilises U is computed. This subgroup, $S(U)$, is called the *suborbit stabiliser* of U.

If the multiplicity of k in the cycle structure of U is exactly one, then the proof of Lemma 2.4 shows that the suborbit stabiliser of U equals the stabiliser of U.

The case where the multiplicity, m, of k in the cycle structure of U is greater than one is now considered. First, some notation is established. Let $M_1, \ldots, M_m$ be the s-step allowable subgroups that are elements of O_k and contain U as a maximal subgroup. Let the stabiliser of R_k be denoted by $St(R_k)$.

Let ϕ be an arbitrary element of the stabiliser of U. If ϕ^* fixes R_k, then $\phi \in S(U)$ and has already been obtained. Otherwise, the image $R_k\phi^*$ equals some M_i in $\{M_1, \ldots, M_m\}$, where $M_i \neq R_k$. There exists an automorphism, ψ, of G whose extension maps M_i to R_k. Then $R_k\phi^*\psi^* = R_k$ and $\phi\psi = \theta$ belongs to $St(R_k)$. Thus, $\phi = \theta\psi^{-1}$ and $U\phi^* = (U\theta^*)\psi^{*^{-1}} = U$. Since $\theta \in St(R_k)$, it follows that $U\psi^* = U\theta^*$ is in the same suborbit as U. Hence, there exists an automorphism ζ that is an element of $St(R_k)$ and satisfies $U\psi^*\zeta^* = U$. Thus, $\psi\zeta$ is an element of the stabiliser of U. Clearly, $R_k\phi^*\psi^*\zeta^* = R_k$. It follows that $\phi\psi\zeta$ is an element of $St(R_k)$ and, since it stabilises U, $\phi\psi\zeta$ is also an element of $S(U)$. Hence, $S(U)\phi = S(U)\zeta^{-1}\psi^{-1}$. Therefore, ϕ and $\zeta^{-1}\psi^{-1}$ are elements of the same coset of $S(U)$.

Using these results, a method can now be described for computing a set of automorphisms of G that together with $S(U)$ generates the stabiliser of U. For each $M_i \in \{M_2, \ldots, M_m\}$, compute an automorphism, ψ, of G whose extension maps M_i to R_k. Now compute the image, $U\psi^*$. If $U\psi^*$ is an element of the same suborbit as U, then compute an automorphism ζ that is contained in the stabiliser of R_k and satisfies $U\psi^*\zeta^* = U$. Then $\psi\zeta$ is an element of the stabiliser of U. The automorphisms obtained in this way together with the suborbit stabiliser generate the stabiliser of U.

The length of an $(s+1)$-step orbit can be computed once the order of the stabiliser of its representative has been determined.

The above discussion is now summarised by listing the remaining steps of the extended algorithm.

2. Let $\mathcal{L}$ be the list obtained by choosing a representative of each suborbit of allowable subgroups. For each member U of $\mathcal{L}$, write down the s-step allowable subgroups that contain U as a maximal subgroup and compute the cycle structure of U.

3. Use Lemma 2.3 to eliminate duplications from $\mathcal{L}$. Lemmas 2.2 and 2.4 may show that certain members of the list are elements of distinct $(s+1)$-step orbits.

4. Each subgroup, U, of a set whose elements satisfy conditions (i) to (iii) given above is processed in turn. For each of the $m-1$ subgroups that are elements of O_k, contain U as a maximal subgroup, and are not R_k, find an automorphism of G whose extension maps the subgroup to R_k. Use the $m-1$ automorphisms to check possible fusion of the suborbits in order to obtain a representative of each $(s+1)$-step orbit.

5. Calculate the stabiliser of each representative by first determining the suborbit

stabiliser of the representative and then calculating any additional generators that are required.

6. For each representative, factor G^* by the allowable subgroup to obtain a reduced p-covering group.

In applying the extended algorithm, it has been assumed that the following information on the s-step orbits is available:

(a) the s-step orbit representatives and their stabilisers;

(b) the representatives of the s-step orbits that contain particular s-step allowable subgroups;

(c) automorphisms that map particular s-step allowable subgroups to their orbit representatives.

The s-step orbits, their representatives, and the stabilisers of the representatives can be computed when the extended algorithm is being applied or the results of previous computations can be used. The required automorphisms are computed when applying the extended algorithm. In iterating the extended algorithm to compute the orbits of $(s+2)$-step allowable subgroups, it would be necessary to obtain the additional information listed above for the $(s+1)$-step orbits.

Each reduced p-covering group and its stabiliser are now input to either the basic or to the extended algorithm. The choice of algorithm depends on the permutation group degrees that arise in processing the reduced p-covering groups. The largest degrees that arise at the second intermediate stage of calculations for (1^6) and (1^5) are 2^{12} and 2^{15}, respectively; therefore, the standard implementation was used to complete the calculations.

3 An implementation of the extended algorithm

Much of the standard implementation can be used in implementing the steps of the extended algorithm. The problem of iterating the extended algorithm has not been addressed. As a consequence, it is assumed that the orbits of the s-step allowable subgroups and the stabilisers of the representatives of these orbits have been calculated using the standard implementation.

The orbits of the maximal subgroups of an s-step orbit representative are first computed. Let R_k be an s-step orbit representative relative to the characteristic subgroup C/R^*; then R_k is a subgroup of rank $t-s$. An option has been provided in the standard implementation which allows a user to specify the generators of R_k. Let α be a generator of the stabiliser of R_k. An extended automorphism α^* is computed and the automorphism matrix A_{α^*}, which represents the action of α^* on the p-multiplicator of G, is assembled. The action of α^* on a generator of R_k can be obtained by adding appropriate multiples of rows of A_{α^*} and selecting a particular submatrix from the result. Thus, a $(t-s) \times (t-s)$ automorphism matrix can be computed which describes the action of the extended automorphism on the generators of R_k.

The techniques outlined in O'Brien (1990, §3.3) are used to describe the maximal subgroups of R_k. The supplied generators of R_k provide a fixed basis for R_k and definition sets for its maximal subgroups can be calculated relative to this fixed basis. Each maximal subgroup can be viewed as the kernel of a linear transformation from R_k, viewed as a space of dimension $t-s$, to its definition set, a space of dimension one. The matrix of the linear transformation is a $1 \times (t-s)$ matrix and provides a standard matrix for the maximal subgroup. A label for each standard matrix can be computed. The permutations of the subgroups induced by the extended automorphisms, the suborbits, and the suborbit stabiliser of each suborbit representative can be computed using the standard implementation.

The cycle structure for each suborbit representative is now computed. The s-step orbit representative, R_k, is represented by an $s \times t$ standard matrix. Its suborbit representatives are subgroups of rank $t-s-1$ which are represented by $1 \times (t-s)$ matrices. Let U be a suborbit representative of R_k. Its $1 \times (t-s)$ matrix is extended to a $1 \times t$ matrix by inserting s entries, all zero, at the beginning of each row of the matrix. An $(s+1) \times t$ matrix is now written down where the $s \times t$ standard matrix representing R_k forms the first s rows of the matrix and the $1 \times t$ matrix forms row $s+1$ of the matrix. Left echelonisation of this matrix gives the standard matrix, S, for the (s+1)-step allowable subgroup U.

The v subgroups of rank $t-s$ that contain U can now be calculated using elementary linear algebra. Certain $s \times t$ matrices are obtained by taking linear combinations of rows of S. The standard matrices of the subgroups are obtained by left echelonisation of these matrices. For example, the standard matrix of one of these subgroups is obtained by taking the matrix consisting of the first s rows of S. After echelonising the $s \times t$ matrix obtained, the label of the s-step allowable subgroup is calculated.

Thus, the standard matrix of each (s+1)-step allowable subgroup, U, in the list $\mathcal{L}$ is first computed. Using this matrix, the labels of the v subgroups of rank $t-s$ that contain U are then calculated. These labels are used to determine the cycle structure of U. Since complete information on the s-step orbits is available, the cycle structure of U is found by looking up which orbits contain the labels.

Lemma 2.3 may now be used to eliminate certain duplications from the list. Lemmas 2.2 and 2.4 may show that certain members of the list are elements of distinct (s+1)-step orbits.

In general, a number of possible duplications remain in the list. Let $U_1, \ldots, U_x$ be suborbit representatives that satisfy conditions (i) to (iii) of Section 2. Let U_i be one of these suborbit representatives and let $M_1, \ldots, M_m$ be the s-step allowable subgroups that contain U_i. For each M_j, an automorphism of G is calculated whose extension maps M_j to R_k. In order to compute such an automorphism, the orbit of R_k is built up systematically until M_j has been obtained as an image in this orbit. An automorphism that maps M_j to R_k can now be calculated.

The permutations of the maximal subgroups induced by the extensions of these automorphisms are now computed. Since each permutation is stored in image form, the image of U_i under the action of an extended automorphism can be found by looking up the appropriate entry in the array used to store the permutation induced by this automorphism. This information is used to eliminate any remaining duplications from the list.

The suborbit stabiliser of each member of the list is calculated at the same time as the suborbits are computed. When a representative of each $(s{+}1)$-step orbit has been obtained, the additional generators (if any) of the stabiliser of the representative are then calculated. An automorphism that maps a particular element of an orbit to the representative of this orbit can be calculated by building up the orbit systematically, as mentioned above. The permutations of the maximal and s-step allowable subgroups induced by the extension of such an automorphism can be computed readily using the standard implementation.

4 An application of the extended algorithm

The extended algorithm is now used to calculate the orbits of 2-step allowable subgroups relative to a characteristic subgroup in the 2-multiplicator of (1^6). A consistent power-commutator presentation for the 2-covering group of (1^6) is

$$\begin{aligned}\{\ a_1,\ldots,a_{27}\ \ :\ \ & [a_2,a_1]=a_7, [a_3,a_1]=a_8, [a_3,a_2]=a_9, [a_4,a_1]=a_{10}, [a_4,a_2]=a_{11},\\ & [a_4,a_3]=a_{12}, [a_5,a_1]=a_{13}, [a_5,a_2]=a_{14}, [a_5,a_3]=a_{15}, [a_5,a_4]=a_{16},\\ & [a_6,a_1]=a_{17}, [a_6,a_2]=a_{18}, [a_6,a_3]=a_{19}, [a_6,a_4]=a_{20}, [a_6,a_5]=a_{21},\\ & a_1^2=a_{22}, a_2^2=a_{23}, a_3^2=a_{24}, a_4^2=a_{25}, a_5^2=a_{26}, a_6^2=a_{27}\ \}\end{aligned}$$

where the relations whose right-hand sides are trivial are not shown.

Both the 2-multiplicator and the nucleus of (1^6) have rank 21. The smallest, characteristic, initial segment subgroup in the 2-multiplicator is the intersection of the commutator subgroup of the 2-covering group of (1^6) with the 2-multiplicator of (1^6);

this subgroup has rank 15. We begin by applying Case II of the algorithm described in O'Brien (1990, §4). At the first stage of the calculations, s' runs from 0 to 2. When s' equals 0 or 1, the standard implementation can be used to calculate the orbits of relative allowable subgroups. As noted earlier, for $s' = 2$, the number of allowable subgroups relative to the characteristic subgroup is 178 940 587.

The number of 1-step allowable subgroups relative to the characteristic subgroup is 32 767. For each 1-step orbit, Table 1 lists a representative and the orbit length.

Orbit	Representative	Length
1	1	651
2	7	18 228
3	593	13 888

Table 1: Summary of 1-step orbits of (1^6) relative to chosen characteristic subgroup

The 1-step allowable subgroups having labels 1, 7 and 593 are, respectively, $\langle a_8, \ldots, a_{21} \rangle$ $\langle a_8,\, a_7a_9,\, a_7a_{10},\, a_{11},\, a_{12}, \ldots, a_{21} \rangle$ and

$$\langle\, a_8,\, a_9,\, a_{10},\, a_{11},\, a_7a_{12},\, a_{13},\, a_7a_{14},\, a_{15},\, a_{16},\, a_7a_{17},\, a_{18},\, a_{19},\, a_{20},\, a_{21} \,\rangle\,.$$

Their stabilisers have orders 30 965 760, 1 105 920 and 1 451 520. Each allowable subgroup has 16 383 maximal subgroups; all of these are 2-step allowable subgroups since the chosen characteristic subgroup, C/R^*, is contained in the nucleus.

The orbits of the maximal subgroups are now computed under the actions of the stabilisers. The results of these computations are summarised in Table 2 where the representatives of suborbits are listed by giving their labels relative to the basis of the allowable subgroup; the suborbit lengths are also listed. Thus, 24 is an upper bound on the number of 2-step orbits relative to C/R^*.

Each suborbit representative is represented by a 1×14 matrix; this matrix is extended to a 1×15 matrix by inserting a zero as the first entry in each row. Each representative is a maximal subgroup of three 1-step allowable subgroups. These are chosen as follows: the 1-step orbit representative, the 1-step allowable subgroup represented by the 1×15 matrix, and the allowable subgroup whose standard matrix is obtained by left echelonisation of the sum of these two matrices. Table 2 gives the cycle structure of each of the 24 suborbit representatives.

Thus, 9 is a lower bound on the number of 2-step orbits. Using Lemma 2.3, the upper bound on the number of 2-step orbits can be reduced to 15.

A 2-step allowable subgroup will be referenced by a vector of length 2: the first entry of the vector is a 1-step orbit representative and the second entry is a suborbit representative.

Lemmas 2.2 and 2.4 show that the subgroups $(1,1)$, $(1,4)$, $(1,9)$, $(1,25)$, $(1,297)$, $(1,1153)$, $(7,297)$, $(7,4102)$, and $(593,583)$ are elements of distinct 2-step orbits. The possible duplications remaining in the list are given in Table 3, where they are organised by cycle structure.

Consider the automorphisms, α_1 and α_2, of (1^6) given below in image form:

$$\begin{array}{llll}
\alpha_1 : & a_1 & \longmapsto & a_1a_2a_3a_4a_6 \ , \\
 & a_2 & \longmapsto & a_5a_6 \\
 & a_3 & \longmapsto & a_2a_4a_6 \\
 & a_4 & \longmapsto & a_1a_2 \\
 & a_5 & \longmapsto & a_2 \\
 & a_6 & \longmapsto & a_2a_4
\end{array}
\qquad
\begin{array}{llll}
\alpha_2 : & a_1 & \longmapsto & a_1a_3a_4a_5 \\
 & a_2 & \longmapsto & a_5 \\
 & a_3 & \longmapsto & a_4a_5 \\
 & a_4 & \longmapsto & a_6 \\
 & a_5 & \longmapsto & a_2a_3a_6 \\
 & a_6 & \longmapsto & a_3a_6 \ .
\end{array}$$

The 2-step allowable subgroup $(7,4097)$ is mapped under α_1^* to $(7,385)$ and α_2^* maps $(7,385)$ to $(7,4097)$. Therefore, the suborbits of 7 having representatives 385 and 4097 fuse. No automorphisms were found that fuse any of the four suborbits whose representatives have cycle structure (2^3); hence, the four allowable subgroups are elements of distinct 2-step orbits. Thus, the number of 2-step orbits relative to C/R^* is 14.

Recall from Section 2 that Lemma 2.3 is applied by deleting those members of the list, $\mathcal{L}$, that are suborbit representatives of some R_k and have cycle structures containing an occurrence of some j where $j < k$. An alternative application of this

1-step orbit rep	Suborbit rep	Suborbit length	Cycle structure
1	1	45	(1^3)
	4	210	(12^2)
	9	560	$(1^2 2)$
	25	5040	(12^2)
	297	3360	(13^2)
	1153	7168	(123)
7	1	15	(12^2)
	2	10	$(1^2 2)$
	6	6	(2^3)
	17	360	(12^2)
	21	1080	(2^3)
	289	1440	(2^3)
	297	1440	(23^2)
	385	3840	$(2^2 3)$
	4097	3840	$(2^2 3)$
	4098	2560	(2^3)
	4102	1536	(23^2)
	4417	256	(123)
593	1	315	(13^2)
	4	3780	(23^2)
	9	336	(123)
	12	5040	$(2^2 3)$
	77	4032	(23^2)
	583	2880	(3^3)

Table 2: The cycle structures and orbit lengths of the suborbit representatives

Cycle structure	2-step allowable subgroups
(2^3)	$(7,6)$ $(7,21)$ $(7,289)$ $(7,4098)$
$(2^2 3)$	$(7,385)$ $(7,4097)$

Table 3: Possible duplications remaining in the list

lemma is now described. Select all suborbit representatives having the same cycle structure in which there are at least two distinct s-step orbit indices. Assume that among these representatives there is one, say U, that is a suborbit representative of some R_l and the multiplicity of l in its cycle structure is exactly 1. In practice, it is sensible to retain U as a member of $\mathcal{L}$ and to delete from $\mathcal{L}$ all other members having the same cycle structure as U. Lemma 2.4 now shows that no other member of the resulting list is an element of the same $(s+1)$-step orbit as U and, in addition, the suborbit stabiliser of U equals its stabiliser. As an illustration, the second of the possible duplications given in Table 3 could have been removed by retaining $(593, 12)$ as a member of $\mathcal{L}$ and deleting $(7, 385)$ and $(7, 4097)$.

A summary of the 2-step orbits is given in Table 4. Recall that each 2-step allowable subgroup is represented by a vector where the first entry of the vector is a 1-step orbit representative and the second entry is a suborbit representative. The length of its 2-step orbit divides the product of the lengths of the orbits containing these entries. This is indicated in the table where the listed divisor is the index of the suborbit stabiliser in the stabiliser of a representative.

Kepert (1983) used some special purpose programs to calculate the lengths of these orbits. The lengths obtained from his calculations agree with those listed in Table 4 in all but one case - orbit 14 which he claims has length 9 332 736. Some results of Ferguson (1946) can be interpreted to show that the number of 2-step orbits relative to the corresponding subgroup is also 14 when the prime is odd.

Orbit	Representative	Length		
1	(1, 1)	$651 \times 45/3$	=	9765
2	(1, 4)	651×210	=	136 710
3	(1, 9)	$651 \times 560/2$	=	182 280
4	(1, 25)	651×5040	=	3 281 040
5	(1, 297)	651×3360	=	2 187 360
6	(1, 1153)	651×7168	=	4 666 368
7	(7, 6)	$18\,228 \times 6/3$	=	36 456
8	(7, 21)	$18\,228 \times 1080/3$	=	6 562 080
9	(7, 289)	$18\,228 \times 1440/3$	=	8 749 440
10	(7, 297)	$18\,228 \times 1440$	=	26 248 320
11	(7, 385)	$18\,228 \times 3840$	=	69 995 520
12	(7, 4098)	$18\,228 \times 2560/3$	=	15 554 560
13	(7, 4102)	$18\,228 \times 1536$	=	27 998 208
14	(593, 583)	$13\,888 \times 2880/3$	=	13 332 480

Table 4: Summary of 2-step orbits of (1^6) relative to chosen characteristic subgroup

5 Summary of group determinations

Table 5 summarises the results of the determination of the groups of order dividing 256. For each $n \in \{1, \ldots, 8\}$ and for each relevant $d \in \{1, \ldots, 8\}$, it lists the number of d-generator groups of order 2^n. It also lists the number of capable d-generator groups of order 2^n.

Using the work of G. Higman (1960), bounds on the number of p-groups of a fixed order having class 2 can be calculated. The lower bound obtained for the number of groups of order 256 having class 2 is 23 640 and the upper bound is about 9.4×10^{11}. In fact, 30 078 of the groups of order 256 have class 2.

A lower bound on the number of groups of order 512 can be obtained by using these techniques to calculate lower bounds on the number of *d*-generator class 2 groups of this order. The results of these calculations are summarised in Table 6.

d	Lower bound
4	5417
5	5 716 605
6	2 723 430
7	73

Table 6: Lower bound on number of *d*-generator class 2 groups of order 512

In addition, there is one 3-generator and twelve 8-generator class 2 groups of order 512 showing that there are at least 8 445 538 groups having class 2 and order 512.

6 Providing access to the results

A library, GPS256, containing descriptions of the 56 092 groups of order 256 is distributed with each of the computational group theory systems, CAYLEY and GAP. For descriptions of these systems, see Cannon (1984) and Nickel, Niemeyer & Schönert (1988), respectively. In both organisation and storage techniques, these libraries are modelled on the library TWOGPS, which is described in Newman & O'Brien (1989). The total storage requirement for the group descriptions is about 2 MB. The average time taken to set up a power-commutator presentation for a group of order 256 is about 0.5 seconds of CPU time on a VAX 8700. The anticipated development of database facilities within the CAYLEY system will be a critical factor in providing easy access within that environment to the group descriptions. The material is also available for use with other systems.

Acknowledgement

This work formed part of my Ph.D., which was obtained from the Institute of Advanced Studies, Australian National University, Canberra. I thank my supervisor, Dr M.F. Newman, for many helpful discussions on its contents.

References

John J. Cannon (1984), "An Introduction to the Group Theory Language, Cayley", *Computational Group Theory* (Durham, 1982), pp. 145-183. Academic Press, London, New York.

William Allen Ferguson (1946), "On the Classification of Finite Metabelian Groups with Six Generators", Ph.D. thesis, University of Illinois (Urbana).

Graham Higman (1960), "Enumerating p-groups. I: Inequalities", *Proc. London Math. Soc.* (3) **10**, 24-30.

Rodney James, M.F. Newman & E.A. O'Brien (1990), "The groups of order 128", *J. Algebra* **129** (1), 136-158.

Jeff Kepert (1983), "The Enumeration of Groups of Prime Power Order", B.Sc. thesis, University of Western Australia.

M.F. Newman (1977), "Determination of groups of prime-power order", *Group Theory* (Canberra, 1975), pp. 73-84. Lecture Notes in Math. **573**. Springer-Verlag, Berlin, Heidelberg, New York.

M.F. Newman & E.A. O'Brien (1989), "A CAYLEY library for the groups of order dividing 128", *Group Theory* (Singapore, 1987), pp. 437-442. Walter de Gruyter, Berlin, New York.

M.H.A. Newman (1951), "The influence of automatic computers on mathematical methods", *Manchester University Computer Inaugural Conference*, pp. 13-15.

Werner Nickel, Alice Niemeyer & Martin Schönert (1988), GAP – *Getting started and Reference Manual*, Lehrstuhl D für Mathematik, Aachen.

E.A. O'Brien (1990), "The p-group generation algorithm", *J. Symbolic Comput.* **9**, 677-698.

E.A. O'Brien

Mathematics Research Section

School of Mathematical Sciences

Australian National University

GPO Box 4, ACT 2601

Prepared on July 13, 1989