COSET ENUMERATION OF GROUPS GENERATED BY SYMMETRIC SETS OF INVOLUTIONS

MOHAMED SAYED

Received 4 June 2005 and in revised form 9 October 2005

All non-abelian finite simple groups can be symmetrically generated by involutions. An algorithm which performs coset enumeration for a group defined in this manner on the cosets of a subgroup of automorphisms of these involutions is presented.

1. Introduction

The well-known Todd-Coxeter algorithm [14], which may be viewed as a means of constructing permutation representations of finitely presented groups, remains a primary reference for coset enumeration programs. All the strategies and variants of this algorithm perform essentially the same calculations as the original algorithm, merely choosing different orders in which to process the available information. A statement of the basic technique and the early study appear in [7, 8]. A detailed survey and comparison of different strategies are given in [2]. A contemporary work is described in [6, 9].

In more recent work, see [11, 12], we developed two related algorithms for enumerating single and double cosets of any group generated by a finite conjugacy class of involutions. Several finite groups, including all non-abelian finite simple groups, can be *symmetrically generated* by involutions. Curtis showed how various sporadic simple groups can be so generated, see for instance [4].

The enumerator described in this paper, which can still be viewed as another variant of the Todd-Coxeter algorithm, has substantial improvements (for space, speed, and simplicity of programming) to the version described in [11]. In particular, the additional algebraic information, in the form of coset stabilizing subgroups, is not needed.

2. Involutory symmetric generation of groups

Let G be a group and let $T = \{t_0, t_1, \ldots, t_{n-1}\}$ be a set of elements of order m in G. Making the definitions $T_i = \langle t_i \rangle$ and $\overline{T} = \{T_0, T_1, \ldots, T_{n-1}\}$ allows us to define $N = \mathcal{N}_G(\overline{T})$, the set normalizer in G of $\overline{T}$. We say that T is a *symmetric generating set* for G if the following two conditions hold:

(i) $G = \langle T \rangle$,

(ii) N permutes $\overline{T}$ transitively.

International Journal of Mathematics and Mathematical Sciences 2005:23 (2005) 3739–3750
DOI: 10.1155/IJMMS.2005.3739

We call N the *control subgroup*. Conditions (i) and (ii) imply that G is a homomorphic image of the *progenitor*

$$m^{*n} : N, \tag{2.1}$$

where m^{*n} represents a free product of n copies of the cyclic group C_m and N is a group of automorphisms of m^{*n} which permutes the n cyclic subgroups by conjugation. For further information about the symmetric generations of groups the reader is referred to [4, 5, 10].

Since in this paper we are only concerned with involutory symmetric generators, we restrict our attention to the case $m = 2$ (while N will simply act by conjugation as permutations of the n involutory symmetric generators).

Theorem 2.1. *All finite non-abelian simple groups can arise as finite homomorphic images of progenitors of the form* $2^{*n} : N$, *where* N *is a transitive subgroup of the symmetric group* S_n.

Proof. Let H be a maximal subgroup of a finite simple group G. Suppose that $1 \neq \mathbf{t} \in G$, $\mathbf{t}^2 = 1$. Under the subgroup H, $\mathbf{t}^G$, the conjugacy class of $\mathbf{t}$ in G, splits into orbits as

$$\mathbf{t}^G = \mathcal{T}_1 \dot{\cup} \mathcal{T}_2 \dot{\cup} \cdots \dot{\cup} \mathcal{T}_r. \tag{2.2}$$

Without loss of generality, we may assume that $\mathcal{T}_1 = \{\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{n-1}\}$ is not a subset of H. It is clear that

$$\mathcal{N}_G(\langle \mathcal{T}_1 \rangle) \geq \langle H, \mathcal{T}_1 \rangle = G, \tag{2.3}$$

since H is maximal in G and $\mathcal{T}_1$ is not a subset of H. Therefore,

$$1 \neq \langle \mathcal{T}_1 \rangle \lhd G, \tag{2.4}$$

and, since G is simple, we have

$$\langle \mathcal{T}_1 \rangle = G. \tag{2.5}$$

Moreover, if $\pi \in H$ and $\mathbf{t}_i^\pi = \mathbf{t}_i$ $(i = 0, 1, \ldots, n-1)$, then $\pi \in \mathcal{Z}(G)$ and so $\pi = 1$, that is, H permutes the elements of $\mathcal{T}_1$ faithfully (and transitively). Now, let 2^{*n} denote a free product of n copies of the cyclic group C_2 with involutory generators $t_0, t_1, \ldots, t_{n-1}$ and let $N \cong H$ consist of all automorphisms of 2^{*n} which permute the t_i as H permutes the $\mathbf{t}_i$:

$$\pi^{-1} t_i \pi = t_i^\pi = t_{\pi(i)} \quad \text{for } \pi \in N. \tag{2.6}$$

Then, clearly G is a homomorphic image of $2^{*n} : N$, a split extension of 2^{*n} by the permutation automorphisms N. □

Since the progenitor is a semidirect product (of $\langle T \rangle$ with N), we may use the equation

$$t_i \pi = \pi t_i^\pi = \pi t_{\pi(i)} \tag{2.7}$$

or $i\pi = \pi i^{\pi}$ as we will more commonly write (see below), to gather the elements of N over to the left. We thus have

$$2^{*n} : N = \{\pi w \mid \text{where } \pi \in N,\ w \text{ is a word in the } t_i\}. \tag{2.8}$$

Indeed, this representation is unique provided w is simplified so that adjacent symmetric generators are distinct. Thus any additional relation by which we must factor the progenitor to obtain G must have the form

$$\pi w(t_0, t_1, \ldots, t_{n-1}) = 1 \qquad \text{or} \qquad \pi = w(t_0, t_1, \ldots, t_{n-1}), \tag{2.9}$$

where $\pi \in N$ and w is a word in T. Another consequence of this is that a relation of the form $(\pi t_i)^n = 1$ for some $\pi \in N$ in a permutation progenitor becomes

$$\pi^n = t_i t_{\pi(i)} \cdots t_{\pi^{n-1}(i)}. \tag{2.10}$$

We will allow i to stand for the coset Nt_i, ij for the coset Nt_it_j, and so forth. The coset N is denoted by $*$. We will also let i stand for the symmetric generator t_i when there is no danger of confusion. Thus we write, for instance, $ij \sim k$ to mean $Nt_it_j = Nt_k$ and $ij = k$ to mean $t_it_j = t_k$.

We define the subgroups $N^i, N^{ij}, N^{ijk}, \ldots$ (for i, j, and k distinct) as follows:

$$\begin{aligned} N^i &= \mathcal{C}_N(\langle t_i \rangle), \\ N^{ij} &= \mathcal{C}_N(\langle t_i, t_j \rangle), \\ N^{ijk} &= \mathcal{C}_N(\langle t_i, t_j, t_k \rangle), \end{aligned} \tag{2.11}$$

or, more generally,

$$N^{i_1 i_2 \cdots i_m} = \mathcal{C}_N(\langle t_{i_1}, t_{i_2}, \ldots, t_{i_m} \rangle) \tag{2.12}$$

for $i_1, i_2, \ldots, i_m$ distinct.

It is sometimes useful to have the notation of a *length* of a coset. The fact that for $\pi \in N$ we have

$$Nw(t_i)\pi = N\pi^{-1}w(t_i)\pi = Nw(t_i^{\pi}) = Nw'(t_i), \tag{2.13}$$

shows that all N-cosets have a representative in $\langle T_0 \cup T_1 \cup \cdots \cup T_{n-1} \rangle$. We are in a position to define the length, $L(Nw) = L(w)$, of a coset Nw. Firstly, we have $L(N) = 0$. If Nw has length k and $t \in T$, then Nwt has length at most $k+1$ and has length precisely $k+1$ if it does not have (or has not been proved to have) length at most k. We specify that all cosets of length $k+1$ have the form Nwt where $L(Nw) = k$ and $t \in T$.

3. Coset enumeration algorithm

We describe how a factor group

$$G \cong \frac{2^{*n} : N}{\pi_1 = w_1, \pi_2 = w_2, \ldots, \pi_s = w_s} \tag{3.1}$$

may be identified. We need to establish the order of G by enumerating the cosets of a subgroup (of G) of known order. Naturally, we would like this subgroup to be the control subgroup N.

The coset decomposition of the progenitor $2^{*n} : N$ is

$$2^{*n} : N = N \cup Nt_0 \cup Nt_1 \cup \cdots \cup Nt_{n-1} \cup Nt_0t_1 \cup Nt_0t_2 \cup \cdots \cup Nt_0t_1t_0 \cup \cdots. \tag{3.2}$$

Therefore, the set of right cosets corresponds to the set of all ordered k-tuples, $k \in \{0, 1, 2, \ldots\}$, of the letters of $\{0, 1, 2, \ldots, n-1\}$ which have no adjacent repetitions. We see that the progenitor has 1 coset of length 0 and at most $n(n-1)^{k-1}$ cosets of length k, $k \geq 1$. Once the progenitor is factored by nontrivial relations, coincidences between these cosets appear, and so lead to reduce the number of cosets.

Note that if the Cayley graph of G in its action on the cosets of N has bounded diameter, then the index $|G : N|$ is finite, and the procedure does finish and succeed in finding the permutation representation of the group G. The proof is very similar to the proof of a theorem of Mendelson (see, e.g., [13]) which states that the Todd-Coxeter method will succeed in finding the permutation representation of a group G provided that the index $|G : H|$ is finite, where H is a subgroup of G.

In this section, we show how the algorithm generates cosets and give an efficient method for identifying the coincidences between cosets and for handling the collapses.

3.1. Input to the algorithm. The input to the algorithm begins with the control subgroup N (of G) as a permutation group of degree n. Now Magma [1] and other theoretical packages handle permutations of a high degree with immense ease. The next piece is a finite set of relations, $\pi_i = w_i$, given as two sequences,

$$\pi = [\pi_1, \pi_2, \ldots, \pi_s], \qquad w = [w_1, w_2, \ldots, w_s], \tag{3.3}$$

where the π_i are elements of N and the w_i are sequences of integers from the set $\{0, 1, \ldots, n-1\}$.

3.2. Initialization. It is worth noting that all conjugates (conjugation by elements of N) of the relations $\pi_i = w_i$ are also relations. So that, in any homomorphic image G of the progenitor $2^{*4} : S_4$, the relation $(2,3) = [t_0t_1]^2$ can be considered as $(i, j) = [t_kt_l]^2$ for all distinct i, j, k, l. Thus, if $\sigma = \nu$ is an element of the set of additional relations

$$\{\pi_1 = w_1, \pi_2 = w_2, \ldots, \pi_s = w_s\}, \tag{3.4}$$

then in G we have $\sigma^\pi = \nu^\pi$ for $\pi \in N$.

We point out the procedure which determines a permutation p of N such that, for any two sequences of symmetric generators,

$$u=[a_1,a_2,\dots,a_r],\qquad v=[b_1,b_2,\dots,b_r],\qquad a_i,b_i\in\{0,1,\dots,n-1\},\tag{3.5}$$

$v^p=u$. It can be used (during the processing coincidences step) to establish new emerged relations. We know that

$$N\geq N^{b_1}\geq N^{b_1b_2}\geq\cdots\geq N^{b_1b_2\cdots b_r}.\tag{3.6}$$

Assume that

$$n_1=\left|N:N^{b_1}\right|,\qquad n_i=\left|N^{b_1\cdots b_{i-1}}:N^{b_1\cdots b_i}\right|,\quad i\in\{2,3,\dots,r\}.\tag{3.7}$$

Consequently, there exist transversals

$$\{\tau_1,\dots,\tau_{n_1}\},\ \{\sigma_1,\dots,\sigma_{n_2}\},\ \{\rho_1,\dots,\rho_{n_3}\},\dots,\ \{\phi_1,\dots,\phi_{n_r}\}\tag{3.8}$$

such that

$$\begin{aligned}
N&=N^{b_1}\tau_1\dot\cup N^{b_1}\tau_2\dot\cup\cdots\dot\cup N^{b_1}\tau_{n_1},\\
N^{b_1}&=N^{b_1b_2}\sigma_1\dot\cup N^{b_1b_2}\sigma_2\dot\cup\cdots\dot\cup N^{b_1b_2}\sigma_{n_2},\\
N^{b_1b_2}&=N^{b_1b_2b_3}\rho_1\dot\cup N^{b_1b_2b_3}\rho_2\dot\cup\cdots\dot\cup N^{b_1b_2b_3}\rho_{n_3},\\
&\vdots\\
N^{b_1\cdots b_{r-1}}&=N^{b_1\cdots b_r}\phi_1\dot\cup N^{b_1\cdots b_r}\phi_2\dot\cup\cdots\dot\cup N^{b_1\cdots b_r}\phi_{n_r}.
\end{aligned}\tag{3.9}$$

If $v^p=u$, $p\in N$, then we can find the permutation $p=\phi'\cdots\rho'\sigma'\tau'$, where $\tau'\in\{\tau_1,\dots,\tau_{n_1}\}$, $\sigma'\in\{\sigma_1,\dots,\sigma_{n_2}\}$, $\rho'\in\{\rho_1,\dots,\rho_{n_3}\},\dots,\phi'\in\{\phi_1,\dots,\phi_{n_r}\}$, as follows. Since $\sigma',\rho',\dots,\phi'$ fix b_1, the equation $b_1^p=a_1$ can be reduced to $b_1^{\tau'}=a_1$. Also, the permutations $\rho',\dots,\phi'$ fix b_2, so the equation $b_2^p=a_2$ can be reduced to $b_2^{\sigma'\tau'}=a_2$. Similarly we have $b_3^{\rho'\sigma'\tau'}=a_3$, $\dots$, $b_r^{\phi'\cdots\rho'\sigma'\tau'}=a_r$. Thus, we can easily identify (in a recursive manner) the permutations $\tau',\sigma',\rho',\dots,\phi'$ and consequently p.

The variable *level* stands for the length of the coset corresponding to the last row in the coset tables.

3.3. The tables and the actions. Following the Todd-Coxeter algorithm, we maintain a sequence of sequences C whose terms are the complete set of coset representative words and a table, for each additional relation, which can be considered as a function $f:C\times T\to C$. We read $f(w,t_i)=w'$ as meaning that $Nwt_i=Nw'$ where w and w' are words in the symmetric generators of length k and at most $k+1$, respectively. Also, we apply a consistency condition to our tables that $f(w,t_i)=w'\Leftrightarrow f(w',t_i)=w$, so that inverses have the behavior we expect.

Of course, as we proceed we will discover identifications between cosets that were considered different. So it is convenient to have some way of recording in the sequence C

when a coset w' has been proved to be the same (in G) as an earlier coset w so that references to w' can be diverted to w. We demand that if Nw is earlier in the table than Nw', then $L(Nw) \leq L(Nw')$.

3.4. Pushing relations and processing coincidences. For each additional relation, we start with an empty table and progressively modify it, using the above function, until it represents the permutation action of T on the cosets of N (in G). We will know that we have completed the coset enumeration when the set of right cosets obtained is closed under right multiplication.

During this process, no other representations of group elements are used; any word w in the symmetric generators are simply put into its canonically shortest form by application of the relations (and their conjugates under N). All the relations,

$$\pi_i = w_i, \quad i \in \{1,2,\ldots,s\}, \tag{3.10}$$

where $\pi_i \in N$ and $w_i = t_{i_1} t_{i_2} \cdots t_{i_r}$, together with their conjugates, are written as

$$t_{i_1} t_{i_2} \cdots t_{i_k} = \pi_i t_{i_r} t_{i_{r-1}} \cdots t_{i_{k+1}}, \tag{3.11}$$

where k equals $r/2$ or $(r+1)/2$ according to whether r is even or odd, respectively.

The procedure checks if a part of any given word w in the symmetric generators of length k is equal to $t_{i_1} t_{i_2} \cdots t_{i_k}$, the left-hand side of one of the previous relations, then the procedure replaces this part by $t_{i_r} t_{i_{r-1}} \cdots t_{i_{k+1}}$ and moves the permutation π_i over to the left of the whole word.

If a new word w' of length less than the length of w is obtained, the procedure replaces the coset represented by w by the new coset represented by w'. References to the coset represented by w can be diverted to the coset represented by w'. On the other hand, if a new word w' of length equal to the length of w is obtained, we say that the coset represented by w' has been proved to be the same (in G) as the coset represented by w. In both cases, we wish w' to have t_j as a last letter whenever t_j is the next symmetric generator, in the relation table, to be pushed.

3.5. Processing collapses. From time to time we pack the sequence of the coset representative words, reclaiming the space that was occupied by the redundant elements and this might lead to the collapse of part or the entire coset diagram. During the pushing relations step we may discover identifications between cosets that are considered different from the additional relations (and their conjugates under N). It is convenient to have some way of recording, in a sequence, all of these coincidences, and so we can use them together with the problem relations to rereduce the coset tables. The strategy here is to use the collapse procedure at the end of each *level*. If the coincidences generate further coincidences, the process must be repeated.

3.6. Output of the algorithm. We say that a coset table is closed if it has no cosets in our tables of length greater than *level*. In this case, we say that the set of right cosets obtained is closed under right multiplication. Since N is a finitely generated subgroup of countable index in a finitely presented group G, the point of termination will always be reached.

Table 4.1. The relation table of the enumeration of S_5 over S_4.

	$\overbrace{0 \quad 1 \quad 0}^{(0,1)}$		
$*$	0	$01 \sim 0$	$*$
0	$*$	1	$10 \sim 1$
1	$10 \sim 1$	$*$	0
2	$20 \sim 2$	$21 \sim 2$	$20 \sim 2$
3	$30 \sim 3$	$31 \sim 3$	$30 \sim 3$

The program returns what is essentially a Cayley graph of the action of G on the cosets of N. Each element of G is represented by a permutation of N followed by a word in the symmetric generators. Indeed, the program allows the user readily to pass between the symmetric representation of an element of G and its action on the cosets of N.

4. Illustrative examples

With the observations of the previous section, we are in a position to carry out simple coset enumerations. We will consider the progenitors $2^{*n} : N$, for $N \cong S_3, S_4$ and $L_2(5)$, for $n = 3, 4$, and 6, respectively.

Example 4.1. Consider the group

$$G \cong \frac{2^{*4} : S_4}{(0,1) = t_0 t_1 t_0}, \tag{4.1}$$

which means that the progenitor $2^{*4} : S_4$ quotiented out by the relation $(0,1) = t_0 t_1 t_0$. Here the control subgroup $N \cong S_4$ acts on the 2^{*4} in its normal action on four points.

It is clear that $N = N(0,1) = N t_0 t_1 t_0$, which we write as $* \sim 010$ in our notation. By postmultiplying both sides by t_0, we deduce that $N t_0 = N t_0 t_1$, that is, $01 \sim 0$. In general, we have $* \sim iji$ and thus $ij \sim i$. The relation table for the coset enumeration of G over N is given in Table 4.1.

The symmetric generator t_0 acts on these five cosets by right multiplication as the transposition interchanging the coset $*$ with the coset 0. Since $(*,0)(*,1)(*,0) = (0,1)$, we see that our additional relation is satisfied by these transpositions, and we have a symmetric presentation of S_5.

Example 4.2. Let

$$G \cong \frac{2^{*3} : S_3}{(0,1) = t_0 t_1 t_0 t_1 t_0, (0,2,1) = t_0 t_1 t_2 t_0 t_1}. \tag{4.2}$$

The result of the coset enumeration of G over S_3 is shown in Tables 4.2 and 4.3. Thus, $|G : N| \leq 10$, so $|G| \leq 60 = |L_2(4)|$, and the (relatively) easy task of finding generators for $L_2(4)$ satisfying the required relations completes the identification of G with $L_2(4)$.

Table 4.2. The first relation table of the enumeration of $L_2(4)$ over S_3.

	$\overbrace{0 \quad 1 \quad 0 \quad 1 \quad 0}^{(0,1)}$				
$*$	0	01	010 ~ 01	0	$*$
0	$*$	1	10	101 ~ 10	1
1	10	101 ~ 10	1	$*$	0
2	20	201 ~ 02	020 ~ 02	021 ~ 20	2
01	010 ~ 01	0	$*$	1	10
10	1	$*$	0	01	010 ~ 01
02	020 ~ 02	021 ~ 20	2	21	210 ~ 12
20	2	21	210 ~ 12	121 ~ 12	120 ~ 21
12	120 ~ 21	2	20	201 ~ 02	020 ~ 02
21	210 ~ 12	121 ~ 12	120 ~ 21	2	20

Table 4.3. The second relation table of the enumeration of $L_2(4)$ over S_3.

	$\overbrace{0 \quad 1 \quad 2 \quad 0 \quad 1}^{(0,2,1)}$				
$*$	0	01	012 ~ 10	1	$*$
0	$*$	1	12	120 ~ 21	2
1	10	101 ~ 10	102 ~ 01	010 ~ 01	0
2	20	201 ~ 02	0	$*$	1
01	010 ~ 01	0	02	020 ~ 02	021 ~ 02
10	1	$*$	2	20	201 ~ 02
02	020 ~ 02	021 ~ 20	202 ~ 20	2	21
20	2	21	212 ~ 21	210 ~ 12	121 ~ 12
12	120 ~ 21	2	$*$	0	01
21	210 ~ 12	121 ~ 12	1	10	101 ~ 10

Example 4.3. Let

$$G \cong \frac{2^{*6} : L_2(5)}{\left[(0,1,2,3,4)t_0\right]^4 = 1}. \tag{4.3}$$

Here the $L_2(5)$ acts on the 2^{*6} as the group of linear fractional transformations (of determinant 1) on the projective line of order 5 whose points may be labelled with the elements of $\mathbf{F}_5 \cup \{\infty\}$. The result of the coset enumeration of G over $L_2(5)$ is shown in Table 4.4. It is easy to recognize the group G—in this case the projective general linear group $PGL_2(11)$ of order $22 \times 60 = 1320$—and check that it does contain such a symmetric generating set.

Table 4.4. The relation table of the enumeration of $PGL_2(11)$ over $L_2(5)$.

	$\overbrace{0 \quad 1 \quad 2 \quad 3}^{(0,4,3,2,1)}$			
$*$	0	$01 \sim 32$	3	$*$
∞	$\infty 0 \sim 12$	$121 \sim 212$	$21 \sim \infty 3$	∞
0	$*$	1	$12 \sim 43$	4
1	10	$101 \sim 242$	$24 \sim 03$	0
2	$20 \sim 41$	4	$42 \sim 13$	1
3	$30 \sim 14$	$141 \sim 232$	23	2
4	$40 \sim 21$	2	$*$	3
$\infty 0$	∞	$\infty 1 \sim 23$	$232 \sim 323$	$32 \sim \infty 4$
$\infty 1 \sim 04$	$040 \sim 131$	$13 \sim 42$	4	$43 \sim \infty 0$
$\infty 2 \sim 10$	1	$*$	2	$23 \sim \infty 1$
$\infty 3 \sim 40$	4	$41 \sim 20$	$202 \sim 343$	$34 \sim \infty 2$
$\infty 4 \sim 01$	$010 \sim 101$	$10 \sim \infty 2$	∞	$\infty 3$
0∞	$0\infty 0 \sim 141$	$14 \sim 2\infty$	$2\infty 2 \sim 313$	$31 \sim 4\infty$
$1\infty \sim 03$	$030 \sim 121$	12	1	$13 \sim 0\infty$
$2\infty \sim 30$	3	$31 \sim 02$	0	$03 \sim 1\infty$
$3\infty \sim 20$	2	21	$212 \sim 303$	$30 \sim 2\infty$
$4\infty \sim 02$	$020 \sim 1\infty 1$	$1\infty \sim 24$	$242 \sim 3\infty 3$	3∞
$\infty 0\infty \sim 0\infty 0$	$0\infty \sim 13$	$131 \sim 2\infty 2$	$2\infty \sim 30$	$303 \sim \infty 4\infty$
$\infty 1\infty \sim 020$	$02 \sim 31$	3	32	$323 \sim \infty 0\infty$
$\infty 2\infty \sim 040$	$04 \sim \infty 1$	∞	$\infty 2 \sim 34$	$343 \sim \infty 1\infty$
$\infty 3\infty \sim 010$	01	0	$02 \sim 31$	$313 \sim \infty 2\infty$
$\infty 4\infty \sim 030$	$03 \sim 1\infty$	$1\infty 1 \sim 202$	$20 \sim 3\infty$	$3\infty 3 \sim \infty 3\infty$

We conclude with a computer example of the use of the program.

Example 4.4. Consider the group

$$G \cong \frac{2^{*4} : S_4}{(3,4) = \left[t_1 t_2\right]^2}. \tag{4.4}$$

The input takes the form

$$\begin{aligned} N &:= \text{permutation group } \langle 4 \mid (1,2,3,4),(3,4) \rangle; \\ \pi &:= \left[N!(3,4)\right]; \\ w &:= \left[\left[1,2,1,2\right]\right]. \end{aligned} \tag{4.5}$$

The result of the coset enumeration of G over S_4 shown in Table 4.5 indicates that $|G : N| \leq 14$, so $|G| \leq 336 = |PGL_2(7)|$. In fact, if we make the correspondence between the N-cosets and the 7 points and the 7 lines of the projective plane of order 2, see [10], we can easily identify G with $PGL_2(7)$.

Table 4.5. The relation table of the enumeration of $PGL_2(7)$ over S_4.

		(3,4)		
1	2	1	2	
1	2	6	3	1
2	1	3	6	2
3	6	2	1	3
4	11	14	9	5
5	10	13	7	4
6	3	1	2	6
7	13	10	5	9
8	12	8	12	8
9	14	11	4	7
10	5	9	14	11
11	4	7	13	10
12	8	12	8	12
13	7	4	11	14
14	9	5	10	13

The list of the 14 single cosets together with their equivalent names is as follows:

$$
\begin{aligned}
&[[\,],\\
&[1],[2],[3],[4],\\
&[[12],[21]],[[23],[32]],[[34],[43]],[[24],[42]],[[14],[41]],[[13],[31]],\\
&[[123],[213],[432],[342],[124],[214],[431],[341]],\\
&[[143],[413],[234],[324],[142],[421],[231],[321]],\\
&[[132],[312],[423],[243],[134],[314],[421],[241]]].
\end{aligned}
\tag{4.6}
$$

The action of the element $x = (1,2,3,4)$ on single cosets is given by $xp = (2,3,4,5)(6,7,8,10)(9,11)(12,13)$. Also, the action of our 4 symmetric generators is given as follows:

$$
\begin{aligned}
t_1 &: (1,2)(3,6)(4,11)(5,10)(7,13)(8,12)(9,14),\\
t_2 &: (1,3)(2,6)(4,7)(5,9)(8,12)(10,13)(11,14),\\
t_3 &: (1,4)(2,11)(3,7)(5,8)(6,12)(9,14)(10,13),\\
t_4 &: (1,5)(2,10)(3,9)(4,8)(6,12)(7,13)(11,14).
\end{aligned}
\tag{4.7}
$$

5. Concluding remark

In this enumerator several modifications have been introduced. For instance, rather than applying the additional relations to all cosets in the relation tables, it is more efficient to apply conjugates of the relations to representatives of the cosets. Moreover, the algorithm

Table 5.1. Result of the coset enumeration of G over N.

G	$2^{*n} : N$	Additional relations	Cosets	Time taken (s)
$PGL_2(11)$	$2^{*6} : L_2(5)$	$(0,4,3,2,1) = t_0t_1t_2t_3$	22	0.05
$\mathbf{J}_1$	$2^{*11} : L_2(11)$	$(0,8,1)(2,7,9,x,6,5)$ $(3,4) = t_0t_1t_8t_0t_1$	266	0.20
$\mathbf{G}_2(4) : 2$	$2^{*100} : (\mathbf{J}_2 : 2)$	$\pi_{01} = t_0t_1t_0$	416	0.50
$3^{\cdot}\mathbf{Suz} : 2$	$2^{*416} : (\mathbf{G}_2(4) : 2)$	$\pi_{01} = t_0t_1t_0$	5346	1.40

is different from existing coset enumeration techniques in the way that it handles the elements of the group and for informing the user more about the structure of the group. In addition, the operations of inversion and multiplication can be performed manually (or mechanically) by means of short algorithms. Also, it is helpful to define the group in terms of generators and relations in the standard way; we can find a symmetric generating set for the group and from this generating set we can determine the relations which we need to add to our progenitor presentation.

This implementation, of course, contains a more detailed description which is omitted here for the sake of brevity. It, although written in Magma, can be readily written in any high-level language. Our next aim is to implement the algorithm as a C++ program and introduce more modifications. For example, we will try to find all coincidences between cosets without using relation tables; only by pushing the additional relations (and their conjugates under N).

The program is run on a Sun Sparc Station 5 with CPU clock rate 110 MHz. In Table 5.1, results are given for some symmetric presentations of G, see [10]. For the notation of the group structures, the reader is referred to [3]. A straightforward coset enumeration [1] for each considered group, using the same machine, takes almost the same CPU time.

References

[1] W. Bosma, J. J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[2] J. J. Cannon, L. A. Dimino, G. Havas, and J. M. Watson, *Implementation and analysis of the Todd-Coxeter algorithm*, Math. Comp. **27** (1973), no. 123, 463–490.

[3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups. Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford University Press, Eynsham, 1985.

[4] R. T. Curtis, *Symmetric generation and existence of the Janko group J_1*, J. Group Theory **2** (1999), no. 4, 355–366.

[5] R. T. Curtis and Z. Hasan, *Symmetric representation of the elements of the Janko group J_1*, J. Symbolic Comput. **22** (1996), no. 2, 201–214.

[6] G. Havas, *Coset enumeration strategies*, Tech. Rep. 200, Key Centre for Software Technology, Department of Computer Science, University of Queensland, Queensland, 1991.

[7] J. Leech, *Coset enumeration on digital computers*, Proc. Cambridge Philos. Soc. **59** (1963), 257–267.

[8] ———, *Coset enumeration*, Computational Group Theory (Durham, 1982) (M. D. Atkinson, ed.), Academic Press, London, 1984, pp. 3–18.

[9] S. A. Linton, *The maximal subgroups of the sporadic groups* **Th**, **Fi**24 *and* **Fi**24′ *and other topics*, Ph.D. thesis, University of Cambridge, Cambridge, 1989.

[10] M. Sayed, *Computational methods in symmetric generation of groups*, Ph.D. thesis, University of Birmingham, Birmingham, 1998.

[11] ———, *Coset enumeration algorithm for symmetrically generated groups*, Proceedings of the International Conference on Mathematics and Its Applications (ICMA 2004), Kuwait Univ. Dep. Math. Comput. Sci., Kuwait, 2005, pp. 424–437.

[12] ———, *Double-coset enumeration algorithm for symmetrically generated groups*, Int. J. Math. Math. Sci. **2005** (2005), no. 5, 699–715.

[13] M. Suzuki, *Group Theory. I*, Fundamental Principles of Mathematical Sciences, vol. 247, Springer, Berlin, 1982.

[14] J. A. Todd and H. S. M. Coxeter, *A practical method for enumerating cosets of finite abstract groups*, Proc. Edinburgh Math. Soc. **5** (1936), 26–34.

Mohamed Sayed: Department of Mathematics and Computer Science, Faculty of Science, Kuwait University, P.O. Box 5969, Safat 13060, Kuwait

E-mail address: msayed@mcs.sci.kuniv.edu.kw