Coset enumeration algorithm for symmeterically presented groups

Mohamed Sayed

Dept. of Eng. Mathematics and Physics, Faculty of Eng., Alexandria University, Alexandria 21544, Egypt

The Todd-Coxeter coset enumeration algorithm was perhaps the first non-trivial algorithm from pure mathematics to be programmed for a digital computer. Recently the author has developed a double coset enumeration algorithm for symmetrically presented groups. This paper describes a different algorithm for enumerating the single cosets of a known subgroup in a group that is generated by symmetric set of involutions.

تعتبر طريقة تود وكوكستر المستخدمة في توليد كوستات لزمره جزئيه معلومه في زمره ما احد اهم تطبيقات الرياضيات فـــى
الحاسبات اللاليه في العقد السابق تم تطوير طريقه جديده لتمثيل الزمر بدلالة مجموعه من المولدات المتماثله. هذه الطريقه غلي
جانب انها تعطي تمثيل بسيط للزمر فهي كذلك تعكس التماثل في الزمر. في هذا البحث تم تطويع وتطوير طريقة تود وكوكستر
لتستخدمه في توليد كوستات لزمره جزئيه معلومه في زمره ممثله علي الطريقه المتماثله.

Keywords: Computational group, Coset enumeration, Symmetric presentation, Involution, Progenitor.

1. Introduction

The Todd-Coxeter coset enumeration is one of the most powerful tools of computational group theory. It may be viewed as a means of constructing permutation representations of finitely presented groups. An account of the basic technique appears in [1], and the early history is described in [2]. A detailed survey and comparison of various strategies is given in [3], and more recent work is described in [4].

All the strategies and variants of the algorithm perform essentially the same calculation as the original Todd-Coxeter algorithm, merely choosing different orders in which to process the available information. The double coset enumeration algorithm described in [5], appeared significantly different, but could still be viewed as another variant, one which used additional group-theoretical information to compress the coset table into a smaller space, and used modified procedures to manipulate the compressed table directly.

In [6] Curtis showed that Mathieu group M_{24} can be generated by seven involutions whose set normalizer in M_{24} is isomorphic to the projective special linear group $PSL_2(7)$, which permutes the generators in the natural way. This construction motivated the search for what we call symmetric presentations of groups. Earlier still, work has been done in this area by Campbell [7] in case the control group (in our parlance) is cyclic or the whole symmetric group. Detailed account of symmetric presentations of groups can be found in [5].

These lead to an alternative view of the Todd-Coxeter algorithm itself, as a way of constructing finitely presented permutation representations of groups generated by symmetric sets of involutions.

2. Involutory symmetric generators of a group

The construction given in this section has been taken from our recent work, see [7].

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

$$t^{i} = \mathfrak{I}_1 \dot{\bigcup} \mathfrak{I}_2 \dot{\bigcup} \dots \dot{\bigcup} \mathfrak{I}_r.$$

Without loss of generality, we may assume that $\mathfrak{I}_1 = \{t_0, t_1, \ldots, t_{n-1}\}$ is not a subset of N. It is clear that

$$N_G(<\mathfrak{I}_1>) \geq <N, \mathfrak{I}_1> = G,$$

since N is maximal in G and $\mathfrak{I}_1$ is not a subset of N. Therefore,

$$1 \neq <\mathfrak{I}_1> \lhd G,$$

and, since G is simple, we have

$$<\mathfrak{I}_1> = G.$$

Moreover, if $\pi \in N$ and $t_i^\pi = t_i \, \forall i \in \{0, 1, \ldots, n-1\}$ then $\pi \in \mathbf{Z}(G)$ (the center of G) and so $\pi = 1$, i.e. N permutes the elements of $\mathfrak{I}_1$ 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 $N \cong N$ consist of all automorphisms of 2^{*n} which permute the t_i as N permutes the t_i:

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

Then, clearly G is a homomorphic image of $2^{*n}:N$, a split extension of 2^{*n} by the permutation automorphisms N. In these circumstances we call N the control subgroup, $T = \{t_0, t_1, \ldots, t_{n-1}\}$ a symmetric generating set for G, and $2^{*n}:N$ the progenitor.

Also, to be noted is that, since the Feit-Thompson theorem [8] implies that all non-abelian finite simple groups have even orders, it is quite easy to show that these are images of progenitors of the form 2^{*n}: N.

Since the progenitor is a semi-direct product (of <T> with N), it follows that in any homomorphic image G, we may use the equation:

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

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

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

Each element of the progenitor can be represented as πw, where $\pi \in N$ and w is a word in the symmetric generators. Indeed, this representation is unique provided w is simplified so that adjacent symmetric generators are distinct. Thus any additional relator by which we must factor the progenitor to obtain G must have the form
$\pi w(t_0, t_1, \ldots, t_{n-1})$,

where $\pi \in N$ and w is a word in T.
Notation. In what follows we will let i stand for the coset Nt_i, ij for the coset Nt_it_j and so on. 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 ~ k to mean $Nt_it_j = Nt_k$.

Writing ij = k would be much the stronger statement that $t_it_j = t_k$.

3. Coset enumeration algorithm

When trying to establish the order of a finitely presented group it is necessary to enumerate the cosets of a subgroup of known order. Naturally, we would like this subgroup to be the control subgroup N. In this section we describe how to enumerate the cosets of a control subgroup N in a group G presented by

$$\frac{2^{*n} : N}{\pi_1 w_1, \pi_2 w_2, \ldots, \pi_s w_s}.$$

The input to the algorithm begins with a set of involutory symmetric generators T. The next piece is a finite set R of additional relations (which have the form $w = \pi$).

The algorithm proceeds by manipulating a table for each relator, analogous to the coset tables used in Todd-Coxeter algorithm. If $t_{i_1} t_{i_2} \ldots t_{i_m} = \pi_i$ is a relation in R then its relator table (which has m+1 columns and infinitely

Table 1
The relater table

	i_1	i_2	...	i_m
.	.	.		.
.	.	.		.
.	.	.		.
w_k	$w_k i_1$	$w_{k} i_1 i_2$		$w_k^{\pi_1}$

many rows) contains a row for each coset Nw_k ,see table 1.

In the first row of each relator table we apply the relation to the coset N (which is denoted by *) and in the next n rows we apply the relation to the length one cosets Nt_i, $i \in \{0, 1, \ldots, n-1)$, and so on. It is convenient to set up a multiplication table which shows the effect of each involutory generator on the cosets when multiplied from the right.

Next, the procedure consists of defining new cosets by inserting words in the next available places in the multiplication table. If w is a representative word of the coset Nw, reduce w by replacing any subword v by πu, $\pi = uv^{-1}$ is in R, and move π to the left of w. To do this, we observe that $Nw\pi = Nw^{\pi}$ whenever $\pi \in N$. In addition, the same coset will often have many names and a coincidence (sometimes called collapse) may occur. Thus, it is convenient to have some way of recording in a table when a coset Nw_1 has been proved to be the same (in G) as another coset Nw_2. When we have pushed all the relators to the cosets from the coset multiplication table then the process should have been finished.

This is in fact much simpler than the usual method of pushing a relator in coset enumeration, since we do not need to work backwards through the relator, or make deductions to exactly fill gaps. As a result, many elements are defined and then almost immediately deleted, so that the algorithm does not waste both space and time. Also, it is to be noted that our algorithm is practical in the sense that it can be programmed readily on a computer and results can be obtained in reasonable time.

We can say that if N is of finite index, closure must be reached after finite number of steps (see the proof given in [8]).

4. Two illustrative examples

In this section we give details of how the algorithm is used to find the cosets in groups symmetrically presented. Consider the group G which is presented by

$$\frac{2^{*4}:S_4}{(2,3)=t_0t_1t_0t_1},$$

which means that the progenitor $2^{*4}:S_4$ quotinted out by the relation $(2,3) = [t_0t_1]^2$.

We observe that 01 ~ 10 and that 010 ~ 1. To see this we utilize our extra relation, namely, $(2,3) = t_0t_1t_0t_1$. Thus $N = N(2,3) = Nt_0t_1t_0t_1$, which we write as * ~ 0101, from which, by postmultiplying both sides by t_1, we deduce that $Nt_0t_1t_0 = Nt_1$, that is 010 ~ 1. Furthermore, postmultiplying both sides by t_0 yields $Nt_1t_0 = Nt_0t_1$ which is 01 ~ 10 in our notation.

The enumeration is complete and we have the relation table 2.

Thus, $|G:N| \leq 14$, so $|G| \leq 336 = |PGL_2(7)|$, and the (relatively) easy task of finding generators for the projective linear group $PGL_2(7)$ satisfying the required relations completes the identification of G with $PGL_2(7)$. Also, one can obtain a natural permutation representation of $PGL_2(7)$ on 14 points.

We close with an example that illustrates the effectiveness of the technique when applied to a progenitor that is factored by more than one additional relation. Consider the alternating group A_5 which is symmetrically presented by

Table 2
Problem relation table

0	1	0	1		
*	0	01~10	1	*	
0	*	1	10~01	0	
1	10~01	0	*	1	
2	20	201~310	31	3	201~2(2,3)10~310
3	30	301~210	21	2	301~3(2,3)10~210
10	1	*	0	01~10	
20	2	21	210~301	30	201~2(2,3)10~310
30	3	31	310~201	20	310~3(2,3)01~201
21	210~301	30	3	31	
31	310~201	20	2	21	
32	320	3201~32	320	3201~23	3201~3(1,3)021~1021
210	21	2	20	201~310	~10(0,3)12~1312~32
310	31	3	30	301~210	201~2(2,3)01~310
320	32	321~320	32	321~230	301~3(2,3)10~210
					321~320~230

Table 3
Second problem relation table

0	1	0	1	0	
*	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
Second problem relation table

0	1	2	0	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	021~20
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

$$\frac{2^{*3}:S_3}{(0,l)=t_0t_1t_0t_1t_0,(0,2,l)=t_0t_1t_2t_0t_1}.$$

The progenitor here is 2^{*3}:S_3, where the S_3 acts on 2^{*3} in its permutation action on three points. Following the algorithm described above, we can obtain all costs of S_3 in A_5. All the lines in all tables are closed and we have relation tables 3 and 4.

Note that in the above hand calculation we have tried to work through the algorithm systematically to point out that the hand calculation and the mechanical calculation are almost identical. Our next aim is to give the results of the implementation on a variety of symmetrically presented groups.

References

[1] J. Leech, Coset Enumeration In Computational Group Theory, ed. M. Atkinson, Academic Press, New York, 3-18 (1984).

[2] J. Leech, "Coset Enumeratation on Digital Computers", Proc. Camb. Phill. Soc. Vol. 59, pp. 257-267 (1963).

[3] J.J.Cannon, L. A. Dimino, G. Haves and J. M. Wastson, "Implementation and Analysis of the Todd-Coxeter Algorithm", Math. Comp., Vol. 27, pp. 463-490 (1973).

[4] G. Havas, Coset Enumeration Strategies, University of Queensland, key Center for Software Technology, Technical Report No. 200 (1991).

[5] M. Sayed, Computational Methods in Symmetric Generation of Groups, Ph.D. Thesis Univ. of Birmingham, (1998)

[6] R.T. Curtis, "Natural Constructions of the Mathieu Groups", Proc. Camb. Phill. Soc.,Vol. 106, pp.423-429 (1989).

[7] C.M. Campbell, "Symmetric Presentations and Linear Groups", Contemp. Math., Vol. 45, pp. 33-39 (1985)

[8] M. Suzuki, Group Theory I, Springer Verlag, (1982)

Received July 25, 2000
Accepted October 22, 2000