A NOTE ON THE TODD-COXETER COSET ENUMERATION ALGORITHM

by M. J. BEETHAM and C. M. CAMPBELL

1. Introduction

In (8) Todd and Coxeter described an algorithm for enumerating the cosets of a finitely generated subgroup of finite index in a finitely presented group. Several authors ((1), (2), (5), (6), (7)) have discussed a modification of the algorithm to give also a presentation of the subgroup in terms of the given generators.

In particular, Mendelsohn (7) gives an algorithm requiring two coset enumerations to find such a presentation together with an example to show that one enumeration is insufficient. W. O. J. Moser has conjectured that one enumeration is sufficient and it is the purpose of this note to prove this and to extend the results to subgroups of countable index.

The algorithm to be described is essentially the same as that described by the above authors but is included here in the form in which it has been implemented on the I.B.M. 360/44 computer of the University of St Andrews Computing Laboratory.

We describe the algorithm in two parts, the classical and the additional algorithms. Section 2 describes the algorithms and Section 3 contains proofs of the validity of their operation.

2. The algorithms

Suppose a group is generated by a set of elements $\{x_i \mid i \in I\}$, I a finite set, and suppose that $\{\sigma_k \mid k \in K\}$ is a set of words in the generators x_i and their inverses; then we will use the notation $G = \langle x_i \mid \sigma_k = 1, i \in I, k \in K \rangle$ to mean the group $F/\bar{L}$, where $\bar{L}$ is the normal closure of the group $L = \langle \sigma_k \mid k \in K \rangle$ in the free group $F = \langle x_i \mid i \in I \rangle$.

If $H = \langle \omega_j \mid j \in J \rangle$ is a subgroup of countable index in G, there are only a countable number of cosets of H in G. We first give a systematic method for finding these cosets. We construct a multiplication table for the cosets in which the rows are indexed by the cosets and the columns by the generators of G and their inverses and proceed in the following way:

(i) Denote by the integer 1 the subgroup H. Apply the subgroup generators ω_j to the coset 1 defining new cosets as necessary to obtain $1 . \omega_j = 1$, for all $\in J$.

(ii) Next, for each coset m in turn in the sequence 1, 2, 3, ...,

(a) define the cosets mx_i and mx_i^{-1} for each $i \in I$ unless these have already been defined or found,

(b) apply the relations to the coset m, defining any new cosets which are necessary, to obtain $m\sigma_k = m$ for all $k \in K$.

Note that any new coset defined in (i) and (ii) must be defined as a previously defined coset multiplied either by a generator x_i or the inverse of a generator. Also the relation $mx_i^\varepsilon = n$ implies $nx_i^{-\varepsilon} = m$, where $\varepsilon \in \{-1, 1\}$.

(iii) In addition, a coincidence (sometimes called collapse) may occur. Suppose a relation is $x_1^{\varepsilon_1} x_2^{\varepsilon_2}...x_i^{\varepsilon_i} = 1$ and we apply that relation to the coset n, then coincidence occurs if we obtain $nx_1^{\varepsilon_1} x_2^{\varepsilon_2}...x_j^{\varepsilon_j} = p$, where $1 \leq j \leq i$, and we also have $nx_i^{-\varepsilon_i} x_{i-1}^{-\varepsilon_{i-1}}...x_{j+1}^{-\varepsilon_{j+1}} = q$, that is $nx_1^{\varepsilon_1} x_2^{\varepsilon_2}...x_j^{\varepsilon_j} = q$, for the labels p and q are both attached to the same coset.

Having discovered a coincidence ($q > p$ say) the pth and qth rows of the multiplication table are compared possibly giving further coincidences and then q is replaced everywhere it occurs by p. These further coincidences are processed in the same manner. At the end of the algorithm the cosets can be relabelled by the first available integers.

Suppose the subgroup generator $\omega_j = x_1^{\varepsilon_1} x_2^{\varepsilon_2}...x_i^{\varepsilon_i}$ and we consider $1.\omega_j$, then coincidence may again occur, for we may discover that $1 . x_1^{\varepsilon_1} x_2^{\varepsilon_2}...x_k^{\varepsilon_k} = p$, where $1 \leq k \leq i$ whereas $1 . x_i^{-\varepsilon_i} x_{i-1}^{-\varepsilon_{i-1}}...x_{k+1}^{-\varepsilon_{k+1}} = q$. Thus p and q are both attached to the same coset and we then process the resulting coincidences as above.

Finally, the label chosen for an unknown coset should be the first available natural number. This completes the classical algorithm.

We next give the additional algorithm:

(iv) Define the identity element of the subgroup H to be the coset representative of the coset 1. Whenever a coset n is defined as mx_i^ε, define the coset representative τ_n to be $\tau_m x_i^\varepsilon$, where τ_m is the coset representative of the coset m, and note that $\tau_m x_i^\varepsilon \tau_n^{-1} = 1$.

(v) If, in consideration of a generator ω of H of the form sxt, where s and t are words in the generators of G and x is either a generator or the inverse of a generator of G, it is found that $mx = n$, where m is the coset $1s$ and n is the coset $1t^{-1}$, then note that $\tau_m x \tau_n^{-1} = \alpha^{-1} \omega \beta^{-1}$, where α is a word in the generators of H calculated as $1x_1^{\varepsilon_1} \tau_{i_1}^{-1} \tau_{i_1} x_2^{\varepsilon_2}...\tau_{i_{k-1}} x_k^{\varepsilon_k} \tau_m^{-1}$, where $s = x_1^{\varepsilon_1} x_2^{\varepsilon_2}...x_k^{\varepsilon_k}$ and where β is calculated in a similar way.

(vi) If, in consideration of a relation of G of the form $st = 1$, it is found that $mx = n$, then note that $\tau_m x \tau_n^{-1} = \alpha^{-1} \beta^{-1}$, where α and β are words in the generators of H calculated as in (v).

(vii) If, in consideration of a generator ω of H, no new cosets are defined and no new information about coset multiplication is found, then

$$\prod_{j=0}^{r} (\tau_{i_j} x_{i_{j+1}}^{\varepsilon_{j+1}} \tau_{i_{j+1}}^{-1}) = \omega$$

is a relation between the generators of H, where $\omega = \prod_{j=0}^{r} x_{i_{j+1}}^{\varepsilon_{j+1}}$.

(viii) If, in consideration of a relation σ applied to a coset m, no new cosets are defined and no new information about coset multiplication is found, then

$$\prod_{j=0}^{r} (\tau_{i_j} x_{i_{j+1}}^{\varepsilon_{j+1}} \tau_{i_{j+1}}^{-1}) = 1 \text{ is a relation between the generators of } H, \text{ where}$$

$\sigma = \prod_{j=0}^{r} x_{i_{j+1}}^{\varepsilon_{j+1}}$ and $\tau_{i_0} = \tau_{i_{r+1}}$ is the coset representative of coset m.

(ix) The last occurrence to be considered is the discovery of a coincidence. If, in consideration of a generator of the subgroup, ω_1 say, it is found that ω_1 is of the form st, where $Hs = m$ and $Ht^{-1} = n$, then this gives $\tau_1 s = \omega_s \tau_m$ and $\tau_1 t^{-1} = \omega_t \tau_n$ from which $\tau_n = (\omega_t^{-1} \omega_1^{-1} \omega_s) \tau_m$. This gives the relationship between the coset representatives and again only involves words in the generators of H.

If, in consideration of a relation of G, a coincidence occurs, then a similar result is obtained. A relation of the form $\tau_n g = \omega \tau_l$ becomes $\tau_m g = \omega_t^{-1} \omega_1 \omega_s \omega \tau_l$. If the result $mg = l$ is already known then this gives a further relation in H. Otherwise this is new information resulting from the coincidence. If it is already known that $mg = k$ with $\tau_m g = \omega' \tau_k$ so that the coincidence $l = k$ is obtained, then $\tau_l = \omega^{-1} \omega_s^{-1} \omega_1^{-1} \omega_t \omega' \tau_k$ so that the l's can be replaced by k's and the τ_l's by this expression involving τ_k and a word in the generators of H.

3. Proofs of results

Lemma 1. *Let F be a free group and H a finitely generated subgroup $\langle \omega_j \,|\, j \in J \rangle$ of countable index in F. If $\{x_i \,|\, i \in I\}$ is a set of generators of F, then the identities $H\omega_j = H$ and $H\theta x_i^{\varepsilon} x_i^{-\varepsilon} = H\theta$, for all cosets $H\theta$, are sufficient to enumerate the cosets of H in F.*

Proof. Suppose that the coset $H\mu = Hv$, where μ and v are words in the generators of F. Then $\mu v^{-1} \in H$, that is $\mu v^{-1} = \omega_{j_1}^{\varepsilon_1} \omega_{j_2}^{\varepsilon_2} ... \omega_{j_n}^{\varepsilon_n}$ for some $\{j_1, j_2, ..., j_n\} \subseteq J$ and for some $\{\varepsilon_1, \varepsilon_2, ..., \varepsilon_n\} \subseteq \{-1, 1\}$. Note that because F is free this equality is an identity apart from words of the form $\eta \eta^{-1}$ on either side of the equation.

Now for each sequence $x_{i_1}^{\varepsilon_1}, x_{i_2}^{\varepsilon_2}, ..., x_{i_n}^{\varepsilon_n}$ define the coset $H_{i_1, i_2, ..., i_n}^{\varepsilon_1, \varepsilon_2, ..., \varepsilon_n}$ to be the coset $H x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} ... x_{i_n}^{\varepsilon_n}$. If we now calculate $H\mu v^{-1}$, we find that this is H provided $H\theta x_i^{\varepsilon} x_i^{-\varepsilon} = H\theta$ for all cosets $H\theta$ and all generators x_i and provided $H\omega_j = H$ for all $j \in J$ (this implies $H\omega_j^{-1} = H$). Thus to find all the equalities between the cosets it is sufficient to check that $H\theta x_i^{\varepsilon} x_i^{-\varepsilon} = H\theta$ and that $H\omega_j = H$ for all the generators ω_j of H.

If we next ask what is the index of the group generated by a set of words $\{\omega_j \,|\, j \in J\}$ in the group $G = \langle x_i \,|\, i \in I, \sigma_k = 1, k \in K \rangle$, then the corresponding

question about free groups is that of finding the index of the subgroup generated by the set $\{\omega_j \mid j \in J\}$ and the normal closure of the group $\langle \sigma_k \mid k \in K \rangle$ in the free group $\langle x_i \mid i \in I \rangle$. The subgroup is not necessarily given as a finitely generated group since the only set of generators we have is

$$\{\omega_j \mid j \in J\} \cup \{\omega^{-1} \sigma_k \omega \mid k \in K, \omega \in \langle x_i \mid i \in I \rangle\}.$$

However, if G is finitely generated and finitely presented, that is if the sets I and K are both finite, and so the subgroup H is of countable index and finitely generated, then it is sufficient to consider a countable number of relations of the type given in Lemma 1.

Lemma 2. *Let H be a finitely generated subgroup $\langle \omega_j \mid j \in J \rangle$ of countable index in a finitely generated finitely presented group*

$$G = \langle x_i \mid \sigma_k = 1, i \in I, k \in K \rangle.$$

Then the identities $H\omega_j = H$, $H\theta\sigma_k = H\theta$ and $H\theta x_i^{\varepsilon} x_i^{-\varepsilon} = H\theta$, $\varepsilon = \pm 1$ are sufficient to enumerate all the cosets of H in G.

Proof. A typical generator $\omega^{-1}\sigma_k\omega$ is equivalent to the relation $H\theta\sigma_k = H\theta$, where $H\theta$ is the coset $1\omega^{-1}$. Thus we have reduced the problem to investigating, for each coset $H\theta$, the relation $H\theta\sigma_k = H\theta$, for each of the given relations $\sigma_k = 1$ of G. Therefore, on adding the identities $H\theta\sigma_k = H\theta$ to the identities in Lemma 1, we are now able to enumerate all the cosets of H in G.

So far we have only shown that given a finitely generated finitely presented group we can find the index of a finitely generated subgroup in a countable number of steps. We next show that when the index of the subgroup is finite, then a finite number of steps is sufficient.

Theorem 3. *Let H be a finitely generated subgroup $\langle \omega_j \mid j \in J \rangle$ of finite index in a finitely generated finitely presented group*

$$G = \langle x_i \mid \sigma_k = 1, i \in I, k \in K \rangle.$$

Then the classical algorithm terminates in a finite number of steps.

Proof. If $H\theta$ is any coset of H, then we can choose a representative of $H\theta$, g say. Expressing g as a word in the generators of G, we have $H\theta = 1.g$ and step (ii) (*a*) of the algorithm ensures that $H\theta$ is given at least one label in the above process in a finite number of steps. As H is of finite index in G we can then find an integer m such that each coset has a label less than m.

We must now show that, again in a finite number of steps, we can identify the cosets ng and ng^{-1} among those m for all non-redundant $n \leq m$ and all g in the generating set. As the number of such cosets is finite we need only show that ng can be identified in a finite number of steps, where g is either a generator or the inverse of a generator. By the choice of m, ng is equal to some coset k say, with $k \leq m$. n is defined as 1σ for some σ in G and similarly k is defined as 1ω for some ω in G.

Now $ng = k$ is equivalent to $\sigma g \omega^{-1} \in H$. However, $\sigma g \omega^{-1} \in H$ if and only if it can be written as a product $\Pi \mu_i$, where μ_i is either a generator of H, the inverse of a generator of H, a conjugate of a relation of G or the inverse of such a conjugate.

But after a finite number of steps the algorithm provides sufficient information to give $1\mu_i = 1$ and so $1\sigma g \omega^{-1} = 1$. Thus all the cosets ng can be identified in a finite number of steps and so the process must terminate for it is then possible to complete the coset enumeration tables without defining further cosets.

Notice that we cannot restrict our attention only to the first m cosets. In fact, there is no upper bound to the number of cosets needed to complete the process in terms of the index, the lengths of the generators and relations and the number of generators and relations.

Theorem 4. *Let H be a finitely generated subgroup $\langle \omega_j \mid j \in J \rangle$ of countable index in a finitely generated finitely presented group $G = \langle x_i \mid \sigma_k = 1, i \in I, k \in K \rangle$. Then the additional algorithm provides a presentation of H. Moreover, if the index of H in G is finite, this presentation is finite.*

Proof. Suppose $h_{i_1}^{e_1} h_{i_2}^{e_2} \ldots h_{i_n}^{e_n} = 1$ is a relation between the generators of H. Then, as this is a consequence of the relations of G, $h_{i_1}^{e_1} h_{i_2}^{e_2} \ldots h_{i_n}^{e_n}$ is freely equal to $\Pi \mu_j$, where μ_j is either a conjugate of a relation of G or the inverse of a conjugate.

$1\mu_j = 1$ modulo the relations of H discovered during the process, that is $1\mu_j = 1$ or $1\mu_j = w.1$, where $w = 1$ is one of the relations. Therefore $1.\Pi\mu_j = 1$ modulo the relations of H discovered during the coset enumeration. On the other hand the initial consideration of generators of H shows that $1.h_i = h_i.1$ modulo any later changes brought about by using relations of H discovered in consequence of coincidences occurring during the algorithm. Thus, as required, the relation $h_{i_1}^{e_1} h_{i_2}^{e_2} \ldots h_{i_n}^{e_n} = 1$ is a consequence of the relations discovered by the algorithm.

4. Applications

The theorems of Section 3 find application in (3), (4) and (7). In (3, Theorem 4), for example, it is shown that the subgroup $H = \langle a, b^2 \rangle$ is of countable index in the group

$$G = \langle a, b \mid [a^2, b^{-1}] = a^{-1}b^{2n}a, [b^2, a^{-1}] = b^{-1}a^{2n}b \rangle$$

and using Theorem 4 of this paper a presentation for H is found.

To show the difference between the above algorithm and that of Mendelsohn (7), the following example shows that four relations are produced by this version of the algorithm instead of the one produced in (7). This same group is also considered in (6).

We consider the subgroup $\langle x, a^8 \rangle$ in the group $\langle x, a \mid x^{-1}a^2x = a^3 \rangle$. Denoting the subgroup generators by α and β respectively we find that it is

necessary to define eight cosets before a coincidence is discovered. At this stage the tables have the following form:

α		β								
x		$a\ a\ a\ a\ a\ a\ a\ a$								
1 1		1 2 3 4 5 6 7 8 1								

	x^{-1}	a	a	x	$=$	a	a	a
	1	1	2	3	4	1	2	3	4
	4	3	4	5	7	4	5	6	7
	7	5	6	7	2	7	8	1	2
	2	7	8	1	1	2	3	4	5

The multiplication table for the coset representatives is $1a = 2$, $2a = 3$, $3a = 4$, $4a = 5$, $5a = 6$, $6a = 7$, $7a = 8$, $8a = \beta1$, $1x = \alpha1$, $3x = \alpha4$, $5x = \alpha7$ and $7x = \alpha\beta2$. The coincidence obtained from the last line of the table gives $5 = [\beta, \alpha]1$. Substitution in the multiplication table now gives the multiplication table $1a = 2$, $2a = 3$, $3a = 4$, $4a = [\beta, \alpha]1$, $1x = \alpha1$, $3x = \alpha4$, the collapses $6 = [\beta, \alpha]2$, $7 = [\beta, \alpha]3$, $8 = [\beta, \alpha]4$ and, by further substitution, $[\beta, \alpha]\alpha1 = \alpha[\beta, \alpha]3$ and $[\beta, \alpha]\alpha4 = \alpha\beta2$ and finally from $8a = \beta1$ we obtain the relation $[\beta, \alpha]^2 = \beta$.

Substitution in the multiplication table for 3 and 4 now gives

$$1a = 2, \quad 2a = [[\beta, \alpha], \alpha]1, \quad 1x = \alpha1$$

as the multiplication table, two more relations, $[[\beta, \alpha], \alpha] = [\alpha, \beta]^{\alpha}\beta$ and $[\alpha, \beta]^{\alpha}\beta[[\beta, \alpha], \alpha] = [\beta, \alpha]$, and the coincidence $[[\beta, \alpha], \alpha]\alpha1 = [\alpha, \beta]\alpha\beta2$ which reduces to $2 = \beta^{-1}[\beta, \alpha]^{\alpha^2}1$.

A final substitution now gives $1a = \beta^{-1}[\beta, \alpha]^{\alpha^2}1$, $1x = \alpha1$ and the relation $(\beta^{-1}[\beta, \alpha]^{\alpha^2})^2 = [[\beta, \alpha], \alpha]$.

Thus we have shown that $\langle x, \alpha^8 \rangle = \langle x, a \rangle$ and in terms of the new generators the group is

$$\langle \alpha, \beta \mid [\beta, \alpha]^2 = \beta, [[\beta, \alpha], \alpha] = [\alpha, \beta]^{\alpha}\beta = \beta^{-1}[\beta, \alpha]^{\alpha}[\beta, \alpha] = (\beta^{-1}[\beta, \alpha]^{\alpha^2})^2 \rangle.$$

From $1a = \beta^{-1}[\beta, \alpha]^{\alpha^2}1$ we obtain the expression for a in terms of α and β, $a = \beta^{-1}[\beta, \alpha]^{\alpha^2}$.

Substituting $[\beta, \alpha]^2$ for the final β in $[[\beta, \alpha], \alpha] = [\alpha, \beta]^{\alpha}\beta$, we obtain $[\beta, \alpha] = [[\beta, \alpha]\alpha]^2$. Using this new relation and substituting for the initial β^{-1} in $\beta^{-1}[\beta, \alpha]^{\alpha}[\beta, \alpha]$, we find this reduces immediately to $[[\beta, \alpha], \alpha]$. Thus the set of relations obtained is in this case redundant. It should be noted that the adaptation of the Reidemeister-Schreier process using two coset enumerations will provide a presentation of the group.

(Note that in the above hand calculation we have not worked through the algorithm systematically but have constructed the tables in a way which avoids introducing more redundant cosets than necessary.)

REFERENCES

(1) C. T. BENSON and N. S. MENDELSOHN, A calculus for a certain class of word problems in groups, *J. Combinatorial Theory* **1** (1966), 202-208.

(2) C. M. CAMPBELL, Dissertation, McGill University, 1965.

(3) C. M. CAMPBELL and E. F. ROBERTSON, Remarks on a class of 2-generator groups of deficiency zero, *J. Australian Math. Soc.* **19** (1975), 297-305.

(4) C. M. CAMPBELL and E. F. ROBERTSON, The orders of certain metacyclic groups, *Bull. London Math. Soc.* **6** (1974), 312-314.

(5) J. J. CANNON, L. A. DIMINO, G. HAVAS and J. M. WATSON, Implementation and analysis of the Todd-Coxeter algorithm, *Math. Comp.* **27** (1973), 463-490.

(6) J. LEECH, Computer proof of relations in groups, *Proceedings of the Royal Irish Academy Summer School on Group Theory and Computation* (Academic Press, to appear).

(7) N. S. MENDELSOHN, Defining relations for subgroups of finite index of groups with a finite presentation, *Computational Problems in Abstract Algebra* edited by J. Leech (Pergamon, Oxford, 1970), 43-44.

(8) J. A. TODD and H. S. M. COXETER, A practical method for enumerating cosets of a finite abstract group, *Proc. Edinburgh Math. Soc.* **5** (1936), 26-34.

MATHEMATICAL INSTITUTE
UNIVERSITY OF ST ANDREWS