ENumeration of Double CoSets

Robert H. GILMAN*
Department of Pure and Applied Mathematics, Stevens Institute of Technology, Castle Point Station, Hoboken, NJ 07030, USA

Communicated by H. Bass
Received 8 September 1981
Revised 11 January 1982

Introduction

Let $H$ and $K$ be subgroups of a group $G$. The double cosets of $H$ and $K$ in $G$ are the sets $HgK$, $g \in G$. In this paper we describe a procedure, $P$, for determining the cardinality of the set $H \setminus G \setminus K$ of double cosets of $H$ and $K$ in $G$ given a finite presentation for $G$ and finite sets of generators for $H$ and $K$.

It is well known that the problem of determining whether or not a group $G$ defined by a finite presentation is finite is unsolvable. As this problem is the same as enumerating $H \setminus G \setminus K$ when $H=K=1$, every double coset enumeration procedure must fail for some inputs. $P$ fails by running forever and never terminating.

Enumeration of $H \setminus G \setminus K$ when $H=1$ is coset enumeration, and the Coxeter-Todd procedure [2, Chapter 2] solves this problem exactly when the number of cosets is finite. By enumerating $G/H$ and $G/K$ in parallel one can use the Coxeter-Todd method to count $H \setminus G \setminus K$ whenever $G/H$ or $G/K$ is finite. Thus our procedure, $P$, is of interest when $G/H$ and $G/K$ are both infinite. Some examples are given in Section 4. Unfortunately Example 3 shows that $P$ need not terminate when $H \setminus G \setminus K$ is finite. A version of $P$ for the case $H=K=1$ appears in [3].

2. A preliminary result

Assume that $G$ is a finitely presented group and $H$ and $K$ are finitely generated subgroups. Let

$$\langle a_1, a_2, \ldots \mid w_1 = v_1, w_2 = v_2, \ldots \rangle$$

be a finite presentation of $G$ as a quotient of a finitely generated free monoid $F$ with generators $a_1, a_2, \ldots$. Such a presentation may be obtained by adding new generators

* Partially supported by N.S.F. Grant MCS-80-02164.

0022-4049/82/0000-0000/$02.75 © 1982 North-Holland
and relations \( gg^{-1} = 1 = g^{-1}g \) for each generator \( g \) in a presentation of \( G \) as a quotient of a free group. Let

\[
\{h_1, h_2, \ldots \}, \quad \{k_1, k_2, \ldots \}
\]

be finite sets of words in \( F \) representing the generators of \( H \) and \( K \), and let \( \pi : F \to G \) be the projection corresponding to the presentation above. The inverse image under \( \pi \) of the double cosets of \( H \) and \( K \) in \( G \) is the set of equivalence classes of the equivalence relation \( = \) generated by

\[
xw_i y = xu_i y, \quad h_j x = x, \quad xk_r = x,
\]

as \( x \) and \( y \) range over all words in \( F \).

\( P \) depends on Proposition 1, which is a special case of a result used to solve word problems in algebras [1], [5]. Order the generators of \( F \) arbitrarily, and define \( r < t \) for \( r \) and \( t \) in \( F \) by \( r < t \) if \( r \) is shorter than \( t \) or if \( r \) and \( t \) have equal length and \( r \) precedes \( t \) in the lexicographic order. Note that \( < \) is a well-ordering (i.e. every non-empty subset of \( F \) has a least element), and \( r < t \) implies \( xry < xty \) for all \( x \) and \( y \) in \( F \).

We assume that \( w_i < v_i \) and \( h_j \neq 1 \neq k_r \) in (1). It follows that applying any of the relations in (1) from left to right to a word \( w \) in \( F \) makes \( w \) smaller.

Proposition 1 [6]. Let \( \sim \) be an equivalence relation on the finitely generated free monoid \( F \). Let \( F \) be ordered by the ordering \( < \) defined above and suppose that \( \sim \) is generated (as an equivalence relation) by a set of generators

\[
S = \{ p_j = q_j \}
\]

with \( p_j > q_j \) for all \( j \). Define \( \to \) to be the transitive reflexive (but not symmetric) closure of \( S \). The following two conditions are equivalent:

(i) If \( p_j = p_k \) then \( q_j \to x \) and \( q_k \to x \) for some \( x \) in \( F \);

(ii) For every \( y \) in \( F \) there is a unique \( z \) in \( F \) denoted by \( y^* \) such that \( y \to z \) and there is no \( x \) with \( z \to x \neq z \). Further \( x = y \) if and only if \( x^* = y^* \).

Proof. Assume (i) holds. Since \( < \) is a well-ordering, there must be at least one \( z \) as in (ii) for each \( y \). Let us call such a \( z \) terminal. If \( z \) is not always unique, then

\[
y = p_j \to q_j \to z_1, \quad y = p_k \to q_k \to z_2
\]

for some \( y \) with \( z_1 \neq z_2 \) and \( z_1, z_2 \) terminal. Take \( y \) to be the minimum for which (2) holds. Pick \( x \) as in (i) and \( z_3 \) terminal with \( x \to z_3 \). By minimality of \( y \), \( z_1 = z_3 = q_j^* \) and \( z_2 = z_3 = q_k^* \). Thus the first part of (ii) holds.

Suppose there exist \( x \) and \( y \) with \( x = y \), \( x^* \neq y^* \). Since \( \sim \) is generated as an equivalence relation by \( \to \), there is a sequence

\[
x^* = z_0 \leftarrow z_1 \leftarrow z_2 \leftarrow \cdots \leftarrow z_{n-1} \to z_n = y^*.
\]

We change \( z_i, i \) even, if necessary so that \( z_i = z_i^* \). Now \( z_0 \neq z_n \) implies \( z_i \neq z_{i+2} \) for some even \( i \) contrary to the first part of (ii) with \( y = z_{i+1} \).

Finally (ii) implies (i) because \( q_j^* = p_j^* = p_k^* = q_k^* \).
3. Procedure P

The input to P is a set of relations (or generators for an equivalence relation $=\,$) on a finitely generated free monoid $F$.

\[ xw_i y = xu_j y \quad \text{for all } x, y \text{ in } F, \]

\[ h_j x = m_j x \quad \text{for all } x \text{ in } F, \]

\[ xk_r = xn_r \quad \text{for all } x \text{ in } F, \]

\[ t_s = u_s, \]

where the indices range over finite sets and $w_i > v_i$, $h_j > m_j$, $k_r > n_r$, $t_s > u_s$ in the ordering $\succ$ defined in Section 2. Clearly (3) includes (1). We say that (3) is complete if it satisfies condition (i) of Proposition 1.

P proceeds as follows: (3) is tested for completeness. If (3) is complete, the equivalence classes of $=\,$ are enumerated as indicated in the next section. If (3) fails the test for completeness, P augments (3) by adding more relations and repeats the test. P continues in this way until (3) becomes complete. If (3) never becomes complete, P fails to terminate.

P tests (3) for completeness by searching for the element $x$ of Proposition 1(i) for each pair of relations in (3). Let $\rightarrow$ be the transitive reflexive closure of (3). For each instance $p_i = p_j$ listed below we apply the relations indicated from left to right in any order to find $x_1$ and $x_2$ with $q_i \rightarrow x_1$, $q_j \rightarrow x_2$ such that none of the indicated relations can reduce $x_1$ or $x_2$ or any further.

<table>
<thead>
<tr>
<th>$p_i = p_j$</th>
<th>Restriction on $p_i, p_j$</th>
<th>Relations to apply</th>
</tr>
</thead>
<tbody>
<tr>
<td>$xw_i y = w_i y$</td>
<td>$w_i$ and $w_j$ overlap</td>
<td>(3)(a)</td>
</tr>
<tr>
<td>$w_i = w_j y$</td>
<td>(3)(a)</td>
<td></td>
</tr>
<tr>
<td>$h_j x = yw_i$</td>
<td>$h_j$ and $w_i$ overlap</td>
<td>(3)(a)(b)</td>
</tr>
<tr>
<td>$h_j = xw_j y$</td>
<td>(3)(a)(h)</td>
<td></td>
</tr>
<tr>
<td>$h_j = h_j x$</td>
<td>(3)(a)(b)</td>
<td></td>
</tr>
<tr>
<td>$xk_r = w_i y$</td>
<td>$k_r$ and $w_i$ overlap</td>
<td>(3)(a)(c)</td>
</tr>
<tr>
<td>$k_r = xw_i y$</td>
<td>(3)(a)(c)</td>
<td></td>
</tr>
<tr>
<td>$k_i = xk_r$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_j x = yk_r$</td>
<td>$h_j$ and $k_i$ overlap</td>
<td>(3)(a)−(d)</td>
</tr>
<tr>
<td>$t_s = xw_i y$</td>
<td>(3)(a)−(d)</td>
<td></td>
</tr>
<tr>
<td>$t_s = h_j x$</td>
<td>(3)(a)−(d)</td>
<td></td>
</tr>
<tr>
<td>$t_s = xk_r$</td>
<td>(3)(a)−(d)</td>
<td></td>
</tr>
<tr>
<td>$t_s = t_{i_2}$</td>
<td>(3)(a)−(d)</td>
<td></td>
</tr>
</tbody>
</table>

Because the indices $i, j, r, s$ run through finite sets, there are only a finite number of instances of the types listed in Table 1; and since $< \,$ is a well-ordering, the calculation of $x_1$ and $x_2$ in each instance involves only a finite number of applications of relations and can be carried out.
Lemma 1. If $x_1 = x_2$ for every instance listed in Table 1, then (3) is complete.

Proof. It suffices to check that all the possibilities $p_i = p_j$ not listed in Table 1 satisfy Proposition 1(i). Suppose we have

$$p_i = x_1 w_{11} y_1 = p_j = x_2 w_{12} y_2.$$  

The other possibilities are all handled similarly. If $w_{11}$ and $w_{12}$ do not overlap, then $p_i = x_1 w_{11} z w_{12} y_2$ (say), and $x = x_1 w_{11} z w_{12} y_2$ satisfies $q_i \rightarrow x$, $q_j \rightarrow x$. Further if $w_{11}$ and $w_{12}$ do overlap, then we may interchange $w_{11}$ and $w_{12}$ if necessary so that one of the following two possibilities holds:

$$p_i = x_3 x w_{11} y_3, \quad p_j = x_3 w_{12} y y_3$$

or

$$p_i = x_3 x w_{11} y_3, \quad p_j = x_3 x w_{12} y y_3$$

for some $x, y, x_3, y_3$ in $F$. In the first case $p_i = p_j'$ occurs in Table 1 for $p_i' = x w_{11}$, $p_j' = w_{12} y$; and in the second case $p_i' = p_j'$ occurs in Table 1 for $p_i' = w_{11}$, $p_j' = x w_{12} y$. By hypothesis $q_i' \rightarrow x'_1$, $q_j' \rightarrow x'_2$ with $x'_1 = x'_2$. Because only relations of type (3)(a) are used in calculating $x_1$ and $x_2$, it follows that

$$q_i = x_3 q'_i y y_3 \rightarrow x_3 x'_1 y_3, \quad q_j = x_3 q'_j y y_3 \rightarrow x_3 x'_2 y_3$$

in both cases. Thus Proposition 1(i) holds for $p_i = p_j$ as desired.

If (3) is not complete, then some of the calculations for $p_i = p_j$ in Table 1 end with $x_1 \neq x_2$. Say $x_1 > x_2$. If only relations of type (3)(a) were used in calculating $x_1$ and $x_2$, we add the relations

$$xx_1 y = xx_2 y$$

for all $x, y$ in $F$

to the set (3)(a). Similarly if only relations of type (3)(a) and (3)(b) were used, we add

$$x_1 y = x_2 y$$

for all $y$ in $F$

to (3)(b), and likewise if only relations of type (3)(a) and (3)(c) were used. In the remaining cases we add the single relation $x_1 = x_2$ to (3)(d). Since each pair of relations originally in (3) satisfies the criterion of Proposition 1(i) if we are allowed to use the new relations added to (3), it follows that in the next test of (3) for completeness we need only test those instances of Table 1 involving at least one of the new relations.

4. Enumeration

Suppose the relations in (3) are complete. It follows that the corresponding equivalence classes each contain a unique representative in

$$L = \{w \mid w \neq x w_{11} y \text{ or } h_j y \text{ or } x k r \text{ or } t_s \text{ for any } x, y \text{ in } F\}.$$
$L$ is a rational subset of $F$, and the enumeration of $L$ is a straightforward application of techniques from the theory of automata and rational languages. For example one can construct a nondeterministic automaton $A$ accepting $F - L$. From $A$ one can obtain first a deterministic automaton accepting $F - L$ and then an automaton $B$ accepting $L$. Given $B$ one easily determines the cardinality of $L$. A text in automata theory and formal languages is [4]. Algorithm $A$ of [3] can be extended to give a more efficient way of enumerating $L$.

We conclude with some examples.

**Example 1.** Enumerate the cosets $G/K$ with

$$G = \langle a, b \mid a^2 = 1 = b^2 \rangle \quad \text{and} \quad K = \langle a \rangle.$$

The input to $P$ is $xa^2y = xy$, $xb^2y = xy$, $xa = x$ which turns out to be complete. A regular expression for $L$ is

$$L = (1 + b)(ab)^*.$$

That is, $L$ is the set of all $w = uv$ with $u = 1$ or $b$ and $v = (ab)^n, n \geq 0$. In particular $L$ is infinite and so is $G/K$.

**Example 2.** Enumerate $H \setminus G/K$ with

$$G = \langle a, b \mid a^3 = 1 = b^2 \rangle, \quad H = \langle ab \rangle, \quad K = \langle ba \rangle.$$

The input to $P$ is $xa^3y = xy$, $xb^2y = xy$, $abx = x$, $xba = x$. Considering pairs of relations in the order (1, 1), (1, 2), (2, 2), (1, 3), (2, 3), (3, 3) ... we find that the first new relation comes from using the second and third relations to compute distinct reductions of the word $ab^2$. We obtain $bx = ax$ (we are ordering the generators alphabetically). $P$ terminates with the further relations $xb = xa$, $a^2 = 1$, and

$$L = 1 + a + (a^2b)(ab + a^2b)^*(a^2).$$

Again the number of cosets is infinite.

**Example 3.** Enumerate $H \setminus G/K$ when

$$G = \{ a, c \mid ac = ca \}, \quad H = \langle c \rangle, \quad K = \langle a \rangle.$$

Since we know that $G$ is the direct product of two infinite cyclic groups, we take as input to $P$ the relations

$$xaby = xy, \quad xbuy = xy, \quad xcdy = xy, \quad xdcy = xy,$$

$$xcay = xacy, \quad xcby = xbcy, \quad xday = xady, \quad xdby = xbdy,$$

$$cx = x, \quad xa = x.$$

Omitting the last two relations gives a complete set of relations for $G$ (i.e. the case $H = 1 = K$). With the full set of relations it is clear that there is just one double coset,
but \( P \) does not terminate. \( P \) produces the infinite set of relations

\[
\begin{align*}
&b x = x, & x d = d, \\
&a^k c x = a^k x, & a^k d x = a^k x, & b^k c x = b^k x, & b^k d x = b^k x, \\
&x a^k c = x c^k, & x a d^k = x d^k, & x b c^k = x c^k, & x b d^k = x d^k
\end{align*}
\]

for all \( x \) in \( F \) and all \( k \geq 1 \). These relations together with the input to \( P \) form a complete set.

One way to improve \( P \) would be to find a rule of inference which allowed the deduction of the relations \( x a y = x y \) and \( x c y = x y \) from the relations produced after some finite number of iterations of \( P \) in Example 3.

References