A Rewriting Alternative to Reidemeister-Schreier

Neil Ghani and Anne Heyworth

Department of Mathematics and Computer Science, University of Leicester

Abstract. One problem in computational group theory is to find a presentation of the subgroup generated by a set of elements of a group. The Reidemeister-Schreier algorithm was developed in the 1930's and gives a solution based upon enumerative techniques. This however means the algorithm can only be applied to finite groups. This paper proposes a rewriting based alternative to the Reidemeister-Schreier algorithm which has the advantage of being applicable to infinite groups.

1 Introduction

In computational group theory [3], one tries to reason about various properties of groups which are finitely presentable, ie groups defined as the quotient of the free group on a set of generators by a set of relations. One of the most common approaches to these sorts of problems is based upon enumerative techniques [7] with another being based upon string rewriting [2, 11]. Although the former are more widely used, their enumerative nature means they are limited to groups with finitely many elements.

One problem in computational group theory is to find a presentation of the subgroup generated by a set of elements of a group. The Reidemeister-Schreier algorithm [7] was developed in the 1930's and gives a solution based upon enumerative techniques. This paper proposes a rewriting based alternative to the Reidemeister-Schreier algorithm which has the advantage of being applicable to infinite groups. A prototype has been implemented and we are currently discussing with the GAP-group how to bring it up to the standard required for integration into the GAP [4] distribution.

Typically a group is given by a monoid presentation consisting of a set of generators X and equations R and we are interested in finding a presentation of the subgroup H generated by a set of words $Y \subseteq X^*$. It is clear that in general one can take as a generating set for H the disjoint union of Y with itself. One half of this union will represent the elements of Y in H while the other half will represent their inverses. However, the difficult question is to take the relations of R, which may refer to words not in Y, and recast them so that they only mention words built from Y and its inverses. To do this, words w_1 and w_2 built from Y but equal under R are considered as rewrite sequences and thus the question becomes when should two rewrite sequences be equal. This takes us into the world of logged [6] or labelled rewriting as is found in Levy equivalence [9], rewriting logic [10] and 2-categorical models of rewriting [12]. Our central idea is that two rewrite sequences are equal if they arise through the analysis of critical pairs as found in Knuth-Bendix completion [8]. Thus, Knuth-Bendix completion is not only a mechanism for completing rewrite systems, but in addition the process of how this completion occurs contains valuable computational information. Since our equations are a by-product of Knuth-Bendix completion, our algorithm can be applied to infinite groups unlike the standard Reidemeister-Schreier algorithm. In more detail, our algorithm is broken down onto three parts.

- Subgroups are intimately connected with the behaviour of the associated cosets. The first step of our procedure is to define a *coset rewriting system* to solve the coset membership problem which asks when two elements of the group belong to the same coset.
- By attaching labels to the rewrites of the coset rewriting system we obtain witnesses to the solution of the coset membership problem.
- Finally, the critical pairs of the coset rewriting system, when labelled, yield the presentation of the subgroup.

As well as providing an application of rewriting, we were pleasantly surprised that our algorithm used some of the theory of rewriting, in particular sesqui-categories [12], Levy equivalence [9] and the interaction of these structures with Knuth-Bendix completion. We are aware that certain readers will not be familiar with these sesqui-categories but we only use the language of sesqui-categories to organise definitions and there is no deep categorical content which could put the reader off. Possibly more of a problem is the group theory used here which, although only of an undergraduate level, some readers may not have met. We have addressed this issue by including all relevant definitions and giving references. However, in the end, it is the nature of applications of rewriting to use concepts from outside the core of rewriting.

The paper is structured as follows. Section 2 contains all the group theoretic definitions required, while Section 3 addresses the coset membership problem. Section 4 gives our algorithm for obtaining a presentation of a subgroup while Section 5 contains two examples which we hope the reader will use to help understand the paper. We finish in Section 6 with some concluding remarks.

2 A Brief Introduction to Group Theory

This section contains all the basic definitions from group theory needed within this paper. A more detailed exposition of this material can be found in any text on computational group theory [3]. Since this paper is addressed to a rewriting audience, standard rewriting knowledge as in [1, 2] will be assumed.

A monoid M consists of a triple $M = \langle X, \circ, e\rangle$ where $\circ$ is an associative binary operation on X with unit e. A group G consists of a quadruple $G = \langle X, \circ, \_^{-1}, e\rangle$ where $\langle X, \circ, e\rangle$ is a monoid and $\_^{-1}$ is a unary operation on X such that for all $x \in X$, x^{-1} is an inverse for x under $\circ$. As is common practice, we use the same notation for a group and its underlying carrier set. A monoid homomorphism $f : M_1 \to M_2$ between monoids is a function on the underlying sets which preserves the unit and composition. A group homomorphism is a monoid homomorphism between the underlying monoids as such monoid homomorphisms automatically preserve the inverse operation. We use the group S_3 of rotations and reflections of an equilateral triangle as a running example throughout this paper.

Example 1 *The group S_3 of rotations and reflections of an equilateral triangle has as elements $\{1, a, aa, ab, ba, b\}$ where a is a rotation by 120 degrees and b is a reflection around one axis. Composition, inverses etc are left to the reader.*

Given a set X, the free monoid X^* on X consists of finite sequences of elements of X. This set is also called the set of words over X. The monoid structure on X^* has as unit the empty word 1 and composition given by concatenation of words. Given a set X, we write $X + X$ for the disjoint union of X with itself. Typical elements of $(X + X)^*$ are written $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ where each $x_i \in X$ and $\epsilon_i \in \{+, -\}$ to denote which half of the disjoint union each element comes from. In practice we write x^+ simply as x. The free group $F_{\mathcal{G}}(X)$ on a set X is the quotient of $(X + X)^*$ by the relations $xx^- = 1 = x^-x$. Freeness of these structures allow us to define monoid homomorphisms $X^* \to M$ by giving functions $X \to M$ and group homomorphisms $F_{\mathcal{G}}(X) \to G$ by giving functions $X \to G$.

2.1 Monoid Presentations and Group Presentations

Most groups are not free. A larger class of groups which include many of practical importance and for which effective computational methods exist are the finitely presentable groups. These are defined via monoid presentations [3].

Definition 2 (Monoid Presentation) *A monoid presentation for a group G is of the form $mon\langle X|R\rangle$, where X is a finite set and R is a finite subset of $X^* \times X^*$ such that G is isomorphic (as a monoid, and hence a group) to the quotient of X^* by the least congruence containing R.*

Given a monoid presentation of a group G by $mon\langle X|R\rangle$ we denote by $\theta : X^* \to G$ the quotient morphism assigning to each word its equivalence class in the group. Note that θ is surjective and a monoid homomorphism. Also given $w \in X^*$, we know that $\theta(w)^{-1} \in G$ and by surjectivity there is a word $z \in X^*$

such that $\theta(z) = \theta(w)^{-1}$. Abusing notation, we denote this word by w^- since it is a word representing the inverse of the word w under θ in G. Of course, w^- is not uniquely defined and we ensure we deal with this whenever required.

As an example of a monoid presentation, consider S_3. Three rotations produce the identity transformation of the triangle, so do two reflections and also a rotation, reflection, rotation and reflection. In fact all other equivalences of rotations and reflections can be deduced from these facts. Thus,

Example 3 *S_3 is presented by mon$\langle\, a, b \mid a^3 = 1,\ b^2 = 1,\ abab = 1 \,\rangle$.*

The most famous problem in computational group theory is the word problem: *Given a group presentation mon$\langle X|R\rangle$ and any two words w and w' in X^*, is it the case that $w \sim_R w'$* where $\sim_R$ is the least congruence on X^* containing R. This problem is in general undecidable but there are a number of approaches which solve the problem under certain circumstances. The most common is based upon *string rewriting* and *Knuth-Bendix completion* [1,2]. Given a monoid presentation, one orients each pair $(u, v) \in R$ as a rewriting rule $u \to_R v$, and proves the resulting rewriting relation is strongly normalising and confluent. Then every word has a computable unique normal form and $w \sim_R w'$ iff the normal form of w is equal to that of w'. If, as is most likely, the rewriting relation is not strongly normalising and confluent, Knuth-Bendix completion can attempt to obtain a rewriting relation $\to_{R'}$ which is strongly normalising, confluent and which generates the same congruence as $\to_R$.

Example 4 *Knuth-Bendix completion (with word length as termination order) of the presentation of S_3 gives the following complete rewriting system.*

$$\begin{array}{lll} aaa \to 1 & bb \to 1 & aab \to ba \\ aba \to b & baa \to ab & bab \to aa \end{array}$$

This paper tackles the problem of finding a presentation for a subgroup of a finitely presentable group. Subgroups are intimately connected with cosets and so we turn to the definition of these concepts.

Definition 5 (Subgroup) *A subgroup of a group G is a non-empty subset $H \subseteq G$ such that $e \in H$ and H is closed under composition and inverses.*

Examples of subgroups of S_3 are $\{1\}, \{1, a, aa\}$ and $\{1, b\}$. If H is a subgroup of G, we can divide or partition G by H into what are called *cosets*.

Definition 6 (Cosets) *Let H be a subgroup of G. Define an equivalence relation on G by $x \sim_H x'$ iff there is an $h \in H$ such that $x = hx'$. The cosets of H in G are written as G/H and defined to be the equivalence classes of G under $\sim_H$. The coset of an element $x \in G$ is written Hx.*

The data used in our rewriting alternative to Reidemeister-Schreier consists of a presentation of the group and a set of words which generate the subgroup.

Definition 7 (Coset Presentation) *A* coset presentation *is a triple* $\langle X, S, Y\rangle$ *where* X *is a set,* $S \subseteq X^* \times X^*$ *and* $Y \subseteq X^*$.

Implicitly a coset presentation P is assumed to determine the following:

- A group G_P defined via the monoid presentation $\langle X, S\rangle$.
- A monoid homomorphism $\theta : X^* \to G_P$.
- A subgroup H_P of G_P defined to be the least subgroup of G_P containing the set $\theta(Y)$. Alternatively, H_P consists of all elements of G_P of the form $\theta(y_1)^{\pm 1} \cdots \theta(y_n)^{\pm 1}$ where each $y_i \in Y$.

We now fix a coset presentation $\langle X, S, Y\rangle$, omit the subscript P and speak simply of the group G and the subgroup H. Any set of generators for H must have enough words to represent each element of H. Clearly $Y + Y$ provides such a set since $\theta(y)$ can be represented by y, $\theta(y)^{-1}$ by y^- and composites of the form $\theta(y_1)^{\pm 1} \cdots \theta(y_n)^{\pm 1}$ can be represented by words over $Y + Y$. Of course θ restricts to a map $Y \to H$ which extends uniquely to a monoid homomorphism $\hat{\theta} : (Y + Y)^* \to H$ by setting $\hat{\theta}(y^-) = \theta(y)^{-1}$. Further evidence that H can be expressed as a quotient of $(Y + Y)^*$ is the following lemma:

Lemma 8 *Let* $\sim_{\hat{\theta}}$ *be the kernel of* $\hat{\theta}$*. Then* H *is isomorphic to* $(Y+Y)^*/\sim_{\hat{\theta}}$.

Proof. We construct a bijection between $(Y+Y)^*/\sim_{\hat{\theta}}$ and H. Given $h \in H$, we have seen that h is of the form $\theta(w)$ for some $w \in (Y+Y)^*$. Thus h is mapped to the equivalence class of w under $\sim_{\hat{\theta}}$. In the reverse direction, given any equivalence class $[w] \in (Y+Y)^*/\sim_{\hat{\theta}}$, we map $[w]$ to $\hat{\theta}(w)$. That these definitions are independent upon the various choices and are mutually inverse are straightforward and left to the reader.

Unfortunately the congruence $\sim_{\hat{\theta}}$ does not give us a presentation and thus we must try to re-axiomatise it as equations using only symbols from $Y + Y$.

3 The Coset Membership Problem

The first step of our algorithm for obtaining a presentation of the subgroup H is to solve the coset membership problem which asks when two elements of the group belong to the same coset. We do this by rewriting over the set HX^* defined by introducing the formal symbol H and defining

$$HX^* = \{Hw \mid w \in X^*\}$$

We stress that in this context, H is just a formal symbol in the same way that elements of X^* are just formal words. The distinction between H used here as such a formal word and H used elsewhere as a subgroup mirrors the distinction between the words in X^* and their equivalence classes as elements of a group. Coset rewriting systems are defined as follows:

Definition 9 (Coset Rewriting System) *If $P = \langle X, S, Y\rangle$ is a coset presentation, a* coset rewriting system *(CRS) for P consists of a pair $R = \langle R_G, R_H\rangle$ where $R_G \subseteq X^* \times X^*$ and $R_H \subseteq HX^* \times HX^*$ such that:*

- *The relations R_G and S generate the same congruence. That is $\sim_S$ and $\sim_{R_G}$ are the same or, equivalently, $\langle X, R_G\rangle$ is a monoid presentation of G.*
- *If $(Hw, Hw') \in R_H$, then (as cosets) $H\theta(w) = H\theta(w')$.*
- *If $h \in H$, then there is a $w \in X^*$ such that $h = \theta(w)$ and $Hw \sim_R H$.*

The congruence $\sim_R$ used in the third clause of Definition 9 is generated from the rewriting relation $\rightarrow_R$ defined as the union of the rewriting relations $\rightarrow_{R_G}$ and $\rightarrow_{R_H}$ on HX^*. In turn these are defined as follows:

- $\rightarrow_{R_G} = \{\ (Hulv, Hurv)\ \mid\ (l, r) \in R_G,\ \ u, v \in X^*\ \}$,
- $\rightarrow_{R_H} = \{\ (Hwv, Hw'v)\ \mid\ (Hw, Hw') \in R_H,\ \ v \in X^*\ \}$.

The intuition underlying Definition 9 is that R_G gives another presentation of G — since we will be using Knuth-Bendix completion R_G cannot simply be taken to be S. We may then think of R_H as performing computation on G, ie rewriting on R_G-equivalence classes. By regarding a CRS as a proof system, the first of the conditions of Definition 9 is the soundness and completeness of R_G with respect to S, the second condition is the soundness of R_H with respect to the subgroup H while the final condition is the completeness of R wrt H.

As with usual rewriting systems, CRSs are closed under inverses and disjoint unions. Formally, if R is a CRS its inverse R^{-1} is the CRS with rules in the reverse direction. Similarly, given two CRSs R_1 and R_2 for the same coset presentation, the union $R_1 + R_2$ is the CRS whose rules are the union of the rules of R_1 and R_2. The following is an easy lemma.

Lemma 10 *If R is a CRS, so is its inverse R^{-1}. Similarly, if R_1 and R_2 are CRSs for the same coset presentation, so is $R_1 + R_2$.*

There are two key lemmas we wish to establish about CRSs; firstly that CRSs can be used to decide the coset membership problem and secondly that a coset presentation defines an initial CRS.

Lemma 11 *If $R = \langle R_G, R_H\rangle$ is a CRS for a coset presentation $\langle X, S, Y\rangle$, then the cosets G/H are in 1-1 correspondence with the equivalence classes $HX^*/\sim_R$.*

Proof. We define functions $\phi : G/H \rightarrow HX^*/\sim_R$ and $\psi : HX^*/\sim_R \rightarrow G/H$; check they are well defined given that their definitions depend upon representatives of cosets and equivalence classes; and prove they are mutually inverse.

To define ϕ consider a coset Hg. Surjectivity of θ means there is an $x_g \in X^*$ such that $\theta(x_g) = g$. Set $\phi(Hg) = [Hx_g]$. We show this definition is independent of the choice of g and the word x_g. Given a y_g such that $\theta(y_g) = g$, then $y_g \sim_S x_g$ and hence $y_g \sim_{R_G} x_g$. Thus $[Hx_g] = [Hy_g]$. Given a g' such that $Hg' = Hg$, there is an $h \in H$ such that $g' = hg$. Thus there is a $w \in X^*$ such that $\theta(w) = h$ and $Hw \sim_R H$. Thus $\theta(wx_g) = g'$ and hence $\phi(Hg') = [Hwx_g] = [Hx_g] = \phi(Hg)$.

Define ψ by mapping an equivalence class $[Hw]$ to the coset $H\theta(w)$. If $[Hw] = [Hw']$ we must show that $H\theta(w) = H\theta(w')$. Without loss of generality, assume Hw' is a one-step rewrite of Hw using either $\to_{R_H}$ or $\to_{R_G}$. Either i) $Hw = Hlv \to_{R_H} Hrv = Hw'$ where $(Hl, Hr) \in R_H$ in which case $H\theta(w) = H\theta(lv) = H\theta(l)\theta(v) = H\theta(r)\theta(v) = H\theta(rv) = H\theta(w')$ where $H\theta(l) = H\theta(r)$ is the second condition in a CRS; ii) $Hw = Hulv \to_{R_G} Hurv = Hw'$ where $(l, r) \in R_G$ in which case $\theta(w) = \theta(w')$ since $\sim_{R_G} = \sim_S$ and θ identifies S-equivalent words.

Finally, $\phi(\psi[Hw]) = \phi(H\theta(w)) = [Hw]$ since we may choose w from the preimage of $\theta(w)$. In the other direction $\psi(\phi(Hg)) = \psi([Hx_g]) = H\theta(x_g) = Hg$ where x_g is an arbitrary element such that $\theta(x_g) = g$.

The other lemma we want is that CRSs actually exist. In fact, a coset presentation actually defines an associated CRS.

Lemma 12 *If $P = \langle X, S, Y\rangle$ is a coset presentation, define*

$$P_G = S \quad \textit{and} \quad P_H = \{(Hy, H) \mid y \in Y\} \cup \{(Hy^-, H) \mid y \in Y\}$$

Then $P_0 = \langle P_G, P_H\rangle$ is a CRS henceforth called the initial CRS generated by P.

Proof. We have three conditions to verify. The first is trivial and so is the second since if $y \in Y$, then $\theta(y), \theta(y)^{-1} \in H$. Next, let K consist of those elements $h \in H$ such that there is a word z such that $\theta(z) = h$ and $Hz \sim_R H$. We want to prove $H \subseteq K$. Clearly K contains all elements of the form $\theta(y)$ for $y \in Y$. K is also trivially closed under multiplication. We finish by showing K is closed under inverses. So let $h \in K$ with, say, $\theta(z) = h$ and $Hz \sim_R H$. Recall there is a $z^- \in X^*$ such that $\theta(z^-) = h^{-1}$ and hence $\theta(zz^-) = 1$. Thus $zz^- \sim_S 1$ and

$$Hz^- \sim_{P_H} Hzz^- \sim_S H$$

and so $Hz^- \sim_{P_0} H$ with $\theta(z^-) = h^{-1}$ as required.

We define $P^= = P_0 + P_0^{-1}$ which, by lemma 10, is also a CRS. The final part of the lemma follows from lemma 10. Given that a coset presentation defines an initial CRS, we now prove that Knuth-Bendix completion of a CRS produces a CRS. We do this in two stages to ensure that we get a complete rewriting system to decide the equality $\sim_S$ defining the group G.

Lemma 13 *Let $R = \langle R_G, R_H\rangle$ be a CRS for a coset presentation $P = \langle X, S, Y\rangle$. If R_G^c is the Knuth-Bendix completion of R_G then $\langle R_G^c, R_H\rangle$ is a CRS for P.*

Proof. Knuth-Bendix completion doesn't alter the strength of the associated congruence. Thus $\sim_{R^c_G}$ is the same as $\sim_{R_G}$. The second property trivially holds, while the third property follows for the same reason as the first.

Knuth-Bendix completion of a CRS also involves an analysis for $R_G - R_H$ critical pairs and $R_H - R_H$ critical pairs and consequently adding new R_H-rewrites to the CRS. The iterative step of this part of the completion considers spans $Hw \to^*_R Hu$ and $Hw \to^*_R Hv$ where Hu and Hv are $\to_R$ normal forms and adds a rewrite $Hu \to_{R_H} Hv$ or $Hv \to_{R_H} Hu$ depending on which term is larger in the termination order.

Lemma 14 *Knuth-Bendix completion of a CRS results in a CRS.*

Proof. We have already dealt with the analysis of $R_G - R_G$ critical pairs. Assume we have a CRS R_n and a critical pair $Hw \to^*_{R_n} Hu$ and $Hw \to^*_{R_n} Hv$ which cannot be completed. We then introduce a new R_H-rewrite $Hu \to Hv$ or vice versa depending upon the termination order. Clearly the first and third condition of a CRS holds after the addition of this rewrite. For the second condition, note that Hu and Hv belong to the same $\sim_{R_n}$ equivalence class. From lemma 11, we conclude that $\psi(Hu) = \psi(Hv)$. Since $H\theta(u) = \psi(Hu)$ and $H\theta(v) = \psi(Hv)$, the second condition is also preserved by the addition of this new rewriting rule.

We now have our first key theorem, namely that if the Knuth-Bendix procedure terminates, coset equivalence is decidable.

Theorem 15 *Assume the Knuth-Bendix procedure terminates. Then given two elements $g, g' \in G$, it is decidable if $Hg = Hg'$.*

Proof. Let R be the CRS resulting from Knuth-Bendix completion in lemma 14 of the initial CRS arising from the coset presentation as described in lemma 12. Further, let $\theta(x_g) = g$ and $\theta(x_{g'}) = g'$. Then $Hg = Hg'$ iff $Hx_g \sim_R Hx_{g'}$ and this later condition can be decided by reducing to normal form.

4 Logged Coset Rewriting System

The second step in our algorithm is to label the rewrites of a CRS which provides proof terms or witnesses for the coset membership problem. By equating those labels which arise from critical pair completion we get our presentation for the subgroup of a coset presentation.

A logged coset rewriting system is simply a rewriting system with proof terms attached to indicate why a term rewrites to another. This is similar in nature to what happens in *rewriting logic* [10] and can be traced back to Levy's *permutation equivalence* [9]. In a different context, the same idea also arises in 2-categorical and sesqui-categorical models of rewriting [12, 13]. Although we use the formal language of sesqui-categories because they provide the most concise language to express our constructions, they do not hide any difficult mathematics and are simply an efficient organisational device. Readers not familiar with sesqui-categories should therefore still be able to follow the argument.

Firstly we give the labels for rewrites. A one-step rewrite will be labelled by the rewrite used and the context within which it is used. For a CRS $\langle R_G, R_H \rangle$, this context is a pair of words if the rule comes from R_G and simply a word if the rule is in R_H. A rewrite sequence will be labelled by a sequence of such one-step labels making sure that the sources and targets match for the sake of well-formedness.

Definition 16 (Theory of a CRS) *Given a CRS $R = \langle R_G, R_H \rangle$ for a coset presentation $P = \langle X, S, Y \rangle$, the theory of R, written S_R, consists of all elements of the following form: $u_1\rho_1v_1 \dots u_n\rho_nv_n$ where*

- *Each $\rho_i \in R_G$ or $\rho_i \in R_H$.*
- *If $\rho_i \in R_G$, then $u_i \in HX^*$ and $v_i \in X^*$.*
- *If $\rho_i \in R_H$, then $u_i = 1$ and $v_i \in X^*$.*
- *Sources/targets of adjacent rewrites match: $u_i tgt(\rho_i) v_i = u_{i+1} src(\rho_{i+1}) v_{i+1}$*

An abstract definition of S_R is as the free sesqui-category on the following graph:

$$\begin{tikzcd} \bullet \arrow[r, "H"] & \bullet \arrow[loop right, "X^*"] \end{tikzcd}$$

with 2-cells consisting of the rewriting rules of $\rightarrow_R$. That S_R is a sesqui-category is just a quick way of saying that rewrite sequences with adjacent sources and targets can be composed in an associative manner with a unit, and that rewrites can be composed on the left and right by words, ie rewrites can be placed in context. The arrow H reflects the fact that R_H rewritings can only be composed on the right. S_R is not a 2-category as the permutation law of Levy equivalence or, equivalently, the interchange laws of a 2-category [13] do not hold.

These labels contain too much information for obtaining a presentation of the subgroup of a coset presentation. For example when we perform Knuth-Bendix completion we don't want to add new labels for the rewriting rules added by the completion process. Rather we want to use the span which led to the addition of a new rewriting rule as its label. We describe the quotienting of this extra information by a sesqui-functor and call this a logged coset rewriting system.

Definition 17 (Logged Coset Rewriting System) *Given a coset presentation $P = \langle X, S, Y \rangle$, a logged coset rewriting system (LCRS) consists of a CRS R and a sesqui-functor $F : S_R \longrightarrow S_{P^=}$ which is the identity on 0- and 1-cells.*

The fact that F is an identity on 0-cells and 1-cells means all F does is to associate each label from a CRS R with a label from the CRS $P^=$ which recall is the symmetric closure of the initial CRS P_0. We call the functor F, the log functor of the LCRS. Of course, the initial CRS P_0 is a logged CRS with the obvious inclusion functor $F : S_{P_0} \longrightarrow S_{P^=}$. As implied above, Knuth-Bendix completion not only maps CRSs to CRSs, but also LCRSs to LCRSs by replacing the label of each new rewriting rule by the span which it completed.

Lemma 18 *Let $L = \langle R, F\rangle$ be a LCRS. If R^c is the Knuth-Bendix completion of R, then there is a canonical LCRS $L^c = \langle R^c, F^c\rangle$.*

Proof. Assume at stage n, we have a CRS R_n and log functor $F_n : S_{R_n} \longrightarrow S_{P^=}$. Given a span $\alpha_1, \alpha_2 : Hw \to^*_{R_n} Hw_1, Hw_2$ with Hw_1 and Hw_2 in R_n-normal form, not only do we form the new CRS by adding a rule, say, $Hw_1 \to Hw_2$ to obtain the CRS R_{n+1}, but we also freely generate a log functor $F_{n+1} : S_{R_{n+1}} \longrightarrow S_{P^=}$ by setting the log of the rewrite $Hw_1 \to Hw_2$ to be $(F_n\alpha_1)^{-1}F_n\alpha_2$.

So the log functor translates the rewrites of a Knuth-Bendix completed CRS into rewrites and their inverses from the initial CRS. The examples of Section 5 show how the logs for specific completed LCRSs are calculated. However, there is more information we wish to delete. For example all the rewrites in R_G describe the construction of the group G from words but tell us nothing about the subgroup H. Thus for the purposes of obtaining a presentation of H they have no computational content and hence we want to ignore them. To do this we wish to set their logs to 1. We also wish to throw away the context from a P_H rewrite and simply record the particular rules from P_H which were used. Thus we define a map $[\![.]\!] : S_{P^=} \longrightarrow (Y+Y)^*$ as follows:

$$\begin{array}{lll} [\![\alpha w]\!] &= y & \text{if there is a } y \in Y+Y \text{ such that } \alpha = (Hy, H) \in P_H \\ [\![\alpha^{-1} w]\!] &= y^- & \text{if there is a } y \in Y+Y \text{ such that } \alpha^{-1} = (H, Hy) \in P_H^{-1} \\ [\![\alpha^{-1} w]\!] &= 1 & \text{if } \alpha \in P_G + (P_G)^{-1} \end{array}$$

We get a map $[\![.]\!] : S_{P^=} \to (Y+Y)^*$ by applying $[\![.]\!]$ as defined above to each logged rewrite in a rewrite sequence. Putting these maps together, for every LCRS $\langle R, F\rangle$, we have the following chain:

$$S_R \xrightarrow{F} S_{P^=} \xrightarrow{[\![.]\!]} (Y+Y)^* \xrightarrow{\hat{\theta}} H \qquad (1)$$

A category theorist will notice that we are abusing notation here in that F is a sesqui-functor, while $[\![.]\!]$ is mapping the 2-cells/logged rewrites of $S_{P^=}$ to a monoid and $\hat{\theta}$ is a monoid homomorphism. Nevertheless, equation 1 shows how rewrites in a LCRS are converted into words in $(Y+Y)^*$.

A crucial part of our algorithm is that elements of the generating set $(Y+Y)^*$, while usually regarded as either atomic symbols or words in X^*, can also be regarded as rewrites in P_0 and thus equality on such words can be axiomatised via equality of rewrites generated from Knuth-Bendix completion. This is shown by the following simple lemma:

Lemma 19 *Let $w \in (Y+Y)^*$ be a word. Then there is a rewrite sequence $r_w : Hw \to^*_{P_H} H$. Furthermore, $[\![r_w]\!] = w$.*

Proof. Define r_w by induction. If $w = 1$, set r_w to be the identity rewrite $H \to^*_{P_H} H$. If w is of the form yw' where $y \in Y + Y$, then we have a P_H-rewrite $\alpha_y : Hy \longrightarrow H$ and r_w can be defined as follows:

$$Hyw' \xrightarrow{\alpha_y w'} Hw' \xrightarrow{r_{w'}} H$$

The second half of the lemma is a trivial calculation.

By lemma 8, we know that H is the quotient of $(Y + Y)^*$ by $\sim_{\hat{\theta}}$. Since critical pair completion results in parallel pairs, proving that the equality derived from critical pair completion is contained in $\sim_{\hat{\theta}}$ is essentially the following lemma.

Lemma 20 *If $\beta : Hw \to^* Hz$ in the LCRS $P^=$, then $w \sim_{\hat{\theta}} [\![\beta]\!]z$. Thus if $\beta, \beta' : Hw \to^* Hz$, then $[\![\beta]\!] \sim_{\hat{\theta}} [\![\beta']\!]$.*

Proof. The first part of the lemma is clearly true if β is a one-step rewrite since i) if β is of the form urv for $r \in P_G$, then $[\![\beta]\!] = 1$ and $w \sim_S z$; ii) if β is of the form rv for $r = (Hy, H)$ for $y \in Y$, then $w = yv$, $[\![\beta]\!] = y$ and $z = v$; and iii) a similar argument holds when β is of the form rv for $r = (H, Hy) \in P_H^{-1}$. The result holds for many-step rewrites since the action of $[\![.]\!]$ on a sequence of rewrites is just the composition of the action of $[\![.]\!]$ on each one-step rewrite.

For the second part of the lemma, we have $[\![\beta]\!]z \sim_{\hat{\theta}} w \sim_{\hat{\theta}} [\![\beta']\!]z$. The result follows from cancellation of z using a word $z^- \in X^*$ such that $\theta(z^-) = \theta(z)^{-1}$

$$[\![\beta]\!] \sim_{\hat{\theta}} [\![\beta]\!]zz^- \sim_{\hat{\theta}} [\![\beta']\!]zz^- \sim_{\hat{\theta}} [\![\beta']\!]$$

We now give a presentation of the subgroup generated from a coset presentation.

Definition 21 *Let $L^c = \langle R^c, F^c \rangle$ be the LCRS arising from Knuth-Bendix completion of the initial LCRS. For each critical pair in R^c, $\alpha_1, \alpha_2 : Hw \to Hw_1, Hw_2$, there are completions $\beta_1, \beta_2 : Hw_1, Hw_2 \to Hw'$. Define $\mathcal{C}$ as follows:*

$$\mathcal{C} = \{(\alpha_1.\beta_1, \alpha_2.\beta_2) \mid \alpha_1, \alpha_2 \textit{ is such a critical pair } \}$$

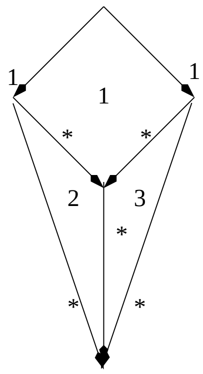
and the equations R_L by:

$$R_L = \{([\![F^c\gamma]\!], [\![F^c\gamma']\!]) \mid (\gamma, \gamma') \in \mathcal{C}\}$$

All that is left to do is prove that this really is a presentation for the subgroup H. Lemma 20 is the key to proving that critical pair equality is contained in $\sim_{\hat{\theta}}$ so not surprisingly the reverse inclusion depends upon what looks like a partial converse to lemma 20.

Lemma 22 *Let $\langle R^c, F^c \rangle$ be a complete logged rewriting system and assume there are rewrites $r_1 : Hw_1 \to^*_{R^c} H$ and $r_2 : Hw_2 \to^*_{R^c} H$ where $w_1 \sim_{R^c_G} w_2$. Then $[\![F^c r_1]\!] \sim_{R_L} [\![F^c r_2]\!]$.*

Proof. We first prove the lemma when $w_1 = w_2$ using a simple tiling argument by induction on the rank of w. If either rewrite has length 0, then so does the other (because of termination) and so the result is trivial. Otherwise we have the following situation:



where the first rewrite of r_1 and the first rewrite of r_2 have been completed via a critical pair in cell (1), while cells (2) and (3) are formed because the completion of this critical pair must rewrite to H. After applying $[\![F^c\_]\!]$ to the rewrites in this diagram, cell (1) commutes up to $\sim_{R_L}$ since it is formed by a critical pair, while cells (2) and (3) commute up to $\sim_{R_L}$ by induction. Thus $[\![F^c r_1]\!] \sim_{R_L} [\![F^c r_2]\!]$.

For the general case, w_1 and w_2 have a common R^c_G reduct and the lemma then follows from the argument above and the observation that for any R^c_G-rewrite sequence r, $[\![F^c r]\!] = 1$.

Finally, we prove our main theorem:

Theorem 23 *Assume $P = \langle X, S, Y\rangle$ is a coset presentation for a subgroup H of G which generates a complete logged rewriting system $L^c = \langle R^c, F^c\rangle$ as described above. Then $\langle Y + Y, R_L\rangle$ is a monoid presentation for H.*

Proof. By lemma 8, we know that $H = (Y + Y)^*/\sim_{\hat{\theta}}$ so the result follows by proving that the congruences $\sim_{\hat{\theta}}$ and $\sim_{R_L}$ are equal.

In one direction, consider a critical pair α_1, α_2 with completions β_1, β_2. Now $(\alpha_1.\beta_1, \alpha_2.\beta_2)$ is a parallel pair and hence by lemma 20 $[\![F^c(\alpha_1.\beta_1)]\!] \sim_{\hat{\theta}} [\![F^c(\alpha_2.\beta_2)]\!]$.

In the reverse direction, let $h \sim_{\hat{\theta}} k$. By lemma 19, there are logged rewrites in P_0 of the form $r_h : Hh \to H$ and $r_k : Hk \to H$. Since P_0 is a CRS, we also have that $Hh \sim_{P_G} Hk$. By lemma 22, $[\![r_h]\!] \sim_{R_L} [\![r_k]\!]$. Since $[\![r_h]\!] = h$ and $[\![r_k]\!] = k$ $h \sim_{R_L} k$ and hence $\sim_{\hat{\theta}}$ is contained in $\sim_{R_L}$.

5 S_3 and an Example with Infinite Cosets

We illustrate our algorithm with our running example of S_3 and another example showing the applicability of our algorithm to a situation where one has an infinite number of cosets. We have kept the examples simple so the reader can follow the examples without too many exhaustive Knuth-Bendix calculations.

Example 1: For S_3, we use the following coset presentation $P = \langle X, S, Y\rangle$:

$$X = \{a, b\} \quad S = \{(aaa, 1), (bb, 1), (abab, 1)\} \quad Y = \{a\}$$

The subgroup generated by a is $\{1, a, aa\}$ which has as presentation $mon\langle\ a \mid (aaa, 1)\ \rangle$. Our algorithm attempts to build a presentation based upon 2 generators a and a^-. Since $\theta(aa) = \theta(a)^{-1}$, the initial CRS $P_0 = \langle P_G, P_H\rangle$ is:

$$P_G = \{(aaa, 1), (bb, 1), (abab, 1)\} \qquad P_H = \{(Ha, H), (Haa, H)\}$$

To complete P_G, add rules $\{(bab, a^2), (ba^2, ab), (a^2b, ba), (aba, b)\}$,. To complete the CRS P_0 add the rule (Hba, Hb) since we have the span $r_a ba : Haba \to Hba$ and $Haba \to_{P_G^c} Hb$. As described in the proof of lemma 18, the application of $[\![F^c\_]\!]$ to any rewrite built from this new rewriting rule will be a^-. The equations of the presentation then come from analysis of the critical pairs. Two of these are given below where we have already applied $[\![F^c\_]\!]$ to the rewrites.

$$\begin{tikzcd}
 & Hbab \arrow[dl, "a^-"'] \arrow[dr, "1"] & \\
Hb^2 \arrow[d, "1"'] & & Ha^2 \arrow[d, "a"] \\
H & & Ha \arrow[ll, "a"]
\end{tikzcd}
\qquad
\begin{tikzcd}
 & Hbaba \arrow[dl, "a^-"'] \arrow[dr, "1"] & \\
Hb^2a \arrow[d, "1"'] & & Hb^2 \arrow[d, "1"] \\
Ha \arrow[rr, "a"'] & & H
\end{tikzcd}$$

The first diagram above comes from resolving the critical pair that occurs on $Hbab$ when the rules $Hba \to Hb$ and $bab \to a^2$ are applied. This gives us the relation $aa = a^-$. The second diagram shows the resolution of the pair $Hba \to Hb$ and $aba \to b$ on $Hbaba$, which gives us the relation $a^-a = 1$. Combining these we get $aaa = 1$. Analysis of other critical pairs gives no new equations and since a^- is definable from a we can delete this generator. Thus the subgroup generated by this coset presentation is the cyclic group of order 3.

Example 2: This example shows how the rewriting methods we describe can be applied to the problem of finding a presentation of a subgroup when the group, subgroup and the number of cosets are infinite.

Let G be the group generated by four elements $\{a, b, c, d\}$ of which the first pair a and b, commute with each other and the second pair c and d, also commute with each other. Let H be the subgroup generated by the four elements $\{ac, ca, bd, db\}$. The initial coset rewrite system then includes the rewrite rules for the group:

$$\begin{aligned}
\{\ &(aa^-, 1), (a^-a, 1), (bb^-, 1), (b^-b, 1), (cc^-, 1), (c^-c, 1), (dd^-, 1), (d^-d, 1),\\
&(ba, ab), (ba^-, a^-b), (b^-a, ab^-), (b^-a^-, a^-b^-),\\
&(dc, cd), (dc^-, c^-d), (d^-c, cd^-), (d^-c^-, c^-d^-)\}
\end{aligned}$$

This system is in fact complete. The rules of this type do not give us information about the subgroup, so we assign to each of them the identity label. The four generators of the subgroup give us four initial H-rules:

$$\{(Hac, H), (Hca, H), (Hbd, H), (Hdd, H)\},$$

which we label $\alpha_1, \ldots, \alpha_4$ respectively. These are the generators for our presentation of the group H. Their inverses, $\alpha_1^{-1}, \ldots, \alpha_4^{-1}$ are the following rules:

$$\{(Hc^-a^-, H), (Ha^-c^-, H), (Hd^-b^-, H), (Hb^-d^-, H)\}.$$

Logged completion uses the shortlex order with $a < a^- < b < b^- < \cdots < d^- < H$, identifies critical pairs and resolves them, adding new logged rules to the system. For example, $Ha^-c^- \to H$ by α_2^{-1} overlaps with $c^-c \to 1$ by 1. The resolution of this is as follows: $Ha^-c^-c \to Hc^-$ by using a rule labelled by α_2^{-1} and $Ha^-c^-c \to Ha^-$ by using a rule labelled by 1. This gives us the new rule $Hc \to Ha^-$ by α_2.

Similarly, $Hbd \to H$ by α_3 overlaps with $dc \to cd$ by 1. The resolution of this is as follows: $Hbdc \to Hc$ by using a rule labelled by α_3 and $Hc \to Ha^-$ by using a rule labelled by α_2 while $Hbdc \to Hbcd$ by using a rule labelled by 1. This gives us the new rule $Hbcd \to Ha^-$ by $\alpha_3\alpha_2$.

As a final example, the rule obtained above $Hbcd \to H$ by $\alpha_3\alpha_2^{-1}$ overlaps with $dd^- \to 1$ by 1. The resolution of this is as follows: $Hbcdd^- \to Ha^-d^-$ by using a rule labelled by $\alpha_3\alpha_2$ and $Hbcdd^- \to Hbc$ by using a rule labelled by 1. This gives us the new rule $Hbc \to Ha^-d^-$ by $\alpha_3\alpha_2$. We can now remove the previous rule $Hbcd \to Ha^-$ from the system, as this is implied by the new rule, together with $dd^- \to 1$.

After a few passes of the logged Knuth-Bendix algorithm we have the same group rules and the following H-rules:

$$\{\ (Hac, H), (Ha^-c^-, H), (Hbd, H), (Hb^-d^-, H), (Hc^-, Ha), (Hc, Ha^-), (Hd^-, Hb),$$
$$(Hd, Hb^-), (Hbc, Ha^-d^-), (Hbc^-, Had^-), (Hb^-c, Ha^-d), (Hb^-c^-, Had)\quad\}$$

with various labels. Now we seek the relations for the subgroup, by looking at the critical pairs of the completed system and noting the labelled rules which are used in resolving them. For example, $Hac \to H$ overlaps with $cc^- \to 1$. The resolution of this is as follows: $Hacc^- \to Hc^-$ by using the rule labelled by α_1 and $Hc^- \to Ha$ by using the rule labelled by α_1^{-1} and $Hacc^- \to Ha$ by using a rule labelled by 1. This gives us the relation $\alpha_1\alpha_1^{-1} = 1$. If we continue, checking all critical pairs, we find that every critical pair yields a trivial relation. Thus, H can be proven to be the free group on four generators.

6 Conclusion

We have presented an algorithm based upon rewriting for calculating a presentation for a subgroup of a finitely presentable group. Within this framework, the number of relations is computed via the critical pairs of a certain rewriting system. This makes it applicable to situations where the group, subgroup and the number of cosets are infinite. These examples cannot be tackled by the traditional Reidemeister-Schreier algorithm which has at its core an enumeration of the elements of the group. The key theoretical idea underpinning our algorithm is that the Knuth-Bendix completion procedure can give us not only a complete rewriting system, but also the nature of these completions contain valuable information.

We are currently thinking of taking this research in two directions. Firstly we wish to see our algorithm implemented and distributed so that it can be used by group theorists. A prototype has already been written for the GAP system and we are currently discussing with the GAP group ways to optimise it so as to improve its efficiency, etc. A couple of referees did comment on the practical viability of our algorithm. The general consensus [5] seems to be a practical one, namely that in any given situation we want to have as many methods available to try and the best solution may well be a mixture of several approaches.

In a more theoretical direction, there are a number of other algebraic structures, eg rings, modules, algebras, where the same problem of obtaining presentations for substructures arise and we are developing analogues of the algorithm presented in this paper to tackle these questions.

References

1. F.Baader and T. Nipkow : Term Rewriting and all That, *Cambridge University Press* 1998.
2. R. Book and F. Otto : String-Rewriting Systems, *Springer-Verlag, New York* 1993.
3. D.B.A. Epstein with J.W.Cannon et al : Word processing in groups, *Jones and Bartlett, Boston* 1992.
4. The GAP Group, 'GAP – Groups, Algorithms, and Programming, Version 4', Aachen, St Andrews, 1998, (`http://www-gap.dcs.st-and.ac.uk/~gap`).
5. Havas, Holt, Keene and Rees: Australian Mathematical Society 0263-6115/0 (1999) http://www.mas.ncl.ac.uk/ nser/abstracts/jams.ps.gz
6. A. Heyworth and C. D. Wensley : Logged rewriting with applications to identities among relations, *Groups St Andrews 2001 in Oxford, eds C. Campbell, E. Robertson and G. Smith, Cambridge University Press* (to appear).
7. D. Johnson : Presentations of Groups, *Cambridge University Press* 1990.
8. M. Johnson : Pasting diagrams in n-categories with applications to coherence theorems and categories of paths, *PhD thesis, University of Sydney,* 1988.
9. J.J. Levy: *Réductions correctes et optimales dans le λ-calcul*, Thèse d'Etat, Paris (1978).
10. J. Meseguer: Research Directions in Rewriting Logic, *Computational Logic, NATO Advanced Study Institute Series F, Vol. 165, pp. 345-398, Springer-Verlag,* 1999.
11. C. C. Sims : Computation with Finitely Presented Groups, *Cambridge University Press,* 1994.
12. J. G. Stell : *Modelling Term Rewriting Systems by Sesquicategories*, Technical Report TR94-02, University of Keele, 1994.
13. R. Street : *Categorical structures*, Handbook of Algebra, Vol. 1 pp.529–577, 1996.