UNIVERSITÄT KAISERSLAUTERN
Zentrum für Computeralgebra

REPORTS ON COMPUTER ALGEBRA
NO. 19

A note on nielsen reduction and coset enumeration

by

B. Reinert, K. Madlener, and T. Mora

February 1998

The Zentrum für Computeralgebra (Centre for Computer Algebra) at the University of Kaiserslautern was founded in June 1993 by the Ministerium für Wissenschaft und Weiterbildung in Rheinland-Pfalz (Ministry of Science and Education of the state of Rheinland-Pfalz). The centre is a scientific institution of the departments of **Mathematics, Computer Science, and Electrical Engineering** at the University of Kaiserslautern.
The goals of the centre are to advance and to support the use of Computer Algebra in industry, research, and teaching. More concrete goals of the centre include

- the development, integration, and use of software for Computer Algebra
- the development of curricula in Computer Algebra under special consideration of interdisciplinary aspects
- the realisation of seminars about Computer Algebra
- the cooperation with other centres and institutions which have similar goals

The present coordinator of the Reports on Computer Algebra is:
Olaf Bachmann (email: `obachman@mathematik.uni-kl.de`)

Zentrum für Computeralgebra
c/o Prof. Dr. G.-M. Greuel, FB Mathematik
Erwin-Schrödinger-Strasse
D-67663 Kaiserslautern; Germany
Phone: 49 - 631/205-2850   Fax: 49 - 631/205-5052
email: `greuel@mathematik.uni-kl.de`
URL: `http://www.mathematik.uni-kl.de/~zca/`

A Note on Nielsen Reduction and Coset Enumeration

Birgit Reinert*
Klaus Madlener
Fachbereich Informatik
Universität Kaiserslautern
67663 Kaiserslautern
Germany

Teo Mora
DISI
Via Dodecaneso, 35
16146 Genova
Italy

February, 1998

Abstract

Groups can be studied using methods from different fields such as combinatorial group theory or string rewriting. Recently techniques from Gröbner basis theory for free monoid rings (non-commutative polynomial rings) respectively free group rings have been added to the set of methods due to the fact that monoid and group presentations (in terms of string rewriting systems) can be linked to special polynomials called binomials. In the same mood, the aim of this paper is to discuss the relation between Nielsen reduced sets of generators and the Todd-Coxeter coset enumeration procedure on the one side and the Gröbner basis theory for free group rings on the other. While it is well-known that there is a strong relationship between Buchberger's algorithm and the Knuth-Bendix completion procedure, and there are interpretations of the Todd-Coxeter coset enumeration procedure using the Knuth-Bendix procedure for special cases, our aim is to show how a verbatim interpretation of the Todd-Coxeter procedure can be obtained by linking recent Gröbner techniques like prefix Gröbner bases and the FGLM algorithm as a tool to study the duality of ideals. As a side product our procedure computes Nielsen reduced generating sets for subgroups in finitely generated free groups.

*The author was supported by the Deutsche Forschungsgemeinschaft (DFG).

1 Introduction

The principal aim of this paper is to establish a link between different methods for computing in groups available in the literature – methods from combinatorial group theory, methods from string rewriting theory and methods from Gröbner basis theory – by giving a coset enumerating procedure using Gröbner basis techniques.

One very popular procedure in combinatorial group theory is due to Todd and Coxeter and systematically enumerates all cosets of a finitely generated subgroup in a given finitely presented group [26]. Nielsen reduced sets allow the computation of Schreier coset representatives hence enabling syntactical solutions to the subgroup problem in finitely generated free groups [22]. Another approach to the study of groups stems from the fact that they can be presented as string rewriting systems and, hence, completion based procedures a la Knuth and Bendix can be applied [12]. Recently, some authors have started using Gröbner basis methods to model groups in appropriate rings and solve group theoretical problems in this setting [17, 4].

In [17] the existence of explicit connections between the word problem for monoids and groups and the ideal membership problem in free monoid and free group rings, respectively, as well as connections between the submonoid problem and the subalgebra problem and between the subgroup problem and the one-sided ideal membership problem is proven. These results strongly encourage people designing new algorithms for attacking monoid or group theoretical problems to look for methods in all three fields mentioned above. Here we want to present the fundamental results of Nielsen and Todd and Coxeter from combinatorial group theory using Gröbner basis techniques for free group rings. More on connections between the Todd-Coxeter coset enumeration procedure (abbreviated by TC in the following) and the Knuth-Bendix completion procedure (abbreviated by KB) for the special case of the trivial subgroup can be found in [2, 25].

A group $\mathcal{G}$ is called **finitely presented** if there is a finite set of **generators** Σ and a finite set of **relators** R such that $\mathcal{G}$ is isomorphic to the quotient of the free group generated by Σ modulo the congruence generated by R. Let $\bar{\Sigma} = \Sigma \cup \Sigma^{-1}$ where $\Sigma^{-1} = \{a^{-1} \mid a \in \Sigma\}$ denotes the set of formal inverses for the generators. The group elements then are represented as words on $\bar{\Sigma}$. In 1911 Dehn stated decision problems for groups, two of which will be studied here using coset enumeration: The **word problem** for a group is to decide whether two representations describe the same group element. The **subgroup problem** for a group is to decide for a group element and a subgroup of the group whether the element is in fact a member of the subgroup. Both problems are undecidable in general, but become decidable when restricted to special classes of groups. For finitely generated free groups the word problem can be solved by free reduction, i.e. by deleting occurrences of subwords of the form aa^{-1} and $a^{-1}a$ for $a \in \Sigma$. The subgroup problem can be solved using Nielsen reduced sets due to the fact that there is a lot of crucial information on the maximal parts of words which can cancel each other when multiplying generating elements of subgroups. A well established procedure for dealing with these two problems in the case of arbitrary finitely presented groups is Tc: Given a set of defining relators for the group $\mathcal{G}$ and a set of generators of the subgroup $\mathcal{H}$ (as words in the generators of $\mathcal{G}$) Tc enumerates the cosets of $\mathcal{H}$ in $\mathcal{G}$. Of course this process can only stop in case $\mathcal{H}$ has finite index in $\mathcal{G}$ and then Tc also provides the multiplication table of the cosets. Now given a word w in the generators of $\mathcal{G}$ we have that $w \in \mathcal{H}$ if and only if w is in the coset of the identity. Hence Tc provides a semi-decision procedure by determining, while enumerating cosets, whether w is in one of the cosets enumerated so far, and answering "yes" in case it is in the coset of the identity. It is obvious that the answer "no" can only be given in case the procedure terminates, since as long as more cosets are enumerated there is the possibility of cosets collapsing, i.e., even if w is found in a coset which is not the identity it might later on be derived that the coset coincides with the coset of the identity. Notice that when choosing the trivial group as the subgroup $\mathcal{H}$ Tc in fact enumerates all elements of the group $\mathcal{G}$ and terminates if and only if $\mathcal{G}$ is finite.

Group presentations can be interpreted as string rewriting systems and this field is well studied (compare [3]). The most important procedure is due to Knuth and Bendix and allows computing convergent[1] presentations for groups. In case such a presentation is additionally finite it can be used to compute unique normal forms for the group elements and hence to decide the word problem for the group. The advantage is that this method is often still applicable to infinite groups. For an overview see e.g. [3] and [13]. The presentation of a finitely generated free group in terms of the inverse relators can be interpreted as a convergent string rewriting system and free reduction is exactly reduction using this string rewriting system. In [2] it is outlined how Tc and Kb are related for the special case of the *trivial* subgroup: for a modified version of Tc, which represents the cosets by appropriate words on $\bar{\Sigma}$ and uses a certain strategy (depending on the ordering chosen for the words representing the elements of the group) to replace cosets when new equations are obtained, on termination the output of Kb is a subset of the rules corresponding to the equations generated by Tc. What now are the essential differences between Tc and Kb in this case? In case Tc terminates so will a specialized version of Kb but the converse does not hold. This is due to the fact that Tc, when viewed as a rewriting procedure, does not apply ordinary string rewriting but *prefix rewriting*. Now if no finite convergent system with respect to prefix rewriting exists, Tc does not detect whether it might already have computed a convergent set of rules with respect to ordinary string rewriting and hence will not terminate although Kb might. Variants of prefix

[1]Convergent presentations for groups are string rewriting systems which are terminating and confluent.

rewriting have a long tradition when studying subgroups using string rewriting techniques (compare [13]). But there are two main differences: These techniques require certain assumptions for the relators defining the group (e.g. convergence) while Tc allows any presentation. The output gained by prefix string rewriting completion techniques is a description of cosets of the subgroup in the group while Tc enumerates cosets of the subgroup generated by the original subgroup generators and the normal closure of the relators in the corresponding free group. This difference explains why prefix string rewriting techniques can also handle cases where the subgroup has infinite index. A well-known algorithm can be found for free groups: In a finitely presented free group the subgroup problem can be solved using Nielsen reduced sets of generators and prefix string rewriting.
Kb techniques can be applied to complete group presentations as string rewriting systems. Sims incorporated prefix string rewriting techniques for the subgroup generators by decoding them as special rules of the form $\$u \longrightarrow \$$ where $\$$ is a new symbol. In [25] he compares running Kb on input $\{r \longrightarrow \lambda \mid r \in R\} \cup \{\$u \longrightarrow \$ \mid u \in U\}$ where R are the relators and U the subgroup generators to Tc. However, in general the completion does not terminate even for subgroups of finite index. This is due to the fact that it will always compute a convergent presentation for the group which need not be finite. In Section 5 we will outline how our procedure using Gröbner basis techniques can be "translated" into a Knuth-Bendix type procedure which simulates Tc *and* always terminates if the subgroup has finite index.
In this paper we present Tc in an unusual framework due to the fact that monoids and groups can be simulated by binomial ideals[2] in free monoid and free group rings. A first explicit connection between finitely presented *commutative* monoids and ideals in *commutative* polynomial rings was used 1958 by Emelichev yielding a solution to the word problem in the monoid by deciding the ideal membership problem (compare [18]): Assuming the commutative monoid $\mathcal{M}$ is presented by a set of generators $x_1, \ldots, x_n$ and a set of defining relations $\ell_1 = r_1, \ldots, \ell_m = r_m$ the following is true: A relation $u = w$ holds in $\mathcal{M}$ if and only if the polynomial $u - w$ lies in the ideal generated by the polynomials $\ell_1 - r_1, \ldots, \ell_m - r_m$ in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$. In his paper Emelichev uses the result of Hermann presented in [9] to show that the latter question is decidable. Of course the ideal membership problem is also solvable using Buchberger's method of Gröbner bases, which is based on a special reduction system associated to finite sets of polynomials which represent ideal congruences in polynomial rings [6].
It was observed independently in [20, 23, 17] that similar results hold for congruences on arbitrary finitely generated monoids and groups. Here we want to develop these ideas for the free group case in order to give a coset enumerating procedure using Gröbner techniques for free group rings:

[2]An ideal is called binomial if it has a basis solely consisting of polynomials of the form $m_1 - m_2$ where m_1, m_2 are monomials.

Let $\mathcal{F}$ denote the free group generated by $\Sigma = \{a_1, \ldots, a_n\}$. The elements of $\mathcal{F}$ are represented by the freely reduced words in $\bar{\Sigma}^*$ and multiplication of two elements, denoted by $\circ$, is just their concatenation followed by free reduction. In the following we will not distinguish between group elements and their representation. The empty word λ represents the unit in $\mathcal{F}$. By $\mathbb{K}[\mathcal{F}]$ we denote the **free group ring**, i.e. the set of finite formal sums $\sum_{i=1}^{k} \alpha_i \cdot t_i$, $\alpha_i \in \mathbb{K}\backslash\{0\}$, $t_i \in \mathcal{F}$ where $\cdot$ denotes multiplication with scalars and $*$ will denote multiplication in $\mathbb{K}[\mathcal{F}]$. The elements are called polynomials. The precedence $a_1 \prec a_2 \prec \ldots \prec a_n \prec a_1^{-1} \prec \ldots \prec a_n$ induces a length lexicographical ordering on $\mathcal{F}$ denoted by $\leq$ which is well-founded and total, but unfortunately not admissible for $\mathcal{F}$[3]. This ordering can be lifted to $\mathbb{K}[\mathcal{F}]$ and used to distinguish the **head term** $\mathsf{HT}(f)$, **head coefficient** $\mathsf{HC}(f)$ and **head monomial** $\mathsf{HM}(f)$ of a polynomial f and $\mathsf{HT}(F) = \{\mathsf{HT}(f) \mid f \in F\}$ for subsets F of $\mathbb{K}[\mathcal{F}]$ as usual. Identifying the elements of $\mathcal{F}$ by their representatives we define the syntactically motivated concept of prefix reduction: For two non-zero polynomials p, f in $\mathbb{K}[\mathcal{F}]$, we say f **prefix reduces** p to q at a monomial $\alpha \cdot t$, $\alpha \in \mathbb{K}\backslash\{0\}$, $t \in \mathcal{F}$ of p in one step, denoted by $p \longrightarrow^{\mathrm{p}}_{f} q$, if $\mathsf{HT}(f)$ is a prefix of t as a word (i.e. $\mathsf{HT}(f)w \equiv t$ for some $w \in \mathcal{F}$ where $\mathsf{HT}(f)w$ stands for the concatenation of $\mathsf{HT}(f)$ and w and $\equiv$ denotes identity as words) and $q = p - \alpha \cdot \mathsf{HC}(f)^{-1} \cdot f * w$. We will call a basis G of a right ideal $\mathfrak{i}$ in $\mathbb{K}[\mathcal{F}]$ a **prefix Gröbner basis** of $\mathfrak{i}$, if $\mathsf{HT}(\mathfrak{i}) = \{uw \mid u \in \mathsf{HT}(G), w \in \mathcal{F}\}$. G is called **reduced** if no polynomial in G is prefix reducible by another polynomial in G. As in the commutative case congruences on the free group $\mathcal{F}$ are modeled using special polynomials: A subset of the free group ring $\mathbb{K}[\mathcal{F}]$ is called a binomial basis of an ideal $\mathfrak{i} \subset \mathbb{K}[\mathcal{F}]$, if it consists solely of polynomials of the form $u - v$ where $u, v \in \mathcal{F}$ and $u > v$[4]. We will speak of **binomial ideals** in case they have a binomial basis. Such ideals are strongly related to the word problem in groups (compare [23, 17]) and hence are the appropriate connection to Tc. The FGLM algorithm[5] (see [7, 8, 19]) was introduced as a tool to study the duality of ideals: the central procedure Matphi enumerates as a bonus the set N (called the *natural basis* of G there) of terms which are irreducible by the Gröbner basis and a table for the multiplication of elements in N by variables. Therefore, by combining a generalization of the Matphi algorithm presented in [8] and prefix Gröbner bases [15, 16] we produce a coset enumeration procedure which is a verbatim interpretation of Tc. An implementation of the procedure was done in Mrc (a system for computing Gröbner bases in monoid and group rings developed at the University of Kaiserslautern).

[3]Notice that while λ is minimal with respect to $\leq$, the ordering is not compatible with multiplication as $\lambda < w$ then would imply $\lambda \circ w^{-1} = w^{-1} < w \circ w^{-1} = \lambda$.

[4]Those familiar with string rewriting systems should notice that prefix reducing a word u with a binomial $\ell - r$ where $\ell > r$ directly corresponds to prefix string reducing u with a rule (ℓ, r) followed by free reduction.

[5]The FGLM Algorithm has been generalized to the setting of finitely presented groups in [5].

The paper is organized as follows: In Section 2 we present the basics on Nielsen reduction and TC. Section 3 summarizes the necessary results from Gröbner basis theory which are applied in Section 4 to give a coset enumeration procedure based on prefix Gröbner bases in free group rings. Section 5 summarizes our results and points out how our procedure can be transformed into a Knuth-Bendix type completion procedure directly comparable to TC.

2 The Subgroup Problem

Computational group theory provides two classical methods for dealing with the subgroup problem: Nielsen reduced sets for subgroups in finitely generated free groups and coset enumeration for subgroups in finitely presented groups.

2.1 Nielsen Reduction

Let us start by giving a short description of Nielsen's method, which can be found in more detail e.g. in [14]. Let $\mathcal{F}$ be a free group with generating set Σ. We call a word $w \equiv w_1 \dots w_k$, $w_i \in \mathcal{F}$, **reduced**, in case $w = w_1 \circ \dots \circ w_k$, i.e., $|w| = \sum_{i=1}^{k} |w_i|$. Subsets of $\mathcal{F}$ are written as $U = \{u_i \mid i \in \mathbb{N}\}$ or $U = \{u_1, \dots, u_n\}$ depending on whether they are finite or not. The subgroup generated by U is the set $\{s_1 \circ \dots \circ s_k \mid k \in \mathbb{N}, s_i \in U \cup U^{-1}\}$ where $U^{-1} = \{u^{-1} \mid u \in U\}$. Then we can define **elementary Nielsen transformations** on a set U as follows:

(T1) Replace some $u_i \in U$ by u_i^{-1}, where u_i^{-1} denotes the inverse of u_i.

(T2) Replace some $u_i \in U$ by $u_i \circ u_j$ where $j \neq i$.

(T3) Delete some $u_i \in U$ where $u_i = \lambda$.

In all three cases it is understood that the u_l remain unchanged for $l \neq i$. A product of such elementary transformations is called a **Nielsen transformation**.

Lemma 1 *If a subset U of $\mathcal{F}$ is carried into a set U' by a Nielsen transformation, then U and U' generate the same subgroup.*

We call a set U **Nielsen reduced**, if for all $v_1, v_2, v_3 \in U \cup U^{-1}$ we have :

(N0) $v_1 \neq \lambda$;

(N1) $v_1 \circ v_2 \neq \lambda$ implies $|v_1 \circ v_2| \geq \max\{|v_1|, |v_2|\}$;

(N2) $v_1 \circ v_2 \neq \lambda$ and $v_2 \circ v_3 \neq \lambda$ imply $|v_1 \circ v_2 \circ v_3| > |v_1| - |v_2| + |v_3|$.

Nielsen reduced sets play an important role, as they are free generating sets for the subgroup they generate. The following theorem due to Zieschang states that freely reducing a product of elements of a Nielsen reduced set cannot result in arbitrary cancellations on the elements involved.

Theorem 2 *Let U be a Nielsen reduced set. Then for every $u \in U \cup U^{-1}$ there are words $a(u)$ and $m(u)$ with $m(u) \neq \lambda$ such that $u \equiv a(u)m(u)(a(u^{-1}))^{-1}$ and if $w = u_1 \circ \ldots \circ u_n$ for some $u_i \in U \cup U^{-1}$, $u_i \circ u_{i+1} \neq \lambda$, then the words $m(u_i)$ remain uncanceled in the reduced form of w. In particular we get $|w| \geq n$.*

This property can be used to solve the subgroup problem using Nielsen reduced sets by computing Schreier coset representatives by prefix rewriting.

Theorem 3 *Let $U \subseteq \mathcal{F}$ be a finite set. Then there is a Nielsen transformation from U into some Nielsen reduced set V.*

The proof of this theorem provided in [14] is constructive and gives rise to a procedure for transforming a finite generating set of a subgroup into a Nielsen reduced set. There are well-known algorithms for performing this task and Avenhaus and Madlener have provided one which works in polynomial time (see [1]). We will see later on how this can be done using prefix Gröbner bases.

2.2 The Todd-Coxeter Coset Enumeration Procedure

The Todd-Coxeter coset enumeration (Tc) is a famous method from combinatorial group theory for studying finitely presented groups (see e.g. [21, 10, 25] for detailed descriptions). It is based on the following fundamental observations: Presenting a group $\mathcal{G}$ in terms of generators Σ and relators R corresponds to viewing it as the quotient of the free group $\mathcal{F}$ (generated by Σ) by the normal subgroup $\mathcal{N}$ generated by R. $\mathcal{N}$ can be viewed as the subgroup of $\mathcal{F}$ generated by $N(R) = \{w \circ r \circ w^{-1} \mid w \in \mathcal{F}, r \in R\}$. Notice that if R is finite, $\mathcal{N}$, while finitely generated as a normal subgroup of $\mathcal{F}$, need not be finitely generated as a subgroup.

Now given a subgroup $\mathcal{U}$ of $\mathcal{G}$ for $g \in \mathcal{G}$ we can study the **cosets** $\mathcal{U}g = \{u \circ g \mid u \in \mathcal{U}\}$ of $\mathcal{U}$ in $\mathcal{G}$. Since for $g, h \in \mathcal{G}$ either $\mathcal{U}g = \mathcal{U}h$ or $\mathcal{U}g \cap \mathcal{U}h = \emptyset$ the group $\mathcal{G}$ is a disjoint union of cosets and the number of different cosets is called the **index** $|\mathcal{G} : \mathcal{U}|$ of $\mathcal{U}$ in $\mathcal{G}$. We know that if $\mathcal{U}$ is generated by a set $U \subseteq \mathcal{G}$ the index of $\mathcal{U}$ in $\mathcal{G}$ is the same as the index of the subgroup $\mathcal{H}$ generated by $U \cup N(R)$ in $\mathcal{F}$. While it is undecidable whether a subgroup has finite index in a group, Tc attempts to *verify* whether the index is finite.

In the following we will always assume that the group $\mathcal{G}$ and the subgroup $\mathcal{U}$ are finitely presented respectively generated, i.e. the sets Σ, R and U are finite. Moreover, Tc requires that each generator should occur in at least one relator. Tc tries to compute the index of $\mathcal{U}$ in $\mathcal{G}$ using the following two facts for cosets: For $u \in U$ we have $\mathcal{U}u = \mathcal{U}$ and for $r \in R$ and any coset $\mathcal{U}g$, $g \in \mathcal{G}$ we have $\mathcal{U}(g \circ r \circ g^{-1}) = \mathcal{U}$.

The procedure proceeds by filling two different kinds of tables with coset representatives, (one row) tables for the subgroup generators $u \equiv x_1 \ldots x_k$ of the form

$$
\begin{array}{c|c|c c|c|c}
\multicolumn{2}{c}{x_1} & & \ldots & \multicolumn{2}{c}{x_k} \\
\hline
\lambda & & & & & \lambda
\end{array}
$$

and (possibly infinite row) tables for the relators $y_1 \ldots y_m$ of the form

$$
\begin{array}{c|c|c c|c|c}
\multicolumn{2}{c}{y_1} & & \ldots & \multicolumn{2}{c}{y_m} \\
\hline
\lambda & & & & & \lambda \\
\vdots & & & & & \vdots
\end{array}
$$

Depending on the strategy used for choosing the next slot in the tables different types of equations (called defining, bonus and collapse) are deduced. While most versions of Tc simply use numbers to represent the cosets, it is possible to describe them using appropriate words as coset representatives. Then the deduced equations $w_i \circ a = w_j$, where w_i, w_j are words representing cosets and $a \in \bar{\Sigma}$, lead to word equations $w_i a = w_j$ or $w_i' = w_j$ depending on whether the last letter of w_i is a^{-1} or not. If $w_i a \equiv w_j$ or $w_i' \equiv w_j$ (i.e. the words of the left and right side are identical) the equations are called *trivial*. Otherwise they are ordered with respect to a well-founded ordering (in our case the length lexicographical ordering defined in the previous section) and used as a prefix string rewriting system (modulo free group reduction[6]) to simplify the existing equations. Of course such a simplification can lead to new rules and to a new simplification and so on. More details of this strategy can be found in [2, 24]. We only list some of the properties and their interpretations here: If the index of $\mathcal{U}$ in $\mathcal{G}$ is finite the procedure halts and produces a prefix closed set of coset representatives and a multiplication table with entries $w \circ a$ for each coset w and each $a \in \bar{\Sigma}$. The (unique) coset representative for any word in $\bar{\Sigma}^*$ can be computed by tracing it through the multiplication table starting with λ or equivalently by using the multiplication table as a prefix string rewriting system as follows: To each coset w, each $a \in \bar{\Sigma}$ and the respective coset w_a corresponding to $w \circ a$, associate a rule[7] $w \circ a \longrightarrow w_a$ which is either of the form $wa \longrightarrow w_a$ or $w' \longrightarrow w_a$ depending on whether the last letter of w is a^{-1}.
Let us illustrate these findings with an example from [10], page 71:

Example 4
Let $\mathcal{G}$ be the Dyck group $D(3,3,2)$ presented by $\Sigma = \{a, b\}$ and $R = \{aaa, bbb, abab\}$ and $\mathcal{U}$ the subgroup of $\mathcal{G}$ generated by $\{a\}$. The index of $\mathcal{U}$ in $\mathcal{G}$ is 4 and Tc (using the length lexicographical ordering induced by $a \prec b \prec a^{-1} \prec b^{-1}$) computes the coset representatives $\{\lambda, b, b^{-1}, ba^{-1}\}$, the multiplication table

[6] We say a free reduced word $w \in \mathcal{F}$ prefix reduces to v (modulo free group reduction) using a rule $\ell \longrightarrow r$ if there exists $x \in \mathcal{F}$ such that $w \equiv \ell x$ and $v = r \circ x$.

[7] Notice that there are trivial rules among these where the left and right hand sides coincide as words and these of course have to be removed in order to make the system terminating.

	a	b	a^{-1}	b^{-1}
λ	λ	b	λ	b^{-1}
b	b^{-1}	b^{-1}	ba^{-1}	λ
b^{-1}	ba^{-1}	λ	b	b
ba^{-1}	b	ba^{-1}	b^{-1}	ba^{-1}

which corresponds to the prefix string rewriting system (omitting trivial rules) $a \longrightarrow \lambda$, $a^{-1} \longrightarrow \lambda$, $ba \longrightarrow b^{-1}$, $bb \longrightarrow b^{-1}$, $b^{-1}a \longrightarrow ba^{-1}$, $b^{-1}a^{-1} \longrightarrow b$, $b^{-1}b^{-1} \longrightarrow b$, $ba^{-1}b \longrightarrow b$, $ba^{-1}a^{-1} \longrightarrow b^{-1}$ and $ba^{-1}b^{-1} \longrightarrow ba^{-1}$.

The coset representative of the word aba can be deduced by either tracing the multiplication table: $\lambda \circ \mathbf{a} = \lambda$, $\lambda \circ \mathbf{b} = b$ and $b \circ \mathbf{a} = b^{-1}$, or by prefix reduction: $aba \longrightarrow^{\mathrm{p}}_{a \longrightarrow \lambda} ba \longrightarrow^{\mathrm{p}}_{ba \longrightarrow b^{-1}} b^{-1}$ In both cases we find that aba lies in the coset represented by b^{-1} which is in fact the minimal representative of this coset.

3 Towards Gröbner Bases

In commutative polynomial rings there is a strong relation between Gröbner bases of an ideal and its quotient ring. In fact Gröbner bases enable computations in the quotient ring by normal form computations. The quotient is determined as a $\mathbb{K}$-vector space by the **natural basis** associated to the reduced Gröbner basis of the ideal. This natural basis consists of those commutative terms which are irreducible with respect to the Gröbner basis, i.e. it is a regular subset of the commutative terms (when viewed as a formal language). Of course such a vector space basis is strongly dependent on the ordering chosen for computing the Gröbner basis. In [8] the procedure MATPHI is presented which, given a reduced Gröbner basis, enumerates the natural basis: This is done systematically by initializing the natural basis to $N = \{\lambda\}$ and the set of border elements to $B = \{X_i \mid X_i \text{ is a variable of the polynomial ring}\}$. While there are elements in B the minimal one τ is removed and it is checked whether it is irreducible with respect to the Gröbner basis. If this is the case for each new element τ added to N the border elements τX_i are added to B. On termination N contains the natural basis. Additionally MATPHI computes a multiplication table which for each $m \in N$ and each variable X_i contains the result of the normal form computation $\mathsf{normal.form}(mX_i, \longrightarrow_G)$. While in general the entries of this multiplication table are vectors, when restricted to binomial polynomials they can be interpreted as terms. Notice that then the output is similar to the one produced by TC where on termination we get a set of coset representatives and a multiplication table $g \circ a$ for all coset representatives g and $a \in \bar{\Sigma}$.

However, MATPHI works in the setting of commutative polynomial rings using a Gröbner basis as input while TC belongs to the setting of groups using arbitrary relators and subgroup generators as input. In order to compare both methods, we have to use the generalized setting presented in Section 1 – binomial ideals in free group rings – and enable the new procedure to deal with possibly infinite

generating sets $U \cup N(R)$ in a finitary manner.
To encode the input of TC as binomials we associate the relators R and the subgroup generators U with two sets of polynomials $F_R = \{r - 1 \mid r \in R\}$ and $F_U = \{u - 1 \mid u \in U\}$. Essentially we want to check whether the subgroup generated by $U \cup N(R)$ in $\mathcal{F}$ is finitely generated and this will be done in an incremental fashion using the fact that for a given finitely generated subgroup of a free group the membership problem can be solved using prefix Gröbner bases and the generating subset of the subgroup is then enlarged by adding polynomials modified by left multiplication with suitable group elements in order to "approximate" $N(R)$.
To compute prefix Gröbner bases of subgroups in the free group ring $\mathbb{K}[\mathcal{F}]$ we need the concept of weak prefix saturation: A set $F \subseteq \mathbb{K}[\mathcal{F}]$ is called **weakly prefix saturated** if for every $p \in F$, $w \in \mathcal{F}$ we have $p * w \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$. This becomes necessary as the ordering on $\mathbb{K}[\mathcal{F}]$ is no longer admissible (see [23] for the details).

Theorem 5 ([23]) *A set $F \subseteq \mathbb{K}[\mathcal{F}]$ is a prefix Gröbner basis of the right ideal it generates if it is prefix reduced and weakly prefix saturated.*

The property of being weakly saturated can be ensured for a set of polynomials by using a procedure to compute a saturating set for a polynomial, i.e. a set such that each right multiple of the polynomial prefix reduces to 0 in *one* step by a polynomial in the saturating set. For free groups there are saturating sets consisting of at most two polynomials called can and acan. In our setting of binomials $u - v$, informally $\mathsf{can}(u - v)$ is gained from $u - v$ by "shortening" the head term u without losing its head position while $\mathsf{acan}(u - v)$ is derived from $\mathsf{can}(u-v)$ by forcing the shortened head term to lose its head position by cutting off its last letter. Then $\mathsf{can}(u-v) = xa - y$ and $\mathsf{acan}(u-v) = (xa-y) \circ a^{-1}$ where $x, y \in \mathcal{F}$, $a, a^{-1} \in \bar{\Sigma}$ and there exists $w \in \mathcal{F}$ such that $u \equiv xaw$, $y = v \circ w^{-1}$, $\mathsf{HT}(\mathsf{can}(u - v)) = \mathsf{HT}((u - v) \circ w^{-1}) = u \circ w^{-1} \equiv xa$ and $\mathsf{HT}(\mathsf{acan}(u - v)) = \mathsf{HT}((u - v) \circ w^{-1}a^{-1}) = v \circ w^{-1}a^{-1} \equiv ya^{-1}$.

Procedure: PREFIX GRÖBNER BASES OF RIGHT IDEALS IN FREE GROUP RINGS

Given: A finite set $F \subseteq \mathbb{K}[\mathcal{F}]$.
Find: G, the monic reduced prefix Gröbner basis of the right ideal generated by F.

$G := \{\mathsf{can}(f), \mathsf{acan}(f) \mid f \in F\}$;
while there is $g \in G$ such that $\mathsf{HT}(g)$ is prefix reducible by $G\backslash\{g\}$ **do**
  $G := G\backslash\{g\}$;
  $f :=$ normal.form$(g, \longrightarrow^{\mathrm{p}}_{G})$;
  % Compute a normal form (if non-zero with head coefficient 1).
  if $f \neq 0$
    then $G := G \cup \{\mathsf{can}(f), \mathsf{acan}(f)\}$;
  endif
endwhile

Correctness and termination follow from the results presented in [23, 16]. The procedure can be used to solve the subgroup problem for a subgroup in $\mathcal{F}$:

Theorem 6 ([15]) *Let U be the generating subset of a subgroup $\mathcal{U}$ in $\mathcal{F}$. Then $w \in \mathcal{F}$ is an element of $\mathcal{U}$ if and only if w prefix reduces to 1 using a prefix Gröbner basis of the right ideal generated by $\{u - 1 \mid u \in U\}$ in $\mathbb{K}[\mathcal{F}]$.*

In [23] it was shown how the computation of the monic prefix Gröbner basis as well as the resulting solution for the subgroup problem are related to Nielsen reduction:

Theorem 7 *Let U be a finite subset of $\mathcal{F}$ and G the monic reduced prefix Gröbner of the right ideal generated by $\{u-1 \mid u \in U\}$ in $\mathbb{K}[\mathcal{F}]$. Then the set $X_G = \{uv^{-1} \mid u - v \in G\}$ is Nielsen reduced for U.*

However, in general the subgroup $\mathcal{H}$ of $\mathcal{F}$ we are interested in is generated by the set $U \cup N(R)$ where the set of relators is *not* empty. We have to find a way to treat this possibly infinitely generated subgroup of $\mathcal{F}$ in a finitary manner in order to verify whether it is in fact finitely generated. The normal closure of a set of relators R can be approached using a result similar to the one presented in [11] to solve the ideal membership problem for two-sided ideals in solvable polynomial rings using one-sided ideals (compare also Zharkov's idea to compute Janet bases in [27]). For a set $F \subseteq \mathbb{K}[\mathcal{F}]$ let $\mathsf{ideal}(F)$ denote the two-sided and $\mathsf{ideal}_r(F)$ the right ideal generated by F in $\mathbb{K}[\mathcal{F}]$.

Theorem 8 ([16]) *For $F \subseteq \mathbb{K}[\mathcal{F}]$ the following properties are equivalent:*

1. *F is a prefix Gröbner basis of $\mathsf{ideal}_r(F)$ and $\mathsf{ideal}_r(F) = \mathsf{ideal}(F)$.*
2. *F is a prefix Gröbner basis of $\mathsf{ideal}_r(F)$ and for all $w \in \mathcal{F}$, $p \in F$ we have $w * p \in \mathsf{ideal}_r(F)$.*
3. *F is a prefix Gröbner basis of $\mathsf{ideal}_r(F)$ and for all $a \in \bar{\Sigma}$, $p \in F$ we have $a * p \in \mathsf{ideal}_r(F)$.*

This theorem is the basis of a procedure which computes prefix Gröbner bases of two-sided ideals by iterating the computation of prefix Gröbner bases and extending them by multiplication with elements in $\bar{\Sigma}$ until a prefix Gröbner basis of the two-sided ideal is computed. For a set of relators R, on input $F_R = \{r - 1 \mid r \in R\}$ this is equivalent to computing a prefix Gröbner basis of an encoding of the the normal closure of R and it halts if and only if the subgroup generated by $N(R)$ in $\mathcal{F}$ is finitely generated. This will be a special case of the procedure presented in the next section.

4 Enumerating Cosets Using Gröbner Techniques

Let $\mathcal{G}, \mathcal{U}, \mathcal{H}$ and Σ, R, U be as defined before. In this section we combine the ideas presented in Section 3 in order to give a procedure with the following output:

1. If $R = \emptyset$ the procedure terminates with the monic prefix Gröbner basis G which allows to decide the subgroup problem for the subgroup generated by U in $\mathcal{F}$ and to compute the Schreier coset representatives (with respect to $>$). The set $\{uv^{-1} \mid u - v \in G\}$ is Nielsen reduced for U.

2. If $R \neq \emptyset$ then, similar to the Todd-Coxeter procedure, the procedure enumerates cosets of the subgroup generated by $U \cup N(R)$ in $\mathcal{F}$ and on termination provides the set of all coset representatives of $\mathcal{H}$ in $\mathcal{F}$ and the multiplication table for the cosets with elements in $\bar{\Sigma}$ encoded in the prefix Gröbner basis.

In contrast to Tc we do *not* need the assumption that each generator occurs in at least one relator.
Let us start by giving an informal description of our procedure: The input are encodings of the relators R and the subgroup generators U in binomial sets $F_R = \{r - 1 \mid r \in R\}$ and $F_U = \{u - 1 \mid u \in U\}$, respectively. All ring operations take place in $\mathbb{K}[\mathcal{F}]$. The following sets are used by the procedure:

1. $N \subseteq \mathcal{F}$ contains potential coset representatives of $\mathcal{H}$ in $\mathcal{F}$. This set corresponds to the *natural basis* in Matphi.

2. $B \subseteq \mathcal{F}$ is a test set for possible coset representatives of $\mathcal{H}$ in $\mathcal{F}$. It corresponds to the *border set* in Matphi.

3. $H \subseteq \mathbb{K}[\mathcal{F}]$ is used to increment the generating set of the subgroup in order to achieve a generating set for $\mathcal{H}$.

4. $G \subseteq \mathbb{K}[\mathcal{F}]$ is the monic prefix Gröbner basis which is used to decide, whether the candidates in B are indeed coset representatives of the subgroup generated so far or not.

In the first step, the procedure checks, whether the set of relators is empty. If this is the case, the prefix Gröbner basis of the set F_U is computed[8] and the output of the procedure is this basis, which allows to solve the subgroup problem for $\mathcal{U}$ and can be transformed into a Nielsen reduced set for U according to Theorem 7. If the set of relators is not empty the procedure starts to enumerate cosets: The set N is initialized with the empty word which is the coset representative

[8]The steps in the computation of the prefix Gröbner basis can be directly related to Nielsen transformations (see [23]).

of the subgroup itself. N will remain prefix closed throughout the computation, i.e. it will contain all prefixes of its elements. The border set is $B = \{a \mid a \in \bar{\Sigma}\}$. The set G contains the monic prefix Gröbner basis[9] which allows to solve the subgroup problem for the subgroup generated by $U \cup R$. Now, while there are elements in B we proceed as follows: The smallest element τ of B is removed. Then if τ is not prefix reducible by G, it is added to N and all border elements τa are added to B where $a \in \bar{\Sigma} \backslash \{(\ell(\tau))^{-1}\}$ and $(\ell(\tau))^{-1}$ is the inverse of the last letter of the freely reduced word τ. Moreover, we compute the auxiliary set $H = \{\tau * (r-1) \mid r \in R\}$[10]. In computing the monic prefix Gröbner basis of the set $G \cup H$ we are then able to solve the subgroup problem for the subgroup now generated by the previous generating set extended by the generators $\tau \circ r \circ \tau^{-1}$. This of course corresponds to incrementally approaching the (infinite) generating set $U \cup N(R)$. According to the new prefix Gröbner basis we have to "correct" our set of possible cosets N. This is done by removing all elements with a prefix reducible with the new prefix Gröbner basis, as these elements are no longer coset representatives of the incremented subgroup[11]. Notice that this operation does not change the property of N of being prefix closed. The procedure terminates as soon as the set B becomes empty.

Procedure: EXTENDED TC SIMULATION

Given: $F_R = \{r - 1 \mid r \in R\}$, a set of binomials encoding the relators.
$F_U = \{u - 1 \mid u \in U\}$, a set of binomials encoding the subgroup generators.

$N := \emptyset$;
if $R = \emptyset$ **then** $G :=$ prefix.groebner.basis(F_U);
else $N := \{\lambda\}$;
  $B := \{a \mid a \in \bar{\Sigma}\}$;
  $G :=$ prefix.groebner.basis$(F_R \cup F_U)$;
  while $B \neq \emptyset$ **do**
    $\tau := \min_<(B)$;
    $B := B \backslash \{\tau\}$;
    if τ is not prefix reducible by G
    then $N := N \cup \{\tau\}$;
      $B := B \cup \{\tau a \mid a \in \bar{\Sigma} \backslash \{(\ell(\tau))^{-1}\}\}$;
      $H := \{\tau * (r-1) \mid r - 1 \in F_R\}$;
      $G :=$ prefix.groebner.basis$(G \cup H)$;
      $S := \{w \in N \mid w$ is prefix reducible by $G\}$;
      $N := N \backslash S$;
    endif

[9] The computation of the prefix Gröbner basis is related to the filling of the first line of the tables in TC and the deduction of equations

[10] The set H realizes the addition of subgroup generators $\tau \circ r \circ \tau^{-1}$ or in TC corresponds to marking the first and last slot of each relator table with the newly found coset representative τ.

[11] This corresponds to the coset collapses in TC.

endwhile
endif

On termination by construction N is either empty or a set of prefix closed coset representatives with respect to the ordering $>$. The latter is ensured as for each τ added to N the set B contains all border elements τa, $a \in \bar{\Sigma} \backslash \{(\ell(\tau))^{-1}\}$ and removing the set of elements $S = \{w \in N \mid w \text{ is prefix reducible by } G\}$ from N does not destroy the property of being prefix closed.
Moreover, we have the following important invariant for the case that R is not empty: Let N_o, B_o, G_o denote the sets when starting the execution of the while loop and N_n, B_n, G_n the ones at the end. Then for the sets N_n, B_n, and G_n at the end of each loop we have that for each w which is *not* prefix reducible by G_n one of the following three conditions holds:

1. $w \in N_n$, or
2. $w \equiv w_1 a$, $a \in \bar{\Sigma}$ and $w_1 \in N_n$, $w \in B_n$, or
3. $w \equiv w_1 a w_2$, $a \in \bar{\Sigma}$, $w_2 \in \mathcal{F}$ and $w_1 \in N_n$, $w_1 a \in B_n$.

This is true for the sets $N_o = \{\lambda\}$ and $B_o = \{a \mid a \in \bar{\Sigma}\}$ before entering the while loop. Notice that due to the construction the elements prefix irreducible with respect to G_n are a (not necessarily proper) subset of those prefix irreducible with respect to G_o. In the loop first the smallest element τ is removed from B_o. If it is prefix reducible by G_o the new sets are $N_n = N_o$, $B_n = B_o \backslash \{\tau\}$ and $G_n = G_o$ and the property still holds, since then τ cannot be a prefix of any element not prefix reducible by G_n. Now if τ is not prefix reducible by G_o it is first added to N and its border elements are added to B. We get $G_n = \mathsf{prefix.groebner.basis}(G_o \cup H)$, $N_n = (N_o \cup \{\tau\}) \backslash S$ and $B_n = (B_o \backslash \{\tau\}) \cup \{\tau \circ a \mid a \in \bar{\Sigma} \backslash \{(\ell(\tau))^{-1}\}\}$. Let w be prefix irreducible with respect to G_n. Then w was also prefix irreducible with respect to G_o and we have to check the three possible cases:

1. If $w \in N_o$, since w is still prefix irreducible by G_n it cannot be in S, hence $w \in N_n$.
2. If $w \equiv w_1 a$, $a \in \bar{\Sigma}$ and $w_1 \in N_o$, $w \in B_o$, as $w_1 \notin S$ we find $w_1 \in N_n$ and either $\tau \equiv w \in N_n$ or $w \in B_n$.
3. If $w \equiv w_1 a w_2$, $a \in \bar{\Sigma}$, $w_2 \in \mathcal{F}$ and $w_1 \in N_o$, $w_1 a \in B_o$, again as $w_1 \notin S$ we find $w_1 \in N_n$ and $\tau \equiv w_1 a \in N_n$ or $w_1 a \in B_n$.

For non-empty R the procedure will only terminate when B becomes empty. Then because of the invariant the set N must contain *all* elements of $\mathcal{F}$ which are not prefix reducible by the final set G. The next theorem now states that on termination the subgroup $\mathcal{H}$ generated by $U \cup N(R)$ in $\mathcal{F}$ is in fact finitely generated (by $\{uv^{-1} \mid u - v \in G\}$). G can be used to decide the subgroup problem for $\mathcal{H}$ by prefix reduction. Moreover, if R is not empty, G contains the respective (non-trivial) equations which are also generated by TC and encode the multiplication table for the cosets with generators as follows: For each polynomial $xa - y$ where $x, y \in \mathcal{F}$, $a \in \bar{\Sigma}$ we know that x and y are coset representatives and the corresponding entry in the table for x and a is $x \circ a = y$.

Theorem 9 *Let R and U be as specified above. If procedure* EXTENDED TC SIMULATION *terminates, then the subgroup $\mathcal{H}$ generated by $U \cup \mathcal{N}(R)$ is finitely generated.*

Proof:
If the set of relators is empty $\mathcal{H}$ is generated by U and we are done. On the other hand, for non-empty R on termination the set G contains a prefix Gröbner basis which can be used to decide the subgroup membership problem for the subgroup $\mathcal{H}_1$ generated by the set $U \cup \{x \circ a \circ r \circ a^{-1} \circ x^{-1} \mid x \in N, a \in \bar{\Sigma}, r \in R\}$ in $\mathcal{F}$ (compare Theorem 6). We have to show that $\mathcal{H}_1$ is in fact $\mathcal{H}$, the subgroup generated by $U \cup N(R)$ in $\mathcal{F}$. This is done by proving that for any $w \in \mathcal{F}$, $r \in R$ the element $w \circ r \circ w^{-1}$ is in $\mathcal{H}_1$. Let us assume $\mathcal{H}_1 \neq \mathcal{H}$. Then there is $w \in \mathcal{F}$ minimal with respect to $>$ such that for appropriate $r \in R$ we have $w \circ r \circ w^{-1} \notin \mathcal{H}_1$. The case $w \in N$ immediately gives us a contradiction to our construction. Therefore, by our invariant w cannot be irreducible by G as this would imply $w \in N$. Hence let $w \equiv w_1 w_2$ such that w_1 is the head term of some polynomial $w_1 - v$ in G. Then we know $w_1 v^{-1} \in \mathcal{H}_1$ and $w > v \circ w_2$. Now we get $w \circ r \circ w^{-1} = w_1 v^{-1} \circ (v \circ w_2) \circ r \circ (v \circ w_2)^{-1} \circ (w_1 v^{-1})^{-1}$ and as w was a minimal counter example $(v \circ w_2) \circ r \circ (v \circ w_2)^{-1} \in \mathcal{H}_1$. But this implies $w \circ r \circ w^{-1} \in \mathcal{H}_1$ as $w_1 v^{-1}, (w_1 v^{-1})^{-1} \in \mathcal{H}_1$ contradicting our assumption. q.e.d.

Now, if $\mathcal{H}$ is finitely generated *and* contains a non-trivial normal subgroup then $\mathcal{H}$ has finite index in $\mathcal{F}$ (Proposition 3.11 in [14]). Since TC terminates in case $\mathcal{H}$ has finite index in $\mathcal{F}$ it remains to show that this is also the case for procedure EXTENDED TC SIMULATION.

Theorem 10 *Let R and U be as specified above. If the subgroup generated by $U \cup N(R)$ has finite index in $\mathcal{F}$, then procedure* EXTENDED TC SIMULATION *terminates.*

Proof:
Let the subgroup $\mathcal{H}$ generated by $U \cup N(R)$ in $\mathcal{F}$ have finite index. If the set of relators is empty then there is nothing to show. The set of coset representatives can for example be computed by enumerating the set of elements which are not prefix reducible by the obtained prefix Gröbner basis G of the right ideal generated by F_U.
Hence let us assume that R is not empty. As $\mathcal{F}$ is finitely generated $\mathcal{H}$ is also finitely generated (Proposition 3.9 in [14]) and hence has a finite Schreier transversal S. Then for $s \in S$, $a \in \bar{\Sigma}$ and every $s \circ a$ there exists just one $s_a \in S$ such that

$s \circ a \in \mathcal{H}s_a$. Since $s \circ a = h \circ s_a$ for some $h \in \mathcal{H}$ we have $s \circ a \circ {s_a}^{-1} = h \in \mathcal{H}$. The set $\{s \circ a \circ {s_a}^{-1} \mid s \in S, a \in \Sigma \cup \Sigma^{-1}\}$ generates $\mathcal{H}$ (compare Chapter 1 in [10]). But then $\{s \circ a \circ r \circ {s_a}^{-1}, s \circ r \circ s^{-1} \mid s \in S, a \in \bar{\Sigma}, r \in R\}$ again is a generating set for $\mathcal{H}$ as $s \circ a \circ {s_a}^{-1} = (s \circ a \circ r \circ {s_a}^{-1}) \circ (s_a \circ r^{-1} \circ {s_a}^{-1})$. Hence the procedure will terminate at least after checking the candidates $s \circ a$ for $s \in S$. q.e.d.

Reviewing Example 4 with $\Sigma = \{a, b\}$, $R = \{aaa, abab, bbb\}$ and $U = \{a\}$ we get the output $N = \{\lambda, b, b^{-1}, ba^{-1}\}$ and $G = \{a - 1, a^{-1} - 1, ba - b^{-1}, ba^{-1}a^{-1} - b^{-1}, ba^{-1}b - ba^{-1}, ba^{-1}b^{-1} - ba^{-1}, bb - b^{-1}, b^{-1}a - ba^{-1}, b^{-1}a^{-1} - b, b^{-1}b^{-1} - b\}$ which corresponds to the non-trivial part of the multiplication table on page 8 when interpreting the polynomials as described above: $\lambda \circ a = \lambda$, $\lambda \circ a^{-1} = \lambda$, $b \circ a = b^{-1}, (ba^{-1}) \circ a^{-1} = b^{-1}, (ba^{-1}) \circ b = ba^{-1}, (ba^{-1}) \circ b^{-1} = ba^{-1}, b \circ b = b^{-1}, b^{-1} \circ a = ba^{-1}, b^{-1} \circ a^{-1} = b, b^{-1} \circ b^{-1} = b$. Notice that the set G does not give us the trivial relations as $\lambda \circ x = x$ or $x \circ x^{-1} = \lambda$ for $x \in \bar{\Sigma}$. They can be applied to make the multiplication table complete. On the other hand G directly corresponds to the prefix string rewriting system in Example 4 by translating rules $u \longrightarrow v$ into polynomials $u - v$ and vice versa.

5 Conclusions

In this paper we have stated that there are strong links between the three fields combinatorial group theory, string rewriting theory and Gröbner basis theory when studying group theoretical problems as the word problem and the subgroup problem. The procedure EXTENDED TC SIMULATION has been presented in the setting of free group rings combining a generalization of the MATPHI procedure from [8] and prefix Gröbner bases from [15]. The implementation of the procedure (done in the system MRC developed at Kaiserslautern) will be compared to TC implementations.

Let us close this section by sketching how this result closes the gap in comparing TC to KB type procedures in string rewriting. The case of the trivial subgroup has successfully been treated in [2, 25] while for the general case a partial solution was presented in [25] which did not necessarily terminate for subgroups of finite index. Now using Knuth-Bendix techniques for prefix string rewriting systems we can give a procedure analogous to EXTENDED TC SIMULATION and hence to TC. We say the rule $\ell \longrightarrow r$ with $\ell > r$ *prefix rewrites* the word $u \in \bar{\Sigma}^*$ to v if ℓ is a prefix of u, say $u \equiv \ell w$, and $v \equiv rw$. Note that in this setting *no* free reduction steps are applied due to the fact that pure prefix string rewriting takes place in the free *monoid*. Therefore, we have to add the inverse relators $\{aa^{-1}, a^{-1}a \mid a \in \Sigma\}$ to the defining relators of the group. Let PREFIXKB be an algorithm which given a finite set of rules $\ell \longrightarrow r$, $\ell, r \in \bar{\Sigma}^*$, $\ell > r$ computes the reduced equivalent convergent system.

Given: $F_R = \{r \longrightarrow \lambda \mid r \in R\} \cup \{aa^{-1} \longrightarrow \lambda, a^{-1}a \longrightarrow \lambda \mid a \in \Sigma\}$,

$F_U = \{u \longrightarrow \lambda \mid u \in U\}$.

$N := \emptyset$;
if $R = \emptyset$ **then** $G := \mathsf{prefix.kb}(F_U)$;
else $N := \{\lambda\}$;
$B := \{a \mid a \in \bar{\Sigma}\}$;
$G := \mathsf{prefix.kb}(F_R \cup F_U)$;
while $B \neq \emptyset$ **do**
$\tau := \mathsf{min}_<(B)$;
$B := B \backslash \{\tau\}$;
if τ is not prefix string reducible by G
then $N := N \cup \{\tau\}$;
$B := B \cup \{\tau a \mid a \in \bar{\Sigma}\}$;
$H := \{\tau r \longrightarrow \tau \mid r \longrightarrow \lambda \in F_R\}$;
$G := \mathsf{prefix.kb}(G \cup H)$;
$S := \{w \in N \mid w$ is not prefix string reducible by G$\}$;
$N := N \backslash S$;
endif
endwhile
endif

A thorough comparison of all three methods is provided in [24].

References

[1] J. Avenhaus and K. Madlener. The Nielsen reduction and p-complete problems in free groups. *Theoretical Computer Science*, 32:61–76, 1984.

[2] B. Benninghofen, S. Kemmerich, and M.M. Richter. *Systems of Reductions.* LNCS 277. Springer, 1987.

[3] R. Book and F. Otto. *String Rewriting Systems.* Springer, 1993.

[4] M. A. Borges and M. Borges. Gröbner bases property on elimination ideal in the noncommutative case. In B. Buchberger and F. Winkler, editors, *Gröbner Bases and Applications (Proc. of the Conference 33 Years of Gröbner Bases)*, volume 251 of *London Mathematical Society Lecture Notes Series*, page to appear. Cambridge University Press, 1998.

[5] M. A. Borges, M. Borges, and T. Mora. Non-commutative gröbner bases and fglm techniques. Draft, 1998.

[6] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.* PhD thesis, Universität Innsbruck, 1965.

[7] B. Buchberger and M. Möller. The construction of multivariate polynomials with preassigned zeroes. In *EUROCAM*, LNCS 144, pages 24–31. Springer, 1982.

[8] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16:329–344, 1993.

[9] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Mathematische Annalen*, 95:737–788, 1926.

[10] D. L. Johnson. *Presentation of Groups*. Cambridge University Press, 1976.

[11] A. Kandri-Rody and V. Weispfenning. Non-commutative Gröbner bases in algebras of solvable type. *Journal of Symbolic Computation*, 9:1–26, 1990.

[12] D. Knuth and P. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, Oxford, 1970.

[13] N. Kuhn, K. Madlener, and F. Otto. Computing presentations for subgroups of polycyclic groups and of context-free groups. *Applicable Algebra in Engineering, Communication and Computing*, 5:287–316, 1994.

[14] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory*. Springer, 1977.

[15] K. Madlener and B. Reinert. Computing Gröbner bases in monoid and group rings. In M. Bronstein, editor, *Proc. ISSAC'93*, pages 254–263. ACM, 1993.

[16] K. Madlener and B. Reinert. String rewriting and Gröbner bases – a general approach to monoid and group rings. In *Proceedings of the Workshop on Symbolic Rewriting Techniques, Monte Verita, 1995*, pages 127–180. Birkhäuser, 1998.

[17] K. Madlener and B. Reinert. Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings. *Theoretical Computer Science*, to appear.

[18] S. Margolis, J. Meakin, and M. Sapir. Algorithmic problems in groups, semigroups and inverse monoids. In J. Fountain, editor, *Semigroups, Formal Languages and Groups*, pages 147–214. Kluwer Academic Press, 1993.

[19] M. G. Marinari, H. M. Möller, and T. Mora. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing*, 4:103–145, 1993.

[20] T. Mora. Gröbner bases and the word problem. Genova, 1987.

[21] J. Neubueser. An elementary introduction to coset table methods in computational group theory. In C. M. Campbell and E. F. Robertson, editors, *Groups St. Andrews 1981*, L.M.S. Lecture Notes 71, pages 1–45. Cambridge University Press, 1982.

[22] J. Nielsen. Om Regning med ikke kommutative Faktoren og dens Anvendelse i Gruppeteorien. *Mat. Tidsskr. B.*, pages 77–94, 1921.

[23] B. Reinert. *On Gröbner Bases in Monoid and Group Rings.* PhD thesis, Universität Kaiserslautern, 1995.

[24] B. Reinert, T. Mora, and K. Madlener. Coset enumeration – a comparison of methods. Technical report, Universität Kaiserslautern, 1998.

[25] C. Sims. *Computation with Finitely Presented Groups.* Cambridge University Press, 1994.

[26] J. Todd and H. Coxeter. A practical method for enumerating cosets of a finite abstract group. In *Proc. Edinburgh Math. Soc.*, volume 5, pages 26–34, 1936.

[27] A. Zharkov and Yu. Blinkov. Involution approach to solving systems of algebraic equations. In *Proc. IMACS'93*, pages 11–16, 1993.

List of papers published in the Reports on Computer Algebra series

[1] H. Grassmann, G.-M. Greuel, B. Martin, W. Neumann, G. Pfister, W. Pohl, H. Schönemann, and T. Siebert. Standard bases, syzygies and their implementation in singular. 1996.

[2] H. Schönemann. Algorithms in singular. 1996.

[3] R. Stobbe. FACTORY: a C++ class library for multivariate polynomial arithmetic. 1996.

[4] O. Bachmann and H. Schönemann. A Manual for the MPP Dictionary and MPP Library. 1996.

[5] O. Bachmann, S. Gray, and H. Schönemann. MPP: A Framework for Distributed Polynomial Computations. 1996.

[6] G.M. Greuel and G. Pfister. Advances and improvements in the theory of standard bases and syzygies. 1996.

[7] G.M. Greuel. Description of SINGULAR: A computer algebra system for singularity theory, algebraic geometry, and commutative algebra. 1996.

[8] T. Siebert. On strategies and implementations for computations of free resolutions. September 1996.

[9] B. Reinert. Introducing reduction to polycyclic group rings – a comparison of methods. October 1996.

[10] O. Bachmann, S. Gray, and H. Schönemann. A proposal for syntactic data integration for math protocols. January 1997.

[11] O. Bachmann. Effective simplification of cr expressions. January 1997.

[12] O. Bachmann, S. Gray, and H. Schönemann. MP Prototype Specification. January 1997.

[13] O. Bachmann. MPT – a library for parsing and Manipulating MP Trees. January 1997.

[14] K. Madlener and B. Reinert. Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings. September 1997.

[15] B. Martin and T. Siebert. Splitting Algorithm for vector bundles. September 1997.

[16] K. Madlener and B. Reinert. String Rewriting and Gröbner Bases – A General Approach to Monoid and Group Rings. October 1997.

[17] Thomas Siebert. An algorithm for constructing isomorphisms of modules. January 1998.

[18] O. Bachmann and H. Schönemann. Monomial Representations for Gröbner Bases Computations. January 1998.

[19] B. Reinert, K. Madlener, and T. Mora. A note on nielsen reduction and coset enumeration. February 1998.