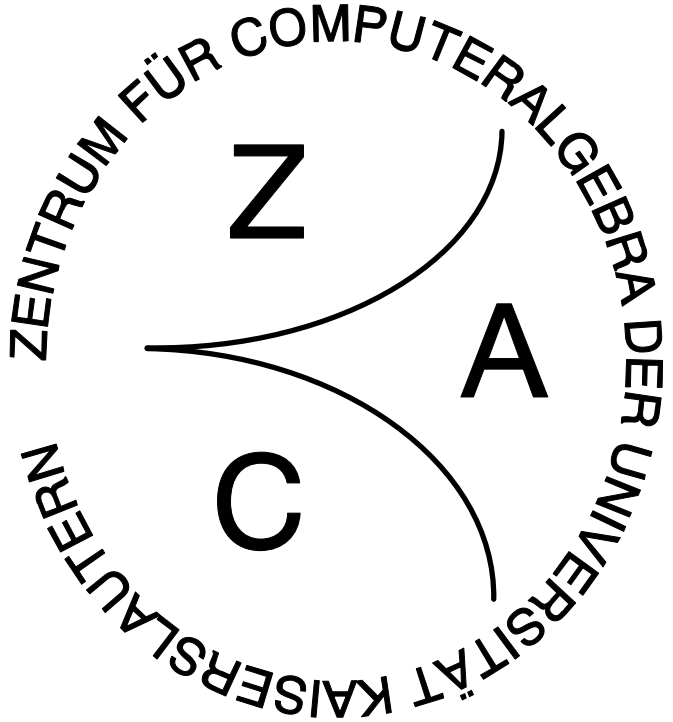
UNIVERSITÄT KAISERSLAUTERN
Zentrum für Computeralgebra

REPORTS ON COMPUTER ALGEBRA
NO. 22



Some Applications Of Prefix-Rewriting In Monoids, Groups, And Rings

by

K. Madlener and O. Friedrich

Nov 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/`

Some Applications Of Prefix-Rewriting In Monoids, Groups, And Rings

Klaus Madlener[(1)] and **Friedrich Otto**[(2)]

[(1)] Fachbereich Informatik, Universität Kaiserslautern, D-67653 Kaiserslautern

E-mail: madlener@informatik.uni-kl.de

WWW: http://www.uni-kl.de/AG-AvenhausMadlener/AG-Madlener.html

[(2)] Fachbereich Mathematik/Informatik, Universität Kassel, D-34109 Kassel

E-mail: otto@theory.informatik.uni-kassel.de

WWW: http://www.db.informatik.uni-kassel.de/FG_TH/otto/

November 3, 1998

Abstract

Rewriting techniques have been applied successfully to various areas of symbolic computation. Here we consider the notion of *prefix-rewriting* and give a survey on its applications to the *subgroup problem* in combinatorial group theory. We will see that for certain classes of finitely presented groups finitely generated subgroups can be described through convergent prefix-rewriting systems, which can be obtained from a presentation of the group considered and a set of generators for the subgroup through a specialized Knuth-Bendix style completion procedure. In many instances a finite presentation for the subgroup considered can be constructed from such a convergent prefix-rewriting system, thus solving the *subgroup presentation problem*. Finally we will see that the classical procedures for computing Nielsen reduced sets of generators for a finitely generated subgroup of a free group and the Todd-Coxeter coset enumeration can be interpreted as particular instances of prefix-completion. Further, both procedures are closely related to the computation of prefix Gröbner bases for right ideals in free group rings.

Keywords: monoid- and group-presentations, subgroup problem, subgroup presentation problem, prefix-rewriting, confluence, λ-confluence, coset enumeration, Gröbner bases in monoid and group rings.

1 Introduction

There is a recent shift in paradigm in mathematics, and in modern algebra in particular, from pure structural considerations back to the notion of computability, that is, one is not merely interested in the structural properties of the mathematical entities under consideration, but one wants to actually perform computations in these structures.

This development has been preceded by that in combinatorial group theory, where algorithmic questions have been of major concern since the beginning of the century. In 1911 M. Dehn formulated three fundamental decision problems for groups given in terms of generators and defining relations [Deh11], the most famous of which is the *word problem*.

Consequently these problems have been shown to be undecidable in general, and much effort has been spent on deriving decidability results for restricted instances. Already in his original paper M. Dehn gave a solution for the word problem for free groups by establishing that the process of freely reducing strings leads to unique representatives for the elements of the free group. In a subsequent paper he proved that the word problem for the fundamental groups of closed, two dimensional, orientable surfaces of genus larger than or equal to two can be solved by a *monotonic reduction process* [Deh12]. Actually, this algorithm, known as *Dehn's algorithm for the word problem*, extends to the class of all small-cancellation groups, which are groups that satisfy certain combinatorial conditions [LS77].

On the other hand, string-rewriting systems that are *convergent*, that is, noetherian and confluent, yield a unique irreducible string for each element of the group (or monoid) presented [BO93]. Hence, if a group admits a presentation involving a finite convergent string-rewriting system, then its word problem is decidable by reduction. The class of groups that admit such presentations includes for example the finite groups, the free groups of finite rank, the finitely generated polycyclic groups, and the finitely generated virtually free groups. Actually, to solve the word problem for a group by reduction, it suffices that the string-rewriting system presenting the group is finite, noetherian, and λ-confluent, that is, each word presenting the identity of the group considered reduces to the empty string [MO87]. In fact, Dehn's algorithm for the word problem corresponds to the process of reduction with respect to a finite, length-reducing, and λ-confluent string-rewriting system [Büc79, LeC86].

A generalization of the word problem that also has received a lot of attention is the *subgroup problem*, also known in the literature as the *generalized word problem* [MKS76]. Let $\langle \Sigma; S \rangle$ be a finite group-presentation of a group G. Then the subgroup problem for $\langle \Sigma; S \rangle$ is the following decision problem:

INSTANCE	:	A finite set $U \subset \underline{\Sigma}^*$, and a string $w \in \underline{\Sigma}^*$.
QUESTION	:	Does w represent an element of the subgroup of G that is generated by U?

Since this is a generalization of the word problem, this problem is also undecidable in general. In fact, it is even undecidable for some groups that can be presented by finite convergent string-rewriting systems [Mil71]. On the other hand, if F is the free group given by the free presentation $\langle \Sigma; \emptyset \rangle$, then a finite set $U \subset \underline{\Sigma}^*$ can effectively be transformed into a *Nielsen reduced set* V that is a set of free generators for the subgroup of F generated by U (see, e.g., [MKS76]). Using this set it is easy to decide whether w is a member of the subgroup.

Another classical approach to the subgroup problem is the *Todd-Coxeter coset enumeration method* [TC36], which, given a presentation $\langle \Sigma; S \rangle$ and a set U, enumerates coset representatives of the subgroup $\langle U \rangle$ of G that is generated by U. This procedure succeeds if and only if $\langle U \rangle$ has finite index in G, and in this case it returns a *coset table*, that is, a complete table for the multiplication of cosets of $\langle U \rangle$ with generators of G.

Unfortunately the so-called *index problem*, that is, the problem of deciding whether or not $\langle U \rangle$ has finite index in G, is also undecidable in general. Thus, the Todd-Coxeter coset enumeration only yields a semi-decision procedure for the subgroup problem.

Here we will show that rewriting methods are a powerful tool to solve the subgroup problem and related problems. A set $U \subset \underline{\Sigma}^*$ induces a left-congruence $\sim_U$ on $\underline{\Sigma}^*$ as follows: two strings x and y are congruent modulo $\sim_U$ if and only if x and y belong to the same right coset of $\langle U \rangle$. This congruence can be expressed through a *prefix-rewriting*

system, that is, a string-rewriting system where the rules are only used to replace prefixes of strings [Bau81, KM89]. If this prefix-rewriting system is noetherian and confluent, then it yields a set of unique coset representatives for the cosets of $\langle U \rangle$ in G. Thus, if in addition the prefix-rewriting process induced by this system is effective, then prefix-rewriting solves the subgroup problem. Further, if this system is finite or at least left-regular, then the set of representatives is a regular language, and hence, the index of $\langle U \rangle$ in G can be computed.

In this paper we give a survey on the applications of prefix-rewriting to the subgroup problem and related problems in groups, monoids, and rings. After establishing notation in Section 2 we define the problems considered in the following. In addition to the subgroup problem and the index problem they include the *subgroup presentation problem*, which asks to compute a finite presentation for the subgroup $\langle U \rangle$ of the given group G.

In Section 3 we discuss three classical algorithms of combinatorial group theory in short: Nielsen's method of transforming a set of generators of a subgroup of a free group into a set of free generators, the Todd-Coxeter coset enumeration method, and the method of Reidemeister and Schreier for determining presentations for subgroups [MKS76].

In the following section we introduce prefix-rewriting systems, and show how they are used to represent left-congruences of groups. ¿From a given finite set U a prefix-rewriting system P_U defining $\sim_U$ is easily obtained, but in general this system will not be confluent. However, specially adopted versions of the Knuth-Bendix completion procedure [KB70] have been defined that, given P_U and a reduction ordering as input, try to generate a prefix-rewriting system Q_U that is convergent, and that generates the left-congruence $\sim_U$. Obviously, this procedure will not always terminate, but it has been shown to terminate successfully if and only if there exists a finite system Q_U that generates $\sim_U$ and that is compatible with the given reduction ordering. This section closes by showing that the process of computing Nielsen reduced sets of generators for subgroups of free groups can be interpreted as a particular instance of prefix-completion. In fact there is a one-to-one correspondence between the prefix-interreduced, canonical prefix-rewriting systems on $\langle \Sigma; \emptyset \rangle$ and the generalized Nielsen-reduced subsets of $\underline{\Sigma}^*$.

In Section 5 it is shown that for some classes of presentations of groups, each finitely generated subgroup can be described through a finite set of prefix-rules such that the prefix-rewriting system obtained from this set together with the prefix-rules corresponding to the string-rewriting system of the given presentation is convergent. Here we will follow R. Cremanns [Cre95], who introduced an abstract condition that guarantees this property, so that then it remains to verify that the classes of presentations considered do indeed satisfy this condition. As it turns out this approach works fine for those finite convergent presentations that involve a special string-rewriting system or a two-monadic string-rewriting system with inverses of length one. In addition it applies to the so-called virtually free presentations, which is a class of finite convergent presentations for the finitely generated virtually free groups. Further, for the class of finite, monadic, and λ-confluent presentations, which also characterize these groups, and for the class of PCP2-presentations, which characterize the finitely presented polycyclic groups, λ-convergent prefix-rewriting systems are obtained.

¿From a finite convergent presentation of a group G and a convergent prefix-rewriting system for a subgroup H of G, a finite presentation of H can be constructed, if H is indeed finitely presented. In Section 6 this property is characterized with the aid of an infinite graph that describes the induced prefix-rewriting relation. This graph is an extension of the graph that C. Squier used to define the notion of *finite derivation type* for monoids and groups [SOK94]. In addition a finite presentation for H can be extracted from this graph based on resolutions of the U- and G-critical pairs [Cre95]. For free groups and for groups

presented by finite, special, and confluent presentations this yields a finite presentation of the same form for the subgroup H. The corresponding result can also be shown for the virtually free presentations, the PCP2-presentations, and the presentations involving a finite, monadic, and λ-confluent string-rewriting system.

In Section 7 we discuss in short a correspondence between automatic structures and prefix-rewriting systems. Automatic structures for groups and monoids have been found very useful, since they are close to geometrical considerations and use natural automata constructions providing an algorithm for solving the word problem that runs in quadratic time [Eps92]. An automatic structure yields a set of representatives for the monoid or group considered, and although in general these representatives need not be unique, each automatic structure can be replaced by another one that yields unique representatives. Now the solution of the word problem corresponds to the left-to-right computation of the representative that corresponds to a given string, and so it can be interpreted as a kind of prefix-rewriting. And in fact if the set of unique representatives is in addition prefix-closed, then a synchronously regular prefix-rewriting system can be constructed that defines the group or monoid considered, is convergent, and yields the same representatives. Conversely, if such a prefix-rewriting system exists, then based on its set of irreducible strings, an automatic structure can be constructed for the monoid or group considered.

Finally, in Section 8 we point out a close correspondence between the process of computing Nielsen reduced sets of generators in free groups and the Todd-Coxeter coset enumeration method on the one hand and the computation of prefix Gröbner bases in the free group ring on the other hand. It turns out that both these classical procedures of combinatorial group theory have their counterparts in the computation of prefix Gröbner bases in this ring. This section is based on recent work of B. Reinert et al [RMM98a].

The paper closes with a short summary and some open problems.

2 The subgroup problem and related problems

Here we introduce the basic notions and notation concerning presentations of groups, and we state the subgroup problem and some related problems that we are interested in in detail. For additional information on the notions introduced we refer to the literature, where [BO93] serves as our main reference on string-rewriting systems and monoid-presentations, while [MKS76, LS77] are our main references on combinatorial group theory.

Let Σ be a finite alphabet, that is, Σ is a finite set of symbols called *letters* or *generators*. Then Σ^* denotes the set of strings over Σ including the empty string λ, and $\Sigma^+ = \Sigma^* \setminus \{\lambda\}$ is the set of all nonempty strings over Σ. The operation of concatenation, which is simply written by juxtaposition, is an associative binary operation on Σ^* with identity λ, and so Σ^* has the algebraic structure of a monoid. It is the *free monoid* generated by Σ.

For $w \in \Sigma^*$, $|w|$ denotes the *length* of w, and $|w|_a$ ($a \in \Sigma$) denotes the *a-length* of w which is simply the number of occurrences of the letter a in w. Analogously, for $\Gamma \subseteq \Sigma$, $|w|_\Gamma := \bigcup_{a \in \Gamma} |w|_a$ is the Γ-*length* of w. Finally, to simplify the notation numerical superscripts will be used to write strings in a more compact and readable form, where $w^0 := \lambda$, $w^1 := w$, and $w^{n+1} := w^n w$ for all $w \in \Sigma^*$ and $n \in \mathbb{N}$.

A *string-rewriting system* on Σ is a subset of $\Sigma^* \times \Sigma^*$. Its elements are called (*rewrite*) *rules*, and usually they will be written as $(\ell \to r)$. If S is a string-rewriting system on Σ, then $\mathrm{dom}(S) := \{\ell \in \Sigma^* \mid \exists r \in \Sigma^* : (\ell \to r) \in S\}$ and $\mathrm{range}(S) := \{r \in \Sigma^* \mid \exists \ell \in \Sigma^* : (\ell \to r) \in S\}$.

A string-rewriting system S on Σ induces several binary relations on Σ^*, the most basic

of which is the *single-step reduction relation* $\rightarrow_S := \{(u\ell v, urv) \mid (\ell \rightarrow r) \in S, u, v \in \Sigma^*\}$. Its reflexive transitive closure $\rightarrow_S^*$ is the *reduction relation* defined by S, while the reflexive, symmetric, and transitive closure $\leftrightarrow_S^*$ of $\rightarrow_S$ is actually a congruence on Σ^*, since $x \leftrightarrow_S^* y$ implies $uxv \leftrightarrow_S^* uyv$ for all $u, v \in \Sigma^*$. It is called the *Thue congruence* generated by S. The set $M_S := \{[w]_S \mid w \in \Sigma^*\}$ of congruence classes forms a monoid with identity $[\lambda]_S$ under the operation $[u]_S \circ [v]_S := [uv]_S$, that is, M_S is the factor monoid $\Sigma^*/\leftrightarrow_S^*$ of the free monoid Σ^* modulo the Thue congruence $\leftrightarrow_S^*$. If M is a monoid that is isomorphic to M_S, then the ordered pair $(\Sigma; S)$ is called a *monoid-presentation* of M with *generators* Σ and *defining relations* S. The monoid M is called *finitely generated* if it has a presentation with a finite set of generators, and it is called *finitely presented* if it has a finite presentation.

¿From a finite presentation $(\Sigma; S)$ one can determine a set of strings $\{u_a \mid a \in \Sigma\}$ such that the monoid M_S is a group if and only if $au_a \leftrightarrow_S^* \lambda \leftrightarrow_S^* u_a a$ holds for all $a \in \Sigma$ [Ott86]. This yields a function $^{-1} : \Sigma^* \rightarrow \Sigma^*$ that realizes the inverse function for the group M_S simply by defining $\lambda^{-1} := \lambda$ and $(wa)^{-1} := u_a w^{-1}$ for all $w \in \Sigma^*$ and $a \in \Sigma$. However, in combinatorial group theory groups are usually presented through so-called group-presentations rather than through monoid-presentations.

Let Σ be a finite alphabet, let $\overline{\Sigma}$ be another finite alphabet in one-to-one correspondence to Σ such that $\Sigma \cap \overline{\Sigma} = \emptyset$, let $\underline{\Sigma} := \Sigma \cup \overline{\Sigma}$, and let $S_0 := \{a\bar{a} \rightarrow \lambda, \bar{a}a \rightarrow \lambda \mid a \in \Sigma\}$, where $^- : \Sigma \rightarrow \overline{\Sigma}$ denotes the one-to-one correspondence between Σ and $\overline{\Sigma}$. Then $(\underline{\Sigma}; S_0)$ is a presentation of the *free group* generated by Σ, that is, $M_{S_0} \cong F_n$, where $n = \mathrm{card}(\Sigma)$.

In addition, let S be a string-rewriting system on $\underline{\Sigma}$. Then the monoid presented by $(\underline{\Sigma}; S \cup S_0)$ is a group, and the ordered pair $\langle \Sigma; S \rangle$ is called a *group-presentation* of this group. The congruence on $\underline{\Sigma}^*$ that is generated by $S \cup S_0$ will simply be written as $=_S$.

Since group-presentations are a special class of monoid-presentations we will give the following definitions only in terms of the latter.

Let G be a group that is given through a presentation $(\Sigma; S)$. The *word problem* for $(\Sigma; S)$ is the following decision problem:

INSTANCE: Two strings $u, v \in \Sigma^*$.

QUESTION: Do u and v present the same element of the group G, that is, does $u \leftrightarrow_S^* v$ hold?

Since the function $^{-1} : \Sigma^* \rightarrow \Sigma^*$ can be determined effectively from $(\Sigma; S)$, the word problem is equivalent to the *special word problem*:

INSTANCE: A string $w \in \Sigma^*$.

QUESTION: Does w present the identity of the group G, that is, does $w \leftrightarrow_S^* \lambda$ hold?

Actually this is the form in which the word problem is usually stated in combinatorial group theory. A generalization of the word problem is the *subgroup problem*, which is also known as the *generalized word problem*:

INSTANCE: A finite set of strings $U \subseteq \Sigma^*$, and a string $w \in \Sigma^*$.

QUESTION: Does w belong to the subgroup $\langle U \rangle$ of G that is generated by U?

A string w belongs to $\langle U \rangle$ if and only if there exist $u_1, \ldots, u_n \in U$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$ such that $w \leftrightarrow_S^* u_1^{\varepsilon_1} u_2^{\varepsilon_2} \cdots u_n^{\varepsilon_n}$. Here $u^1 := u$, and u^{-1} denotes the inverse of u. To simplify the notation we will usually assume that the set U is *closed under inverses*, that is, for each $u \in U$ there is an element $v \in U$ such that $v \leftrightarrow_S^* u^{-1}$.

With U we associate a binary relation $\sim_U$ on Σ^* as follows:

$$x \sim_U y \text{ iff } \exists u \in \langle U \rangle : x \leftrightarrow_S^* uy.$$

Then $\sim_U$ is a left-congruence on Σ^*, that is, it is an equivalence relation such that $x \sim_U y$ implies $xz \sim_U yz$ for all $z \in \Sigma^*$.

By $[w]_U$ we denote the congruence class of w modulo $\sim_U$. Obviously, it is simply the left coset of $\langle U \rangle$ in G containing w. The number of left cosets of $\langle U \rangle$ is called the *index* of $\langle U \rangle$ in G and is written as $|G : \langle U \rangle|$. The *index problem* is an important decision problem:

INSTANCE: A finite set of strings $U \subseteq \Sigma^*$.

QUESTION: What is the index of $\langle U \rangle$ in G?

Finally, the subgroup $\langle U \rangle$ of G may or may not be finitely presented as a group. In the former case it would be of interest to actually determine a finite presentation of the group $\langle U \rangle$. This is the *subgroup presentation problem*:

INSTANCE: A finite set of strings $U \subseteq \Sigma^*$.

TASK: Decide whether or not the subgroup $\langle U \rangle$ of G is finitely presented, and in the affirmative determine a finite presentation for $\langle U \rangle$!

There are finitely presented groups with undecidable word problem. Hence, also the subgroup problem is undecidable in general. Actually the subgroup problem is even undecidable for the direct product $F_2 \times F_2$ of the free group F_2 of rank 2 with itself [Mik58], whose word problem is easily decidable. Further there are finitely presented groups for which the index problem is undecidable, and there are finitely presented groups for which it is undecidable whether or not a finitely generated subgroup is itself finitely presented [BBN59]. Thus, all the problems above are undecidable in general.

On the other hand these problems have been solved successfully for some restricted classes of presentations. The restrictions we are interested in concern the properties of the single-step reduction relation and the syntactic form of the rules.

Let S be a string-rewriting system on Σ. A string $u \in \Sigma^*$ is called *reducible* modulo S if there exists a string $v \in \Sigma^*$ such that $u \to_S v$ holds; otherwise, u is called *irreducible* modulo S. By $\mathrm{RED}(S)$ we denote the set of all reducible strings, and by $\mathrm{IRR}(S)$ the set of all irreducible strings. Obviously $\mathrm{RED}(S) = \Sigma^* \cdot \mathrm{dom}(S) \cdot \Sigma^*$ and $\mathrm{IRR}(S) = \Sigma^* \setminus \mathrm{RED}(S)$. Hence, if S is a finite system, then these sets are regular, and in fact in this case deterministic finite-state acceptors (dfsa's) can be constructed for them in polynomial time.

The string-rewriting system S is called

- *noetherian* if there is no infinite sequence of reduction steps of the form $w_0 \to_S w_1 \to_S \ldots \to_S w_i \to_S w_{i+1} \to_S \ldots$;
- *weight-reducing* if there exists a weight function $g : \Sigma \to \mathbb{N}_+$ such that the extension of g to a morphism $g : \Sigma^* \to \mathbb{N}$ satisfies $g(\ell) > g(r)$ for each rule $(\ell \to r) \in S$;
- *length-reducing* if $|\ell| > |r|$ holds for each rule $(\ell \to r) \in S$.

If S is noetherian, then each string has some irreducible descendants, since the process of performing reduction steps modulo S terminates. Unfortunately, however, it is undecidable in general whether or not a given finite string-rewriting system is noetherian. On the other hand, if $\geq$ is an admissible well-founded partial ordering on Σ^* such that S is *compatible* with $\geq$, that is, $\ell > r$ holds for each rule $(\ell \to r) \in S$, then S is necessarily noetherian. Here a partial ordering $\geq$ on Σ^* is called *admissible* if $x \geq y$ implies that $uxv \geq uyv$ holds for all $u, v \in \Sigma^*$, and it is called *well-founded* if there is no infinite sequence of strings that is strictly decreasing. For example, a weight function $g : \Sigma \to \mathbb{N}_+$ yields the partial ordering $\geq_g$ defined through $x \geq_g y$ iff $g(x) \geq g(y)$, which is admissible

and well-founded, but not linear. If we assume that the alphabet Σ is linearly ordered by $\geq_\Sigma$, then we can combine the partial ordering $\geq_g$ and the lexicographical ordering on Σ^* that is induced by $\geq_\Sigma$ into an admissible well-ordering $\geq_{g,\mathrm{lex}}$ as follows:

$$x \geq_{g,\mathrm{lex}} y \quad \text{iff} \quad \begin{array}{lll} g(x) > g(y) & \text{or} & \\ g(x) = g(y) & \text{and} & x \geq_{\mathrm{lex}} y. \end{array}$$

A special case is the *length-lexicographical ordering* $\geq_{\ell\ell}$, which is obtained by taking the length of a string as its weight.

The string-rewriting system S is called *monadic* if $\mathrm{range}(S) \subseteq \Sigma \cup \{\lambda\}$ and $\ell \geq_{\ell\ell} r$ holds for each rule $(\ell \to r) \in S$, and it is called *special* if it is length-reducing and $\mathrm{range}(S) = \{\lambda\}$. Obviously, monadic systems are noetherian.

Finally, we turn to restrictions that limit the number of irreducible strings that can occur within certain congruence classes. A string-rewriting system S on Σ is called

- *locally confluent* if, for all $u, v, w \in \Sigma^*$, $u \to_S v$ and $u \to_S w$ imply that $\Delta_S^*(v) \cap \Delta_S^*(w) \neq \emptyset$, where $\Delta_S^*(x) := \{z \in \Sigma^* \mid x \to_S^* z\}$ denotes the *set of all descendants* of x modulo S;
- *confluent* if, for all $u, v, w \in \Sigma^*$, $u \to_S^* v$ and $u \to_S^* w$ imply that $\Delta_S^*(v) \cap \Delta_S^*(w) \neq \emptyset$;
- λ-*confluent* if, for all $w \in \Sigma^*$, $w \leftrightarrow_S^* \lambda$ implies that $w \to_S^* \lambda$ holds.

If S is λ-confluent, then $[\lambda]_S$ contains at most a single irreducible string, which has to be λ. Analogously, if S is confluent, then no congruence class can contain more than a single irreducible string. Hence, if S is λ-*convergent*, that is, noetherian and λ-confluent, then $[\lambda]_S \cap \mathrm{IRR}(S) = \{\lambda\}$, and if S is *convergent*, that is, noetherian and confluent, then each congruence class contains a unique irreducible string. Thus, if S is a finite convergent system, then the word problem for S can simply be solved by reduction.

The system S is called *interreduced* if $\mathrm{range}(S) \subseteq \mathrm{IRR}(S)$ and $\ell \in \mathrm{IRR}(S \setminus \{(\ell \to r)\})$ holds for each rule $(\ell \to r) \in S$. A system is called *canonical* if it is convergent and interreduced. In fact, from a convergent system a canonical system can be constructed which generates the same Thue congruence and has the same set of irreducible strings.

In this paper we will mainly be interested in groups that are given through finite presentations involving certain λ-convergent or convergent string-rewriting systems. Since the group $F_2 \times F_2$ is presented through the presentation $(\Gamma; R)$, where $\Gamma := \{a, b, c, d, \bar{a}, \bar{b}, \bar{c}, \bar{d}\}$ and $R := \{x^\varepsilon \bar{x}^\varepsilon \to \lambda \mid x \in \{a, b, c, d\}, \varepsilon \in \{1, -1\}\} \cup \{y^\varepsilon x^\mu \to x^\mu y^\varepsilon \mid x \in \{a, b\}, y \in \{c, d\}, \varepsilon, \mu \in \{1, -1\}\}$, which is canonical, we see that the subgroup problem is in general even undecidable for groups that are given through finite canonical presentations. Hence, our restrictions will have to be even more specific.

3 Classical results

Here we review some classical approaches to the subgroup problem: the Nielsen reduced sets for subgroups of free groups, the Todd-Coxeter method for enumerating cosets of finitely generated subgroups of finitely presented groups, and the Reidemeister-Schreier method for constructing presentations for subgroups of finitely presented groups. For more details we refer to the literature, where [MKS76, LS77] serve as our main references on these topics.

Let $F = \langle \Sigma; \emptyset \rangle$ be the free group generated by Σ, that is, F is presented through the monoid-presentation $(\underline{\Sigma}; S_0)$. The system $S_0 = \{a\bar{a} \to \lambda, \bar{a}a \to \lambda \mid a \in \Sigma\}$ is special and

convergent, and hence, $\mathrm{IRR}(S_0)$ is a set of unique representatives for F. The elements of $\mathrm{IRR}(S_0)$ are called *freely reduced* strings, and the process of reduction modulo S_0 is called *free reduction.*

Let $U := \{u_1, \ldots, u_m\}$ be a subset of $\mathrm{IRR}(S_0)$, and let $U^{-1} := \{u_i^{-1} \mid u_i \in U\}$ be the corresponding set of irreducible inverses. The *elementary Nielsen transformations* on U are defined as follows:

(NT1) Replace an element $u_i \in U$ by its inverse u_i^{-1}.

(NT2) Replace an element $u_i \in U$ by the irreducible descendant of $u_i u_j$ for some $j \neq i$.

(NT3) Delete some element $u_i \in U$, where $u_i = \lambda$.

In each of these three cases all the other elements of U remain unchanged. A finite sequence of such transformations is called a *Nielsen transformation.*

Proposition 3.1. *Let $U_1 \subseteq \mathrm{IRR}(S_0)$, and let U_2 be obtained from U_1 through a Nielsen transformation. Then $\langle U_1 \rangle = \langle U_2 \rangle$, that is, U_1 and U_2 generate the same subgroup of F.*

A subset $U \subseteq \mathrm{IRR}(S_0)$ is called *Nielsen reduced* if, for all $v_1, v_2, v_3 \in U \cup U^{-1}$, the following three conditions are satisfied:

(N0) $v_1 \neq \lambda$,

(N1) $v_1 v_2 \neq_F \lambda$ implies that $|(v_1 v_2)\downarrow| \geq \max\{|v_1|, |v_2|\}$, and

(N2) $v_1 v_2 \neq_F \lambda$ and $v_2 v_3 \neq_F \lambda$ imply that $|(v_1 v_2 v_3)\downarrow| > |v_1| - |v_2| + |v_3|$.

Here $w\downarrow$ denotes the (unique) irreducible descendant of w modulo S_0.

Nielsen reduced sets are of importance as they are free generating sets for the subgroups they generate. Actually they satisfy the following strong property.

Proposition 3.2. *Let U be a Nielsen reduced set. Then, for each element $u \in U \cup U^{-1}$, there exist strings a_u and m_u such that $m_u \neq \lambda$ and $u = a_u m_u (a_{u^{-1}})^{-1}$, and if $w = (u_1 u_2 \cdots u_m)\downarrow$ for some $u_1, \ldots, u_m \in U \cup U^{-1}$, where $u_i u_{i+1} \neq_F \lambda$ for $i = 1, \ldots, m-1$, then the strings $m_{u_1}, \ldots, m_{u_m}$ remain uncancelled in w.*

Hence, if $w = (u_1 u_2 \cdots u_m)\downarrow$ as above, then w has the prefix $a_{u_1} m_{u_1}$. ¿From this prefix u_1 can be determined, and we can consider $w_1 := (u_1^{-1} w)\downarrow = (u_2 \cdots u_m)\downarrow$. Iterating this process we can reconstruct the sequence $u_1, \ldots, u_m \in U \cup U^{-1}$ from w. Hence, the subgroup problem for F is solved provided the set U given is Nielsen reduced.

Proposition 3.3. *Given a finite set $U \subseteq \mathrm{IRR}(S_0)$ a Nielsen transformation can be found effectively that transforms U into a Nielsen reduced set V.*

Actually this task can be performed in polynomial time [AM84]. This yields the following result.

Corollary 3.4. *For finitely generated free groups the subgroup problem is decidable in polynomial time.*

We will see in the next section how this approach to the subgroup problem of free groups can be described and even extended by using the notion of prefix-rewriting.

Next we turn to the *Todd-Coxeter coset enumeration method* (TC). While it is undecidable in general whether a finitely generated subgroup $\langle U \rangle$ has finite index in a finitely presented group G, TC attempts to verify whether the index is finite by systematically enumerating the cosets of $\langle U \rangle$ in G. It is based on the following observation. Assume that G is given through the finite presentation $\langle \Sigma; S \rangle$. Then G is the

quotient of the free group F generated by Σ by the normal subgroup N that is generated by S. This normal subgroup N is the subgroup of F that is generated by the set $N(S) := \{w \cdot \ell r^{-1} \cdot w^{-1} \mid (\ell \to r) \in S, w \in \mathrm{IRR}(S_0)\}$. Thus, N is finitely generated as a *normal* subgroup of F, since S is finite, but N may not be finitely generated as a subgroup of F.

Now let H be the subgroup of G that is generated by $U \subseteq \underline{\Sigma}^*$. We are interested in the index $|G : H|$ of the subgroup H in the group G. It is easily seen that this index coincides with the index $|F : \langle U \cup N(S)\rangle|$ of the subgroup generated by $U \cup N(S)$ in the free group F. TC now attempts to verify that this index is finite.

For the following considerations we assume that $\langle \Sigma; S\rangle$ is a finite presentation of G, and that $U \subseteq \underline{\Sigma}^*$ is a finite set. Moreover TC requires that each generator $a \in \Sigma$ occurs in at least one of the defining relations S. TC tries to determine the index $|G : H|$ by exploiting the following facts about cosets:

(1.) For each $u \in U$, $Hu = H$.

(2.) For each rule $(\ell \to r) \in S$ and each coset Hu, $H(u \cdot \ell r^{-1} \cdot u^{-1}) = H$.

It proceeds as follows. With each generator $u = a_1 a_2 \cdots a_k \in U$, where $k \geq 1$ and $a_1, \ldots, a_k \in \underline{\Sigma}$, a table of the form below is associated:

a_1	a_2	a_3	$\ldots$	a_{k-1}	a_k
λ					λ

Here λ represents the coset H, and the empty slots are to be filled with representatives for the cosets $Ha_1, Ha_1a_2, \ldots, Ha_1a_2 \cdots a_{k-1}$. Further, with each defining relation $(\ell \to r) \in S$, or more exactly with the freely reduced form $b_1 b_2 \cdots b_m$ of ℓr^{-1}, where $m \geq 1$ and $b_1, \ldots, b_m \in \underline{\Sigma}$, a table of the following form is associated:

b_1	b_2	b_3	$\ldots$	b_{m-1}	b_m
λ					λ
$\vdots$					$\vdots$

These tables will contain a row for each coset encountered. If w is a coset representative, then the slots in the row starting with w will be filled with representatives for the cosets $Hwb_1, Hwb_1b_2, \ldots, Hwb_1b_2 \cdots b_{m-1}$.

Depending on the strategy used for determining the slot to be filled next, different types of equations between coset representatives are deduced. For example, if the representative of $Ha_1a_2 \cdots a_{k-1}$ happens to be the string $w \in \underline{\Sigma}^*$, then we see from the table for $u = a_1 \cdots a_k$ that $(Hw) \cdot a_k = H$, that is, with respect to their operation on cosets we obtain the equation $w \cdot a_k \sim_H \lambda$, which is called a *bonus equation*. On the other hand, if we have the coset representatives w for $Ha_1 \cdots a_i$ and z for $Ha_k^{-1} \cdots a_{i+1}^{-1}$, then we see that $Hw = Ha_1 \cdots a_i = Hu \cdot a_k^{-1} \cdots a_{i+1}^{-1} = Ha_k^{-1} \cdots a_{i+1}^{-1} = Hz$, which implies that w and z represent the same coset. This gives the *collaps equation* $w \sim_H z$. By identifying the cosets represented by w and z we may obtain additional information on other cosets. A detailed presentation of TC can be found in [Sim94].

To illustrate this procedure, and also for future reference, we give a simple example, which is taken from [Joh76], page 71.

Example 3.5. Let G be the Dyck group D(3,3,2), which is given through the presentation $\langle a, b; a^3, b^3, abab\rangle$. Here a^3 stands for the defining relation $a^3 \to \lambda$, and similar for the other strings given. Further, let H be the subgroup that is generated by $U := \{a\}$. Then the table for $a \in U$ yields the equation $a \sim_H \lambda$, and correspondingly $\bar{a} \sim_H \lambda$. In order to choose a unique coset representative we use the length-lexicographical ordering induced by $a < b < \bar{a} < \bar{b}$.

Now filling in the tables for a^3, b^3, and $abab$, and choosing the smaller string as the coset representative whenever an equation is obtained, we get the complete set of coset representatives $\{\lambda, b, \bar{b}, b\bar{a}\}$ and the following coset table for the cosets of H in G:

	a	$\bar{a}$	b	$\bar{b}$
H	H	H	Hb	$H\bar{b}$
Hb	$H\bar{b}$	$Hb\bar{a}$	$H\bar{b}$	H
$H\bar{b}$	$Hb\bar{a}$	Hb	H	Hb
$Hb\bar{a}$	Hb	$H\bar{b}$	$Hb\bar{a}$	$Hb\bar{a}$

The coset representative of the string aba can now be deduced by tracing this table starting from the coset H:

$$H \cdot a = H,\ H \cdot b = Hb, \text{ and } Hb \cdot a =_H H\bar{b}, \text{ that is, } Haba = H\bar{b}.$$

□

Actually the coset table yields a prefix-rewriting system that is convergent, and correspondingly the coset representative for a string w can be obtained by prefix-rewriting (see [RMM98a] for how to deduce this system and for further details).

Concerning the behavior of TC we have the following result.

Proposition 3.6. *Given a finite group-presentation $\langle \Sigma; S\rangle$ of a group G such that each generator $a \in \Sigma$ actually occurs in S and a finite set $U \subseteq \underline{\Sigma}^*$, TC terminates if and only if the index of $\langle U\rangle$ in G is finite. In this case TC determines a set of unique coset representatives for $\langle U\rangle$ in G and the corresponding coset table.*

Finally we restate in short the method of Reidemeister and Schreier for constructing presentations of subgroups. Again G is a group given through a finite group-presentation $\langle \Sigma; S\rangle$, and $U \subseteq \underline{\Sigma}^*$ is a finite set of generators for a subgroup H of G. ¿From $\langle \Sigma; S\rangle$ and U we would like to construct a presentation for H. For doing so we assume that in addition to the above we have a complete set C of coset representatives for H in G, and that we have an effective process $\varrho : \underline{\Sigma}^* \to C$ that maps a string $w \in \underline{\Sigma}^*$ to its coset representative $\varrho(w) \in C$. Then H is actually generated by the set $V := \{ca\varrho(ca)^{-1} \mid c \in C, a \in \Sigma\}$. Thus, if the index $|G : H|$ is finite, then H is finitely generated.

Let $\Gamma := \{b_{c,a} \mid c \in C, a \in \Sigma\}$ be a new alphabet in one-to-one correspondence to the set V, and let $\varphi : \underline{\Gamma}^* \to \underline{\Sigma}^*$ be the morphism that is induced by mapping $b_{c,a}$ to the string $ca\varrho(ca)^{-1}$ $(c \in C, a \in \Sigma)$. Then φ induces a homomorphism from the free group F_Γ generated by Γ onto the subgroup H of G. Thus, H is isomorphic to the factor group $F_\Gamma / \ker(\varphi)$ of the free group F_Γ by the kernel of the homomorphism φ.

Since each string $u \in U$ represents an element of H, there exists a string $\tau(u) \in \underline{\Gamma}^*$ such that $\varphi(\tau(u)) =_S u$. In fact, based on C and ϱ, a *rewriting function* $\tau : \langle U\rangle \to \underline{\Gamma}^*$ can be obtained that satisfies $\varphi(\tau(w)) =_S w$ for all $w \in \langle U\rangle$. Such a rewriting function based on coset representatives is called a *Reidemeister rewriting function.*

Proposition 3.7. *If τ is a Reidemeister rewriting function for the subgroup $H := \langle U \rangle$ of the group G presented by $\langle \Sigma; S \rangle$, then H is described by the presentation $\langle \Gamma; \{b_{c,a} \to \tau(ca\varrho(ca)^{-1}) \mid c \in C, a \in \Sigma\} \cup \{\tau(c\ell r^{-1}c^{-1}) \to \lambda \mid c \in C, (\ell \to r) \in S\}\rangle$, where C is the set of coset representatives for H in G underlying τ.*

Thus, if G is finitely presented and H has finite index in G, then H is finitely presented. If the set of coset representatives C is chosen in such a way that it is *prefix-closed*, that is, all the prefixes of a representative $c \in C$ are themselves representatives, then the presentation obtained for H is simplified considerably. A rewriting function that is based on a prefix-closed set of representatives is called a *Reidemeister-Schreier rewriting function.*

Proposition 3.8. *If τ is a Reidemeister-Schreier rewriting function for the subgroup $H := \langle U \rangle$ of the group G presented by $\langle \Sigma; S \rangle$, then H has the presentation*

$$\begin{aligned}\langle \Gamma; \quad & \{b_{c,a} \to \lambda \mid c \in C, a \in \Sigma \text{ such that } c \cdot a = \varrho(ca)\} \cup \\ & \{\tau(c\ell r^{-1}c^{-1}) \to \lambda \mid c \in C, (\ell \to r) \in S\}\rangle.\end{aligned}$$

Observe that the presentation obtained for H is infinite whenever the index $|G : H|$ of H in G is infinite. Using prefix-rewriting systems we will see in Section 6 that for certain classes of finite presentations of groups finite presentations can be obtained even for subgroups of infinite index.

4 Prefix-rewriting

When using the coset table obtained by the Todd-Coxeter coset enumeration method to determine the representative of a coset $H \cdot w$, this is done by reading w from left to right and replacing each prefix of w by its corresponding representative. Hence, this computation is an application of prefix-rewriting. Here we introduce prefix-rewriting systems in detail and relate them to the subgroup problem.

Let Σ be a finite alphabet. A *prefix-rewriting system* on Σ is a subset of $\Sigma^* \times \Sigma^*$. Its elements are called *prefix-rules*. If P is a prefix-rewriting system on Σ, then $\mathrm{dom}(P)$ and $\mathrm{range}(P)$ are defined as for string-rewriting systems.

The *prefix-reduction relation* $\Rightarrow_P^*$ defined by P is the reflexive transitive closure of the *single-step prefix-reduction relation* $\Rightarrow_P := \{(\ell w, rw) \mid (\ell, r) \in P, w \in \Sigma^*\}$, and by $\Leftrightarrow_P^*$ we denote the reflexive, symmetric, and transitive closure of $\Rightarrow_P$. Obviously $\Leftrightarrow_P^*$ is a left-congruence on Σ^*.

A string $u \in \Sigma^*$ is called *reducible* modulo P if $u \Rightarrow_P v$ holds for some $v \in \Sigma^*$; otherwise, u is *irreducible* modulo P. By $\mathrm{RED}(P)$ we denote the set of all reducible strings, and $\mathrm{IRR}(P)$ denotes the set of irreducible strings. Obviously, $\mathrm{RED}(P) = \mathrm{dom}(P) \cdot \Sigma^*$ and $\mathrm{IRR}(P) = \Sigma^* \setminus \mathrm{RED}(P)$. Hence, if $\mathrm{dom}(P)$ is a regular language, then $\mathrm{RED}(P)$ and $\mathrm{IRR}(P)$ are regular languages as well. In this situation the prefix-rewriting system P is called *left-regular*.

The prefix-rewriting system P is called *noetherian*, *confluent*, *convergent*, *λ-confluent*, *λ-convergent*, *interreduced*, or *canonical* if the corresponding condition is satisfied by $\Rightarrow_P$. It is interesting to observe that a prefix-rewriting system is convergent whenever it is interreduced [Sny89, Ott98b], that is, it is canonical if and only if it is interreduced.

Next we will show how prefix-rewriting systems are related to the subgroup problem. Let G be a group that is given through a finite presentation $(\Sigma; S)$, and let $^{-1} : \Sigma^* \to \Sigma^*$ denote a function realizing the inverse function of G. Further, let $U \subseteq \Sigma^*$ be a finite set. Without loss of generality we can assume that U is closed under inverses. Hence,

a string $w \in \Sigma^*$ presents an element of the subgroup $\langle U \rangle$ of G if and only if there exist $u_1, \ldots, u_k \in U$ such that $w \leftrightarrow_S^* u_1 u_2 \cdots u_k$.

With $(\Sigma; S)$ and U we now associate a prefix-rewriting system $P := P_U \cup P_S$, where

$$P_U := \{(u, \lambda) \mid u \in U\}$$

and

$$P_S := \{(x\ell, xr) \mid x \in \Sigma^* \text{ and } (\ell \to r) \in S\}.$$

Then P is a left-regular system, and the following property is easily verified.

Proposition 4.1. *The left-congruences $\sim_U$ and $\Leftrightarrow_P^*$ coincide.*

Hence, if P is λ-confluent, then a string $w \in \Sigma^*$ belongs to $\langle U \rangle$ if and only if $w \Rightarrow_P^* \lambda$, and if P is convergent, then $\mathrm{IRR}(P)$ is a complete set of coset representatives for $\langle U \rangle$ in G.

If S is noetherian, then P is noetherian, but in general P will not be convergent even in case S is. For future reference we consider the following simple example.

Example 4.2. Let $F_2 = \langle a, b; \emptyset \rangle$, and let $U_0 := \{ab, ba, aa\}$. Then $U := U_0 \cup \{\bar{b}\bar{a}, \bar{a}\bar{b}, \bar{a}\bar{a}\}$ is closed under inverses, and $\langle U_0 \rangle = \langle U \rangle$. Let $w := \bar{b}\bar{a}aa\bar{a}\bar{b}$. Then $w \to_{S_0}^* \bar{b}\bar{b} \in \mathrm{IRR}(P)$, and $w \Rightarrow_{P_U}^* \lambda$. Hence, P is not even λ-confluent, although S_0 is a canonical string-rewriting system. □

In order to solve the subgroup problem by prefix-rewriting we need a procedure that transforms the prefix-rewriting system P defined above into an equivalent prefix-rewriting system P_1 that is convergent or at least λ-convergent.

Let $(\Sigma; S)$ be a finite presentation of (a group) G, let P_U be a finite prefix-rewriting system on Σ, and let $P := P_U \cup P_S$, where P_S is the infinite prefix-rewriting system corresponding to the string-rewriting system S as above. If P is noetherian, for example it may be compatible with some admissible well-founded partial ordering on Σ^*, then P is confluent if and only if it is locally confluent. In order to determine the points of local divergence we introduce various forms of critical pairs.

If there are two rules $(u_1, v_1), (u_2, v_2) \in P_U$ such that $u_1 = u_2 y$ for some $y \in \Sigma^*$, where either $y \neq \lambda$ or $v_1 \neq v_2$, then $v_1 \Leftarrow_{P_U} u_1 = u_2 y \Rightarrow_{P_U} v_2 y$, and $(v_1, v_2 y)$ is called a *U-critical pair* of P. If there are rules $(u, v) \in P_U$ and $(\ell \to r) \in S$ such that $uy = x\ell z$ for some $x, y, z \in \Sigma^*$ satisfying $|x| < |u|$ and at least one of y or z is λ, then $vy \Leftarrow_{P_U} uy = x\ell z \Rightarrow_{P_S} xrz$, and (vy, xrz) is called a *G-critical pair* of P. Finally, if there are rules $(\ell_1 \to r_1), (\ell_2 \to r_2) \in S$ such that $\ell_1 = x\ell_2 y$ or $\ell_1 y = x\ell_2$, where $|x| < |\ell_1|$, then $(r_1, xr_2 y)$ or $(r_1 y, xr_2)$ is a critical pair of the string-rewriting system S, and correspondingly $(wr_1, wxr_2 y)$ or $(wr_1 y, wxr_2)$ is an *S-critical pair* of P for each string $w \in \Sigma^*$.

Proposition 4.3. *The prefix-rewriting system $P = P_U \cup P_S$ is locally confluent iff all U-, G-, and S-critical pairs of P resolve, that is, if (p, q) is one of these critical pairs, then p and q have a common descendant modulo P.*

The string-rewriting system S is locally confluent if and only if each of its critical pairs resolves. Thus, if S is locally confluent, then all S-critical pairs of P resolve, that is, in this situation it suffices to consider the U- and G-critical pairs of P. If P_U and S are both finite, then there are only finitely many of these pairs, and they can be computed in polynomial time. Hence, we have the following decidability result.

Proposition 4.4. *Let $(\Sigma; S)$ be a finite presentation such that S is convergent, and let P_U be a finite prefix-rewriting system on Σ. If $P := P_U \cup P_S$ is noetherian, then it is decidable whether or not P is confluent.*

If P is not confluent, since some U- or G-critical pairs do not resolve, then by introducing additional prefix-rules, these critical pairs can be resolved. This is the basic idea of the following procedure which is an adapted version of the Knuth-Bendix completion procedure [KB70, KN85]. Here we present only the most basic form of this procedure in order to illustrate it.

Procedure 4.5. Knuth-Bendix completion procedure for prefix-rewriting systems.

INPUT: A finite convergent presentation $(\Sigma; S)$, a finite prefix-rewriting system P_U on Σ, and an admissible well-founded partial ordering $\geq$ on Σ^* such that S is compatible with $\geq$.

begin $Q_0 \leftarrow \emptyset$;
  while $P_U \neq \emptyset$ **do**
  begin choose $(u, v) \in P_U$;
    if u and v are incomparable under $\geq$ **then failure**;
    if $u > v$ **then** $Q_0 \leftarrow Q_0 \cup \{(u, v)\}$;
    if $v > u$ **then** $Q_0 \leftarrow Q_0 \cup \{(v, u)\}$;
    $P_U \leftarrow P_U \setminus \{(u, v)\}$
  end;
  (Comment: Q_0 is obtained from P_U by orienting all prefix-rules with respect to $\geq$)
  $i \leftarrow -1$;
  repeat $i \leftarrow i + 1$; $Q_{i+1} \leftarrow \emptyset$;
    $CP \leftarrow$ set of U- and G-critical pairs of $Q_i \cup P_S$;
    while $CP \neq \emptyset$ **do**
    begin choose a minimal pair $(p, q) \in CP$;
      compute normal forms $\hat{p}$ and $\hat{q}$ of p and q modulo $Q_i \cup P_S$;
      if $\hat{p}$ and $\hat{q}$ are incomparable under $\geq$ **then failure**;
      if $\hat{p} > \hat{q}$ **then** $Q_{i+1} \leftarrow Q_{i+1} \cup \{(\hat{p}, \hat{q})\}$;
      if $\hat{q} > \hat{p}$ **then** $Q_{i+1} \leftarrow Q_{i+1} \cup \{(\hat{q}, \hat{p})\}$;
      $CP \leftarrow CP \setminus \{(p, q)\}$
    end;
    (Comment: all critical pairs of $Q_i \cup P_S$ have been resolved)
    if $Q_{i+1} \neq \emptyset$ **then** $Q_{i+1} \leftarrow Q_i \cup Q_{i+1}$
  until $Q_{i+1} = \emptyset$;
  $Q_U \leftarrow \bigcup_{i \geq 0} Q_i$
end.

Concerning the behavior of this procedure the following results have been obtained.

Proposition 4.6. [KM89, Kuh91]
Let $(\Sigma; S)$ be a finite convergent presentation, let P_U be a finite prefix-rewriting system on Σ, and let $\geq$ be an admissible well-founded partial ordering on Σ^* such that S is compatible with $\geq$. If the Knuth-Bendix completion procedure does not stop with failure given $(\Sigma; S)$, P_U and $\geq$ as input, then the system Q_U generated has the following properties:

(1.) $Q_U \cup P_S$ is equivalent to $P_U \cup P_S$.

(2.) $Q_U \cup P_S$ *is compatible with* $\geq$.

(3.) $Q_U \cup P_S$ *is convergent.*

Proposition 4.7. [KM89, Kuh91]
Let $(\Sigma; S)$ *and* P_U *be as above, and let* $\geq$ *be an admissible well-ordering on* Σ^* *such that* S *is compatible with* $\geq$. *Then given* $(\Sigma; S)$, P_U *and* $\geq$ *as input, the Knuth-Bendix completion procedure will enumerate a prefix-rewriting system* Q_U *that has the properties (1.) to (3.) of the previous proposition. It will terminate after finitely many steps, thus generating a finite system* Q_U, *if and only if there exists at all a finite prefix-rewriting system on* Σ *that has these properties.*

In particular, if the induced left-congruence has finite index, then termination of the procedure is guaranteed.

If P_U has the property that $\mathrm{dom}(P_U) \cup \mathrm{range}(P_U) \subseteq \mathrm{IRR}(S)$, then also the resulting system Q_U has this property. In this case we say that Q_U is *S-reduced*. Further, we will call a prefix-rewriting system $P = P_U \cup P_S$ *prefix-interreduced*, *p-interreduced* for short, if $v \in \mathrm{IRR}(P)$ and $u \in \mathrm{IRR}(P \setminus \{(u, v)\})$ hold for each prefix-rule $(u, v) \in P_U$, and we call it *p-canonical* if it is convergent and p-interreduced.

Example 4.2. (continued)
Let $\geq$ be the length-lexicographical ordering on $\underline{\Sigma}_2^*$ that is induced by $\bar{b} > b > \bar{a} > a$, and let $P_U := \{(ab, \lambda), (ba, \lambda), (aa, \lambda), (\bar{b}\bar{a}, \lambda), (\bar{a}\bar{b}, \lambda), (\bar{a}\bar{a}, \lambda)\}$. Then $Q_0 = P_U$, there are no U-critical pairs, but there are three G-critical pairs for $Q_0 : CP_0 = \{(\bar{b}, a), (\bar{a}, b), (\bar{a}, a)\}$. Hence, we get $Q_1 := Q_0 \cup \{(\bar{b}, a), (b, \bar{a}), (\bar{a}, a)\}$.

The G-critical pairs of Q_1 all resolve, but there is an unresolved U-critical pair: $(a\bar{b}, \lambda)$. This yields $Q_2 := Q_1 \cup \{(a\bar{b}, \lambda)\}$, which in turn gives the unresolved G-critical pair (b, a). Finally, we obtain $Q_3 := Q_2 \cup \{(b, a)\}$, and $Q_3 \cup P_{S_0}$ is convergent.

By interreduction Q_3 is transformed into the system $Q_U := \{(ab, \lambda), (\bar{b}, a), (a\bar{b}, \lambda), (b, a), (aa, \lambda), (\bar{a}, a)\}$. The prefix-rewriting system $P := Q_U \cup P_{S_0}$ is p-canonical, satisfying $\Leftrightarrow_P^* = \sim_U$. Thus, $\mathrm{IRR}(P) = \{\lambda, a\}$ is a complete set of coset representatives for $\langle U \rangle$ in F_2, showing that $|F_2 : \langle U \rangle| = 2$. □

For the following considerations we fix a group-presentation $\langle \Sigma; \emptyset \rangle$ of a free group F. Recall that S_0 denotes the set of trivial rules $S_0 = \{a\bar{a} \to \lambda, \bar{a}a \to \lambda \mid a \in \Sigma\}$.

Proposition 4.8. [Cre95]
Let P_U *be a prefix-rewriting system on* $\langle \Sigma; \emptyset \rangle$, *and let* $P := P_U \cup P_{S_0}$. *Then the system* P *is p-canonical if and only if the following two conditions are satisfied:*

(1.) P *is p-interreduced, and*

(2.) for each rule $(ua, v) \in P_U$, *where* $u, v \in \underline{\Sigma}^*$ *and* $a \in \underline{\Sigma}$, (va^{-1}, u) *is also a rule of* P_U.

Let $P = P_U \cup P_{S_0}$ be a p-canonical system on $\langle \Sigma; \emptyset \rangle$. If the left-congruence $\Leftrightarrow_P^*$ on $\underline{\Sigma}^*$ is finitely generated, then P_U contains a finite subsystem P_{U_1} such that $P_1 := P_{U_1} \cup P_{S_0}$ also generates this left-congruence. Let $P_{U_2} := P_{U_1} \cup \{(va^{-1}, u) \mid (ua, v) \in P_{U_1}\}$. Then P_{U_2} is still a finite subsystem of P_U, and $P_2 := P_{U_2} \cup P_{S_0}$ generates the left-congruence $\Leftrightarrow_P^*$. However, by Proposition 4.8 P_2 is itself p-canonical, which implies that P_2 coincides with P_U. This gives the following result.

Proposition 4.9. [Cre95]
Let P_U be a prefix-rewriting system on $\langle \Sigma; \emptyset \rangle$ such that $P := P_U \cup P_{S_0}$ is p-canonical. If the left-congruence $\Leftrightarrow_P^*$ is finitely generated, then P_U is itself finite.

Now let U be a finite subset of $\underline{\Sigma}^*$ that is closed under inverses, and let $P_U := \{(u, \lambda) \mid u \in U\}$. Then $\Leftrightarrow_P^* = \sim_U$, where $P := P_U \cup P_{S_0}$ and hence, $\Leftrightarrow_P^*$ is finitely generated. Thus, if $\geq$ is any admissible well-ordering on $\underline{\Sigma}^*$, then the p-canonical prefix-rewriting system Q_U that is compatible with $\geq$ and that satisfies $\Leftrightarrow_{Q_U \cup S_0}^* = \sim_U$ is finite. Hence, given $(\underline{\Sigma}; S_0)$, P_U and $\geq$ as input, the Knuth-Bendix completion procedure for prefix-rewriting systems is guaranteed to terminate successfully.

Actually we can characterize the p-canonical prefix-rewriting systems on $\langle \Sigma; \emptyset \rangle$ as follows.

Definition 4.10. Let $U \subseteq \underline{\Sigma}^*$ be a set of freely reduced strings, that is, $U \subseteq \mathrm{IRR}(S_0)$.

(a) The set U is called *reduced* if $\lambda \notin U$ and if, for each string $w \in U$, $w^{-1} \notin U$. By $\underline{U}$ we denote the set $\underline{U} := U \cup U^{-1}$. A prefix of a string in $\underline{U}$ is called *isolated* if it does not occur as a prefix of any other string of $\underline{U}$.

(b) The set U is called *marked* if $\lambda \notin U$ and one letter of each string $w \in U$ is marked as the *central factor* of w. For a string $w = uav \in U$, where $u, v \in \underline{\Sigma}^*$ and $a \in \underline{\Sigma}$ is the marked letter, ua is called the *major prefix* of w, and $v^{-1}a^{-1}$ is called the *major suffix* of w.

(c) The set U is called *generalized Nielsen reduced* if it is reduced and marked, and if each major prefix and each major suffix is isolated.

It can be checked fairly easily that a Nielsen reduced set is generalized Nielsen reduced. For a string of odd length, the letter in the middle can be marked, and for a string of even length one of the letters next to the middle of the string can be marked (see, e.g., [MKS76], p.123).

Generalized Nielsen reduced sets can be used to characterize p-canonical prefix-rewriting systems of the form $P := P_U \cup P_{S_0}$. Let P_U be a prefix-rewriting system on $\langle \Sigma; \emptyset \rangle$ such that P is p-canonical. Then by Proposition 4.8 P_U is the union of two-rule systems of the form $\{(ua, v), (va^{-1}, u)\}$. With a two-rule system of this form we associate the freely reduced string uav^{-1}, where we mark the letter a at position $|u| + 1$. Let V be the set consisting of all these strings. Since P is p-reduced, it is easily verified that V is a generalized Nielsen reduced set, and that $\Leftrightarrow_P^* = \sim_V$. Conversely, if $V \subseteq \underline{\Sigma}^+$ is a generalized Nielsen reduced set, then with each string $w = uav \in V$, where $a \in \underline{\Sigma}$ is the marked letter, we associate the two prefix-rules (ua, v^{-1}) and $(v^{-1}a^{-1}, u)$. Let P_U be the prefix-rewriting system consisting of all these rules, and let $P := P_U \cup P_{S_0}$. Since all elements of V are freely reduced, we see that $ua, v^{-1}, v^{-1}a^{-1}, u \in \mathrm{IRR}(S_0)$. Further, since each major prefix ua and each major suffix $v^{-1}a^{-1}$ is isolated, P is in fact p-interreduced. Thus, by Proposition 4.8 P is p-canonical. Hence, we have the following result which extends a result of G. Bauer [Bau81].

Proposition 4.11. [Cre95]
There is a one-to-one correspondence between the set of p-canonical prefix-rewriting systems of the form $P = P_U \cup P_{S_0}$ on $\langle \Sigma; \emptyset \rangle$ and the set of generalized Nielsen reduced subsets of $\underline{\Sigma}^+$.

In particular, it follows that the computation of a (generalized) Nielsen reduced set V from a given finite set U can be interpreted as completing the prefix-rewriting system $P_U \cup P_{S_0}$.

We close this section by taking another look at the Todd-Coxeter coset enumeration method. If $\langle \Sigma; S \rangle$ is a finite presentation, $U \subseteq \underline{\Sigma}^*$ a finite set, and $\geq$ an admissible well-ordering on $\underline{\Sigma}^*$, then in TC we can always choose those coset representatives that are minimal with respect to $\geq$. By this we mean the following. If w is currently a coset representative, and the slot for $w \cdot a$ is not yet filled in one of the tables, then wa is taken as a representative. If later a collaps equation $wa \sim z$ or a bonus equation $wa \cdot b \sim z$ is discovered, then wa and z, respectively wa and zb^{-1}, are compared with respect to $\geq$, and the smaller of the two strings will be chosen as the new representative for the coset of wa. If TC terminates, then the set of coset representatives is prefix-closed, and the prefix-rewriting system $\{(ua, v) \mid u, v \text{ are representatives}, a \in \underline{\Sigma}, ua \neq v\}$, which is essentially just a description of the non-trivial part of the coset multiplication table determined by TC, is canonical and it defines the left-congruence $\sim_U$. Thus, TC can also be seen as a method that determines finite canonical prefix-rewriting systems for subgroups of finite index. The correspondence between TC and standard string-rewriting completion has first been observed by B. Benninghofen et al [BKR87] in the case that the subgroup considered is trivial.

5 Uniform solvability of the subgroup problem

As seen in the previous section for free groups the subgroup problem can be solved by determining p-canonical prefix-rewriting systems for the left-congruences generated by the subgroups considered. This approach exploited the fact that the free groups considered are presented through standard presentations of the form $\langle \Sigma; \emptyset \rangle$, that is, through finite, special, and confluent presentations of the form $(\underline{\Sigma}; S_0)$. Here we will see that these results can be carried over to certain classes of more general presentations. We follow the development given by R. Cremanns [Cre95].

Definition 5.1. Let $(\Sigma; S)$ be a finite convergent presentation. This presentation is said to satisfy the *local finiteness condition for p-canonical prefix-rewriting systems* if the following condition holds for each p-canonical prefix-rewriting system $P := P_U \cup P_S$ on Σ^*:

(lfc) for each rule $(u, v) \in P_U$, there exists a finite subsystem $P_{U'}$ of P_U such that $(u, v) \in P_{U'}$ and $P' := P_{U'} \cup P_S$ is p-canonical.

Proposition 4.8 shows essentially that the presentation $\langle \Sigma; \emptyset \rangle$ satisfies the above condition. Accordingly the arguments leading to Proposition 4.9 can be generalized, giving the following result.

Proposition 5.2. *Let $(\Sigma; S)$ be a finite convergent presentation that satisfies the local finiteness condition for p-canonical prefix-rewriting systems, and let $P := P_U \cup P_S$ be a p-canonical prefix-rewriting system on Σ. If the left-congruence $\Leftrightarrow_P^*$ is finitely generated, then the subsystem P_U is itself finite.*

Thus, if $(\Sigma; S)$ is a finite presentation of a group G such that S is convergent and $(\Sigma; S)$ satisfies the condition (lfc), then the Knuth-Bendix completion procedure for prefix-rewriting systems is guaranteed to terminate with success, when $(\Sigma; S)$, a finite set $P_U = \{(u, \lambda) \mid u \in U \cup U^{-1}\}$, and an arbitrary admissible well-ordering $\geq$ are given as input. The resulting finite set Q_U has the property that $Q_U \cup P_S$ is convergent and generates the left-congruence $\sim_U$.

Corollary 5.3. *For each finite convergent presentation $(\Sigma; S)$ satisfying the condition (lfc) the subgroup problem and the index problem can be solved by effectively determining a finite set of prefix-rules P_Q such that $P := P_Q \cup P_S$ is convergent, and $\Leftrightarrow_P^* = \sim_U$.*

Which classes of finite convergent presentations of groups do satisfy the condition (lfc)? In order to verify the condition (lfc) for certain classes of presentations, R. Cremanns introduced the following technical notion.

Definition 5.4. Let $(\Sigma; S)$ be a finite convergent presentation of a group, and let $^{-1} : \Sigma^* \to \Sigma^*$ be a function realizing the inverse function of the group presented such that $a^{-1} \neq \lambda$ for all $a \in \Sigma$. The presentation $(\Sigma; S)$ is called *compact* if there exists a set of strings $C \subseteq \Sigma^*$ that satisfies all of the following conditions:

(1.) C only contains elements of finitely many congruence classes modulo S, that is, there is a finite subset $C' \subseteq C$ such that $\bigcup_{u \in C} [u]_S = \bigcup_{u \in C'} [u]_S$;

(2.) $C \supseteq \mathrm{dom}(S)$;

(3.) C is closed under the following operations:

  (3.1) substrings, that is, if $xuy \in C$, then $u \in C$,

  (3.2) S-reductions, that is, if $u \in C$, then $\Delta_S^*(u) \subseteq C$,

  (3.3) overlaps, that is, if $xy \in C$ and $yz \in C$ for some $y \neq \lambda$, then $xyz \in C$,

  (3.4) inverses, that is, if $u \in C$, then $u^{-1} \in C$;

(4.) for all $a \in \Sigma$, $aa^{-1} \in C$ and $a^{-1}a \in C$.

Assume that $(\Sigma; S)$ is compact, and that $C \subseteq \Sigma^*$ is the corresponding compact subset of Σ^*. By (4.) and (3.1) we have $\Sigma \subseteq C$. Further (4.) and (3.3), (3.4) imply that $uu^{-1}, u^{-1}u \in C$ for all $u \in C$. Compact presentations are of interest because of the following result.

Proposition 5.5. *If a finite convergent presentation of a group is compact, then it satisfies the local finiteness condition for p-canonical prefix-rewriting systems.*

Hence, Corollary 5.3 applies to finite convergent presentations of groups that are compact.

Proposition 5.6.

(a) If $(\Sigma; S)$ is a finite presentation of a group such that S is a special and canonical string-rewriting system, then $(\Sigma; S)$ is compact.

(b) If $(\Sigma; S)$ is a finite presentation of a group such that S is a monadic and canonical string-rewriting system satisfying $\mathrm{dom}(S) \subseteq \Sigma^2$ and $|a^{-1}| = 1$ for all $a \in \Sigma$, then $(\Sigma; S)$ is compact.

(c) If $(\Sigma; S)$ is a finite convergent presentation of a finite group, then $(\Sigma; S)$ is compact.

The presentations in (b) are called *two-monadic* with *inverses of length* 1. Thus, we have the following result.

Corollary 5.7. [Kuh91, Cre95]
Let a group G be given through a finite canonical presentation $(\Sigma; S)$ such that S is special or two-monadic with inverses of length 1, and let $U \subseteq \Sigma^*$ be a finite set. For any admissible well-ordering that is compatible with S, a finite set of prefix-rules Q_U can be determined such that $P := Q_U \cup P_S$ is p-canonical and $\Leftrightarrow_P^* = \sim_U$, thus solving the subgroup problem and the index problem for $(\Sigma; S)$.

If $(\Sigma; S)$ is a finite presentation of a group such that the string-rewriting system S is two-monadic and confluent, then a finite subset Σ_1 of Σ exists such that each letter $a \in \Sigma_1$ has an inverse of length one, the subsystem $S_1 := S \cap (\Sigma_1^2 \times (\Sigma_1 \cup \{\lambda\}))$ is confluent, and $(\Sigma_1; S_1)$ presents the same group as $(\Sigma; S)$ [AMO86]. Hence, $(\Sigma_1; S_1)$ satisfies the hypothesis of Corollary 5.7. Since Σ_1 can be determined effectively from $(\Sigma; S)$, this implies that Corollary 5.7 extends to two-monadic confluent presentations of groups.

There is one other class of finite convergent presentations for which the subgroup problem has been solved by computing p-canonical prefix-rewriting systems. This is a very special class of presentations for the finitely generated virtually free groups, which by a result of D.E. Muller and P.E. Schupp coincide with the context-free groups [MS83].

Let F_Σ be the free group presented by $\langle \Sigma; \emptyset \rangle$, and let E be a finite group. Further, let D be a finite alphabet in one-to-one correspondence to $E \setminus \{1\}$, where we assume without loss of generality that $D \cap \underline{\Sigma} = \emptyset$. For each $a \in D$, let $\varphi_a : \underline{\Sigma} \to \mathrm{IRR}(S_0)$ be a function, and for all $a, b \in D \cup \{\lambda\}$, let $z_{a,b} \in \mathrm{IRR}(S_0)$ be a freely reduced string. By φ_λ we denote the inclusion $\underline{\Sigma} \to \mathrm{IRR}(S_0)$. Now let $\Gamma := \underline{\Sigma} \cup D$, and let S be the string-rewriting system on Γ that consists of the following three groups of rules:

(F)	$s\bar{s} \to \lambda$, $\bar{s}s \to \lambda$	for all $s \in \Sigma$;
(E)	$ab \to cz_{a,b}$	for all $a, b \in D, c \in D \cup \{\lambda\}$ satisfying $ab =_E c$;
(K)	$sa \to a\varphi_a(s)$	for all $s \in \underline{\Sigma}$ and $a \in D$.

It is easily seen that S is noetherian, but in general S will not be confluent. The presentation $(\Gamma; S)$ is called *virtually free* if S is confluent, that is, S is even canonical.

Lemma 5.8. [CO94]
The presentation $(\Gamma; S)$ described above is canonical if and only if the following three conditions are satisfied:

(1.) For all $a \in D$ and all $s \in \underline{\Sigma}$, $\varphi_a(s)\varphi_a(s^{-1}) \leftrightarrow_{S_0}^* \lambda$.

(2.) For all $a, b, c \in D \cup \{\lambda\}$, $\varphi_c(z_{a,b}) \leftrightarrow_{S_0}^* z_{ab,c}^{-1} z_{a,bc} z_{b,c}$.

(3.) For all $a, b \in D \cup \{\lambda\}$ and all $s \in \underline{\Sigma}$, $\varphi_b(\varphi_a(s)) \leftrightarrow_{S_0}^* z_{a,b}^{-1} \varphi_{ab}(s) z_{a,b}$.

If $(\Gamma; S)$ is a virtually free presentation, then the monoid presented by $(\Gamma; S)$ is obviously a group. In fact, it is an extension of the free group F_Σ by the finite group E. Conversely, each group of this form admits a virtually free presentation. Hence, we have the following characterization.

Proposition 5.9. *A monoid admits a virtually free presentation if and only if it is a finitely generated virtually free group, that is, a context-free group.*

Because of Lemma 5.8 it is easily decidable whether or not a finite presentation is virtually free. Hence, the virtually free presentations form an easily recognizable subclass of the class of all finite canonical presentations of groups. Notice that context-free groups

may also admit finite canonical presentations of a different form, and that the virtually free presentations are not at all succinct, since they contain the complete multiplication table of the finite extension group.

Let $(\Gamma; S)$ be a virtually free presentation of a group G. Then G is represented by the set of normal forms $\mathrm{IRR}(S) = (D \cup \{\lambda\}) \cdot \mathrm{IRR}(S_0)$. Accordingly in order to describe subgroups of G we can restrict our attention to sets P_U of prefix-rules satisfying $P_U \subseteq \mathrm{IRR}(S) \times \mathrm{IRR}(S)$.

Proposition 5.10. [CO94]
Let $(\Gamma; S)$ be a virtually free presentation, and let $P_U \subseteq \mathrm{IRR}(S) \times \mathrm{IRR}(S)$ be a set of prefix-rules. Then the prefix-rewriting system $P := P_U \cup P_S$ is p-canonical if and only if the following two conditions are satisfied:

(1.) P is p-interreduced, and

(2.) for each rule $(aus, bv) \in P_U$, where $a, b \in D \cup \{\lambda\}$, $u, v \in \underline{\Sigma}^*$, and $s \in \underline{\Sigma}$, (bvs^{-1}, au) is also a rule of P_U.

This yields as a consequence the fact that each virtually free presentation satisfies the local finiteness condition for p-canonical prefix-rewriting systems, which in turn implies that the Knuth-Bendix completion procedure for prefix-rewriting systems terminates with success whenever it is given a virtually free presentation $(\Gamma; S)$, a finite set of prefix-rules P_U and an arbitrary admissible well-ordering on Γ^* (Proposition 5.2). Actually by exploiting the particular properties of virtually free presentations the following stronger result can be derived.

Proposition 5.11. [CO94]
There exists an algorithm that solves the following task in polynomial time:

INPUT: *A virtually free presentation $(\Gamma; S)$ and a finite set of generators $U \subseteq \Gamma^*$.*

OUTPUT: *A finite set P_U of prefix-rules such that the prefix-rewriting system $P := P_U \cup P_S$ is p-canonical, and P generates the left-congruence $\sim_U$ on Γ^*. Further, P_U has a partition $P_U = P_1 \cup P_2$ of the form $P_1 \subseteq D \times (D \cup \{\lambda\}) \cdot \underline{\Sigma}^*$ and $P_2 \subseteq \bigcup_{a \in D \cup \{\lambda\}} (a \cdot \underline{\Sigma}^* \times a \cdot \underline{\Sigma}^*)$.*

In order to solve the subgroup problem for a presentation $(\Sigma; S)$ by prefix-rewriting, it suffices to construct a finite set P_U of prefix rules such that the system $P := P_U \cup P_S$ generates the left-congruence $\sim_U$, and P is noetherian and λ-confluent. Unfortunately λ-confluence is in general much harder to decide than confluence. In the following we restrict our attention to finite canonical presentations $(\Sigma; S)$ of groups.

Let P_U be a finite set of prefix-rules on Σ, and let $P := P_U \cup P_S$. For $w \in \Sigma^*$ let $RC(w) := \{z \in \mathrm{IRR}(S) \mid wz \Rightarrow_P^* \lambda\}$ be the set of *right contexts* of w. Using sets of this form we obtain the following characterization for λ-confluence of P.

Proposition 5.12. [KMO90]
Let $(\Sigma; S)$ be a finite convergent presentation, and let P_U be a set of prefix-rules on Σ such that $P := P_U \cup P_S$ is noetherian. Then the following two statements are equivalent:

(1.) The prefix-rewriting system P is λ-confluent.

(2.) For each U- or G-critical pair (p, q) of P, p and q are joinable modulo P or $RC(p) = RC(q)$.

Although the sets of U- and G-critical pairs are finite for each finite system P_U, the characterization above has the serious drawback that the sets $RC(w)$ of right contexts need not even be recursive. However, in certain restricted instances these sets are quite simple.

Example 5.13. Let $G = \mathbb{Z} \times \mathbb{Z}_2$ be given by the presentation $(\Sigma; S)$, where $\Sigma := \{a, \bar{a}, b\}$ and $S := \{ba \to ab, b\bar{a} \to \bar{a}b, b^2 \to \lambda, a\bar{a} \to \lambda, \bar{a}a \to \lambda\}$, and let $P_U := \{(b, \lambda)\}$, that is, we consider the subgroup of G that is generated by $U := \{b\}$.

Then it can be shown that there does not exist a finite set of prefix-rules P_1 such that the prefix-rewriting system $P_1 \cup P_S$ is convergent and equivalent to $P := P_U \cup P_S$. On the other hand, there are no U-critical pairs for P_U and only the following three G-critical pairs: $(a, ab), (\bar{a}, \bar{a}b), (b, \lambda)$.

The pair (b, λ) is joinable by $b \Rightarrow_P \lambda$. Further,

$RC(a) = \{a^i b^\varepsilon \mid i \in \mathbb{Z}, \varepsilon \in \{0,1\} \text{ such that } a^{i+1}b^\varepsilon \Rightarrow_P^* \lambda\} = \{\bar{a}, \bar{a}b\}$,
$RC(ab) = \{a^i b^\varepsilon \mid i \in \mathbb{Z}, \varepsilon \in \{0,1\} \text{ such that } aba^i b^\varepsilon \Rightarrow_P^* \lambda\} = \{\bar{a}, \bar{a}b\}$, and
$RC(\bar{a}) = \{a, ab\} = RC(\bar{a}b)$.

Hence, P is λ-confluent, that is, $w \in \langle U \rangle$ if and only if $w \Rightarrow_P^* \lambda$. □

Proposition 5.12 yields a test for deciding λ-confluence of P whenever the presentation $(\Sigma; S)$ has the following properties:

(a) The languages of the form $RC(w)$ belong to a family of languages for which equality is decidable.

(b) From $(\Sigma; S)$, P_U and $w \in \Sigma^*$, a specification of the language $RC(w)$ can be computed effectively such that the equality test of (a) is applicable to this specification.

For example, if $(\Sigma; S)$ is a finite, confluent, and weight-reducing presentation of a group, then the languages of the form $RC(w)$ are regular, and finite-state acceptors can effectively be constructed for them [KMO90]. Thus, λ-confluence of prefix-rewriting systems is decidable for this class of presentations. Actually, since the equivalence problem is decidable for multi-tape deterministic finite-state acceptors [HK91], this result carries over to finite direct products of groups presented by finite, confluent, and weight-reducing presentations. Observe, however, that the finite, confluent, and weight-reducing presentations only describe a proper subclass of the context-free groups [MO89].

In addition to Proposition 5.12 there is still another criterion for deciding λ-confluence. Let $(\Sigma; S)$ be a finite convergent presentation of a group, let P_U be a set of prefix-rules on Σ, and let $P := P_U \cup P_S$, where we assume that the set $U := \{uv^{-1} \mid (u, v) \in P_U\}$ is closed under taking inverses. Then $[\lambda]_P = \langle U \rangle$, and hence, $w \in [\lambda]_P$ if and only if $w \Leftrightarrow_P^* z$ for some $z \in U^*$. Now P is λ-confluent if and only if each string $w \in \langle U \rangle \setminus \{\lambda\}$ is reducible by P, that is, if and only if $[\lambda]_P \cap \mathrm{IRR}(P) = \{\lambda\}$. However, since S is convergent, the latter equality is equivalent to the equality $(\Delta_S^*(U^*) \cap \mathrm{IRR}(S)) \cap \mathrm{IRR}(P) = \{\lambda\}$.

If S and P_U are both finite, then the sets $\mathrm{IRR}(S)$ amd $\mathrm{IRR}(P)$ are both regular, and finite-state acceptors for them can be constructed effectively. Also U^* is a regular set in this situation. Hence, this criterion becomes decidable whenever the set $\Delta_S^*(U^*)$ (or the set $\Delta_S^*(U^*) \cap \mathrm{IRR}(S)$) allows an effective specification for which the intersection with the regular set $\mathrm{IRR}(P)$ can be determined effectively.

If $(\Sigma; S)$ is a finite, weight-reducing, and confluent presentation of a group and $U \subseteq \Sigma^*$ is a finite set, then it is still an open problem whether or not the set $\Delta_S^*(U^*)$ is necessarily regular. However, if we restrict the set $\Delta_S^*(U^*)$ to only those strings that are obtained by left-most reductions, then this subset $\Delta_{L,S}^*(U^*)$ can be shown to always be regular

[Kuh91]. In fact, a finite-state acceptor for this language can be constructed effectively. Since $\Delta^*_{L,S}(U^*) \cap \mathrm{IRR}(S) = \Delta^*_S(U^*) \cap \mathrm{IRR}(S)$, we obtain a finite-state acceptor for the set $\Delta^*_S(U^*) \cap \mathrm{IRR}(P)$. This gives the following decidability result.

Proposition 5.14. [Kuh91]
Let $(\Sigma; S)$ be a finite, weight-reducing, and confluent presentation of a group, and let P_U be a finite set of prefix-rules on Σ such that the set $U := \{uv^{-1} \mid (u, v) \in P_U\}$ is closed under taking inverses. Then it is decidable whether the prefix-rewriting system $P := P_U \cup P_S$ is λ-confluent.

Now assume that $(\Sigma; S)$ is a finite, weight-reducing, and confluent presentation of a group G, let $U \subseteq \Sigma^+$ be a finite set that is closed under taking inverses, and let $P_U := \{(u, \lambda) \mid u \in U\}$. ¿From $(\Sigma; S)$ and U we can construct a finite-state acceptor $A = (Q, \Sigma, q_0, F, \delta)$ for the language $\Delta^*_S(U^*) \cap \mathrm{IRR}(S)$. ¿From A we extract a finite set of prefix-rules P'_U as follows, where we identify A with its state graph in order to simplify the notation:

(i) For every simple path in A leading from the initial state q_0 to a final state $q_f \in F$, which does not pass through any final state, we put the rule (x, λ) into P'_U, where x is the label along the path considered.

(ii) For every path p in A from q_0 to a final state $q_f \in F$, which does not pass through any final state, and which can be partitioned into three parts $p = p_1, p_2, p_3$ such that p_1 is a simple path, and p_2 is a simple loop, we put the rule $(x_1 x_2, x_1)$ into P'_U, where x_i is the label along the subpath p_i, $i = 1, 2$.

Obviously, P'_U is a finite set of prefix-rules that can effectively be obtained from A. For $w \in \langle U \rangle$ there exists a unique string $w_0 \in \mathrm{IRR}(S)$ such that $w \to^*_S w_0$. Since $w \in \langle U \rangle$, $w_0 \in \Delta^*_S(U^*) \cap \mathrm{IRR}(S)$, and hence, w is accepted by A. ¿From the construction of P'_U it follows that $w \Rightarrow^*_{P'} \lambda$ holds, where $P' := P'_U \cup P_S$. Since $u \sim_U v$ holds for each rule $(u, v) \in P'_U$, it follows that $\Leftrightarrow^*_{P'} = \sim_U$, and P' is a λ-convergent prefix-rewriting system for $\sim_U$.

Proposition 5.15. [Kuh91]
Let $(\Sigma; S)$ be a finite, weight-reducing, and confluent presentation of a group G, and let $U \subseteq \Sigma^+$ be a finite set. Then a finite set of length-reducing prefix-rules P'_U can be determined effectively such that the prefix-rewriting system $P := P'_U \cup P_S$ is λ-convergent and $\Leftrightarrow^*_P = \sim_U$.

If $(\Sigma; S)$ is a finite convergent presentation of a group, and $U \subseteq \Sigma^*$ is a finite set that is closed under taking inverses, then $\Delta^*_S(U^*) \cap \mathrm{IRR}(S)$ is a set of unique representatives for the subgroup $\langle U \rangle$. However, if the string-rewriting system S is not confluent, then there may exist irreducible strings $w \in \mathrm{IRR}(S)$ such that $w \in \langle U \rangle$, but $w \notin \Delta^*_S(U^*)$. In this situation the construction above will not yield a λ-convergent prefix-rewriting system presenting $\sim_U$.

The situation can be saved if the string-rewriting system S is finite, monadic, and λ-confluent, because of the following fact.

Proposition 5.16. [MO91]
Let S be a finite, monadic, and λ-confluent string-rewriting system on Σ such that the monoid presented by $(\Sigma; S)$ is a group. Then, for each regular language $L \subseteq \Sigma^*$, the set $I_S(L) := \{w \in \mathrm{IRR}(S) \mid \exists u \in L : u \leftrightarrow^*_S w\}$ is regular as well. In addition, a finite-state acceptor for $I_S(L)$ can be constructed in polynomial time from S and a finite-state acceptor for L.

Observe that a group can be presented through a finite, monadic, and λ-confluent string-rewriting system if and only if it is a context-free group [ABS87]. By applying the construction of a prefix-rewriting system described above to a finite-state acceptor for $I_S(U^*)$ we obtain the following result.

Proposition 5.17. [KMO94]
Let $(\Sigma; S)$ be a finite, monadic, and λ-confluent presentation of a group, and let $U \subseteq \Sigma^+$ be a finite set. Then a finite set of length-reducing prefix-rules P'_U can be constructed effectively such that the prefix-rewriting system $P := P'_U \cup P_S$ is λ-convergent and $\Leftrightarrow_P^* = \sim_U$.

Even though the prefix-rewriting system P is not convergent, it can be used to determine the index $|G : \langle U \rangle|$, where G is the group presented by $(\Sigma; S)$. This is due to the fact that in the situation described in the proposition above, the intersection $[y]_P \cap \mathrm{IRR}(P)$ is finite for each string $y \in \Sigma^*$. Thus, the index $|G : \langle U \rangle|$ is infinite if and only if $\mathrm{IRR}(P)$ is infinite, and in case $\mathrm{IRR}(P)$ is finite, we can actually determine the index $|G : \langle U \rangle|$ by checking which of the finitely many strings of $\mathrm{IRR}(P)$ belong to the same coset.

We finally turn to presentations of polycyclic groups. Let $\Sigma = \{a_1, \bar{a}_1, \ldots, a_n, \bar{a}_n\}$, let $\Sigma_i := \{a_i, \bar{a}_i, \ldots, a_n, \bar{a}_n\}$ for $i = 1, 2, \ldots, n$, and let $\Sigma_{n+1} := \emptyset$. We need several particular classes of rules on Σ. A rule $(\ell \to r)$ is called

- a *CP2-rule* if $\ell = a_j^\delta a_i^\varepsilon$ and $r = a_i^\varepsilon z$ for some $j > i$, $\delta, \varepsilon \in \{1, -1\}$, and $z \in \Sigma_{i+1}^*$,
- a *positive P-rule* if $\ell = a_i^k$ and $r \in \Sigma_{i+1}^*$ for some $i \in \{1, \ldots, n\}$ and $k > 0$,
- a *negative P-rule* if $\ell = \bar{a}_i$ and $r = a_i^k z$ for some $i \in \{1, \ldots, n\}$, $k \geq 0$, and $z \in \Sigma_{i+1}^*$.

A set S of rules is called

- a *P-system* if it contains P-rules only, and for each $i \in \{1, \ldots, n\}$, S either contains exactly one rule with left-hand side a_i^k for some $k > 0$ and exactly one rule with left-hand side $\bar{a}_i$, or S contains no rule with left-hand side from $\{a_i, \bar{a}_i\}^+$,
- a *CP2-system* if it contains CP2-rules only, and for each $i, j \in \{1, \ldots, n\}$, $j > i$, and each $\delta, \varepsilon \in \{1, -1\}$, S contains exactly one rule with left-hand side $a_j^\delta a_i^\varepsilon$.

A presentation $(\Sigma; S)$ is called a *PCP2-presentation* if S can be written as $S = S_0 \cup R \cup C$, where $S_0 = \{a_i \bar{a}_i \to \lambda, \bar{a}_i a_i \to \lambda \mid i = 1, \ldots, n\}$ is the set of trivial rules, R is a P-system, and C is a CP2-system.

Using a particular ordering D. Wißmann shows that a string-rewriting system of this form is noetherian. Further, he proves that a group G can be described through a finite PCP2-presentation if and only if G is a finitely presented polycyclic group [Wiß89]. Actually the PCP2-presentations are closely related to the polycyclic presentations of [BCM77]. In fact, based on a specialized version of the Knuth-Bendix completion procedure D. Wißmann proves that each finite PCP2-presentation of a polycyclic group G can be transformed into a finite convergent PCP2-presentation of G. Accordingly in the following we consider polycyclic groups that are given through finite convergent PCP2-presentations.

Let $(\Sigma; S)$ be a finite convergent PCP2-presentation of a polycyclic group G, let U be a finite subset of Σ^+, and let $H := \langle U \rangle$. As shown by D. Wißmann a canonical base Ω for the subgoup H can be constructed effectively by employing a specialized completion procedure [Wiß89]. With Ω a finite set of prefix-rules P_U can be associated in a straightforward manner. The resulting prefix-rewriting system $P := P_U \cup P_S$ is λ-convergent, and $\Leftrightarrow_P^* = \sim_U$. Thus, we have the following result.

Proposition 5.18. [Wiß89]
Let $(\Sigma; S)$ be a finite (convergent) PCP2-presentation of a polycyclic group G, and let U be a finite subset of Σ^+. Then a finite set of prefix-rules P_U can be constructed effectively such that the prefix-rewriting system $P := P_U \cup P_S$ is λ-convergent, and $\Leftrightarrow_P^* = \sim_U$.

For a more detailed presentation of this result see for example [KMO94]. Using a different ordering on the letters and slightly different convergent presentations for polycyclic groups this result can be strengthened to obtain a finite set of prefix-rules such that P is even convergent [MR98c].

6 The subgroup presentation problem

Using prefix-rewriting systems that are λ-convergent or even convergent we have been able to solve the subgroup problem for certain classes of finite presentations of groups. The groups presented by these classes of presentations are the finitely generated polycyclic groups, the context-free groups, and certain subclasses thereof. However, the polycyclic groups and the context-free groups are both subgroup closed, that is, each finitely generated subgroup of a finitely presented polycyclic, respectively context-free, group is itself a finitely presented polycyclic, respectively context-free, group. Hence, each subgroup of this form has a finite presentation, and accordingly, from the given presentation of the group and the given set of generators for the subgroup we want to determine a finite presentation of the subgroup effectively. Preferably we would like to obtain a presentation for the subgroup that is of the same type as the presentation of the group given.

For the class of free groups given through free presentations of the form $\langle \Sigma; \emptyset \rangle$ this problem has already been solved implicitly in Section 4. For a presentation $\langle \Sigma; \emptyset \rangle$ and a finite set of strings $U \subseteq \underline{\Sigma}^*$, a finite set P_U of prefix-rules can be constructed effectively such that the prefix-rewriting system $P := P_U \cup P_{S_0}$ is convergent, and $\Leftrightarrow_P^* = \sim_U$. ¿From P_U a finite set V can be obtained that is generalized Nielsen reduced, and that generates the same subgroup as U. Thus, V is a set of free generators for $\langle U \rangle$, that is, $\langle \Gamma_V; \emptyset \rangle$ is a free presentation of $\langle U \rangle$, where Γ_V is an alphabet in one-to-one correspondence to V.

Actually this process is a special case of a procedure that applies to finite convergent presentations of groups and convergent prefix-rewriting systems presenting subgroups. In order to describe this procedure we need some additional notions.

Let $(\Sigma; S)$ be a finite canonical presentation of a group G, let P_U be a finite set of prefix-rules on Σ such that the prefix-rewriting system $P := P_U \cup P_S$ is convergent, and let H denote the subgroup of G that is generated by P_U. Our aim is to present a construction that yields a finite presentation for H from $(\Sigma; S)$ and P_U.

With $(\Sigma; S)$ and P_U we associate an infinite graph $\Gamma := (V, E, \sigma, \tau, ^{-1})$, where

(a) $V := \Sigma^*$ is the set of vertices,

(b) $E := \{(x, (\ell, r), y, \varepsilon) \mid (\ell, r) \in S, x, y \in \Sigma^*, \varepsilon \in \{1, -1\}\} \cup \{((u, v), y, \varepsilon) \mid (u, v) \in P_U, y \in \Sigma^*, \varepsilon \in \{1, -1\}\}$

is the set of edges,

(c) $\sigma, \tau : E \to V$ are mappings that associate with each edge $e \in E$ its initial vertex $\sigma(e)$ and its terminal vertex $\tau(e)$:

$$\sigma(x, (\ell, r), y, \varepsilon) := \left\{ \begin{array}{ll} x\ell y, & \text{if } \varepsilon = 1 \\ xry, & \text{if } \varepsilon = -1 \end{array} \right\}, \quad \tau(x, (\ell, r), y, \varepsilon) := \left\{ \begin{array}{ll} xry, & \text{if } \varepsilon = 1 \\ x\ell y, & \text{if } \varepsilon = -1 \end{array} \right\},$$

and

$$\sigma((u,v),y,\varepsilon) := \left\{ \begin{array}{ll} uy, & \text{if } \varepsilon = 1 \\ vy, & \text{if } \varepsilon = -1 \end{array} \right\}, \quad \tau((u,v),y,\varepsilon) := \left\{ \begin{array}{ll} vy, & \text{if } \varepsilon = 1 \\ uy, & \text{if } \varepsilon = -1 \end{array} \right\},$$

(d) $^{-1} : E \to E$ is a mapping that associates with each edge $e \in E$ its inverse edge e^{-1}:

$$(x,(\ell,r),y,\varepsilon)^{-1} := (x,(\ell,r),y,-\varepsilon), \quad \text{and} \quad ((u,v),y,\varepsilon)^{-1} := ((u,v),y,-\varepsilon).$$

Thus, this graph represents the relation $\Rightarrow_P$ on Σ^*. It is obtained from the graph Γ_S considered by C. Squier [SOK94] for the (finite) monoid-presentation $(\Sigma; S)$ by adding the edges corresponding to the prefix-rules P_U.

This graph has some additional structure in the form of a right action of Σ^* on Γ. Let $z \in \Sigma^*$. Then $w \cdot z := wz$ for each $w \in V$, and $(x,(\ell,r),y,\varepsilon) \cdot z := (x,(\ell,r),yz,\varepsilon)$ and $((u,v),y,\varepsilon) \cdot z := ((u,v),yz,\varepsilon)$ for all edges $(x,(\ell,r),y,\varepsilon) \in E$ and $((u,v),y,\varepsilon) \in E$.

By $P(\Gamma)$ we denote the set of paths in Γ, where we include a path (w) of length zero from w to w for each $w \in V$. The mappings $\sigma, \tau, ^{-1}$ and the right action of Σ^* easily extend to paths. By $P^{(2)}(\Gamma)$ we denote the following set of pairs of paths in Γ:

$$P^{(2)}(\Gamma) := \{(p,q) \mid p,q \in P(\Gamma), \sigma(p) = \sigma(q), \text{ and } \tau(p) = \tau(q)\}.$$

We are interested in certain subsets of $P^{(2)}(\Gamma)$. The *set of disjoint derivations* D_Γ is defined as

$$\begin{array}{rcl} D_\Gamma & := & \{(p \cdot \sigma(q) \circ \tau(p) \cdot q, \sigma(p) \cdot q \circ p \cdot \tau(q)) \mid p \in P(\Gamma), \text{ and } q \in P(\Gamma) \text{ such that} \\ & & \quad q \text{ does not contain any } P_U\text{−edges}\}, \end{array}$$

where $\circ$ denotes the concatenation of paths. The *set of inverse derivations* I_Γ is defined as

$$I_\Gamma := \{(p \circ p^{-1}, (\sigma(p))) \mid p \in P(\Gamma)\}.$$

Clearly, D_Γ and I_Γ are subsets of $P^{(2)}(\Gamma)$. Further, by $P^{(2)}(\Gamma_S)$ we denote the set of pairs $(p,q) \in P^{(2)}(\Gamma)$ of paths such that neither p nor q does contain any P_U-edges.

Definition 6.1. An equivalence relation $\simeq$ on $P(\Gamma)$ is called a *homotopy relation* if it satisfies all of the following conditions:

(1.) $D_\Gamma \cup I_\Gamma \cup P^{(2)}(\Gamma_S) \subseteq \simeq \subseteq P^{(2)}(\Gamma)$,

(2.) if $p \simeq q$, then $p \cdot z \simeq q \cdot z$ for all $z \in \Sigma^*$, and

(3.) if $p, q_1, q_2, r \in P(\Gamma)$ satisfy $\tau(p) = \sigma(q_1) = \sigma(q_2)$, $\tau(q_1) = \tau(q_2) = \sigma(r)$, and $q_1 \simeq q_2$, then $p \circ q_1 \circ r \simeq p \circ q_2 \circ r$.

For each subset $B \subseteq P^{(2)}(\Gamma)$ there exists a smallest homotopy relation $\simeq_B$ on $P(\Gamma)$ that contains B. Accordingly $\simeq_B$ is called the homotopy relation *generated* by B.

Definition 6.2. The prefix-rewriting system $P = P_U \cup P_S$ is said to have *finite derivation type* if there exists a finite set $B \subseteq P^{(2)}(\Gamma)$ that generates the homotopy relation $P^{(2)}(\Gamma)$, that is, $P^{(2)}(\Gamma)$ is the only homotopy relation on $P(\Gamma)$ containing B.

C. Squier introduced this very notion for monoid-presentations proving that a finite canonical monoid-presentation has finite derivation type [SOK94]. Although this property has been investigated thoroughly [OK97], no algebraic characterization has been obtained so far for the class of finitely presented monoids (or groups) that have finite derivation type. For the case of prefix-rewriting systems presenting subgroups of groups the situation is more positive.

Proposition 6.3. [Cre95]
Let $(\Sigma; S)$ be a finite presentation of a group G, let P_U be a finite set of prefix-rules on Σ, let $P := P_U \cup P_S$, and let H be the subgroup of G that is generated by P_U. Then H is itself finitely presented if and only if P has finite derivation type.

If $(\Sigma; S)$ is convergent, and P is convergent as well, then it can be shown that P does have finite derivation type. This yields the following consequence.

Corollary 6.4. [Cre95]
Let $(\Sigma; S)$ be a finite convergent presentation of a group G, and let P_U be a finite set of prefix-rules on Σ such that the prefix-rewriting system $P := P_U \cup P_S$ is convergent. Then the subgroup H of G that is generated by P_U is finitely presented.

Actually a finite presentation for H can be constructed from $(\Sigma; S)$ and P_U as follows. Let $(\Sigma; S)$ be a finite canonical presentation of a group G, let P_U be a finite set of prefix-rules on Σ such that the prefix-rewriting system $P := P_U \cup P_S$ is p-canonical, let H be the subgroup of G that is generated by P_U, and let Γ be the graph associated with $(\Sigma; S)$ and P_U. By $P_+(\Gamma)$ we denote the set of all paths in Γ that only contain positive edges, that is, edges of the form $(x, (\ell, r), y, 1)$ and $((u, v), y, 1)$. In analogy to the definition of critical pairs we obtain critical pairs of edges.

An ordered pair (e_1, e_2) of edges of Γ is called a *G-critical pair of edges*, if $e_1 = ((uw, v), z, 1)$ and $e_2 = (u, (wz, r), \lambda, 1)$, where $(uw, v) \in P_U$, $(wz, r) \in S$, and $w \neq \lambda$. Then (e_1, e_2) corresponds to the G-critical pair (vz, ur) of P.

The ordered pair (e_1, e_2) of edges of Γ is called a *U-critical pair of edges*, if $e_1 = ((uw, v), \lambda, 1)$ and $e_2 = ((u, z), w, 1)$, where $(uw, v), (u, z) \in P_U$ and $w \neq \lambda$ or $v \neq z$. Then (e_1, e_2) corresponds to the U-critical pair (v, zw) of P.

Since the prefix-rewriting system P is convergent, there exists a pair (p_1, p_2) of paths $p_1, p_2 \in P_+(\Gamma)$ for each critical pair of edges (e_1, e_2) such that $\sigma(p_1) = \tau(e_1)$, $\sigma(p_2) = \tau(e_2)$, and $\tau(p_1) = \tau(p_2)$, that is, $(e_1 \circ p_1, e_2 \circ p_2) \in P_+^{(2)}(\Gamma)$. Such a pair (p_1, p_2) is called a *resolution* of (e_1, e_2).

Let B denote the set consisting of all pairs $(e_1 \circ p_1, e_2 \circ p_2)$, where (e_1, e_2) is a G- or a U-critical pair of edges, and (p_1, p_2) is a fixed resolution chosen for (e_1, e_2). Then $B \subseteq P_+^{(2)}(\Gamma)$ is a finite set of pairs of positive paths. Further, let Γ_P be a new alphabet in one-to-one correspondence to P_U, and let f denote the function $f : P_+(\Gamma) \to \Gamma_P^*$ that is defined as follows:

$$
\begin{aligned}
f(p) &:= \lambda, \text{ if } p \text{ is a path of length 0;} \\
f(p \circ e) &:= \begin{cases} f(p), & \text{if } p \in P_+(\Gamma), e = (x, (\ell, r), y, 1), \text{ and } \tau(p) = x\ell y, \\ f(p) \cdot a_{(u,v)}, & \text{if } p \in P_+(\Gamma), e = ((u, v), y, 1), \text{ and } \tau(p) = uy. \end{cases}
\end{aligned}
$$

Here $a_{(u,v)} \in \Gamma_P$ is the letter corresponding to the prefix-rule $(u, v) \in P_U$. Thus, for $p \in P_+(\Gamma)$, $f(p)$ yields (an encoding of) the sequence of prefix-rules from P_U that are applied along the path p. Then the following result holds.

Proposition 6.5. [CO94]
Let $(\Sigma; S)$ be a finite canonical presentation of a group G, let P_U be a finite set of prefix-rules on Σ such that the prefix-rewriting system $P := P_U \cup P_S$ is p-canonical, and let H be the subgroup of G that is generated by P_U. Then $(\Gamma_P; f(B))$ is a finite presentation of H.

Observe that $(\Gamma_P; f(B))$ can be constructed effectively from $(\Sigma; S)$ and P_U.

Example 6.6. Let $\Sigma = \{a, \bar{a}, b, \bar{b}\}$, and let $S = \{b^\varepsilon a^\mu \to a^\mu b^\varepsilon \mid \varepsilon, \mu \in \{1, -1\}\} \cup S_0$. Then $(\Sigma; S)$ is a finite canonical presentation of the group $G = F_1 \times F_1$. Let H be the subgroup of G that is generated by $\{ab\}$, and let $P_U := \{(a, \bar{b}), (\bar{a}, b)\}$. Then $P := P_U \cup P_S$ is a p-canonical prefix-rewriting system such that $\Leftrightarrow_P^* = \sim_H$.

P has no U-critical pairs, but it has the following two G-critical pairs: $\{(\bar{b}\bar{a}, \lambda), (ba, \lambda)\}$. Since $a\bar{a} \Rightarrow_{P_U} \bar{b}\bar{a} \to_S \bar{a}\bar{b} \Rightarrow_{P_U} b\bar{b} \to_{S_0} \lambda \leftarrow_{S_0} a\bar{a}$, and $\bar{a}a \Rightarrow_{P_U} ba \to_S ab \Rightarrow_{P_U} \bar{b}b \to_{S_0} \lambda \leftarrow_{S_0} \bar{a}a$, we obtain the following presentation for H, where α corresponds to the prefix-rule $(a, \bar{b})$, and β corresponds to the prefix-rule $(\bar{a}, b)$:

$$(\{\alpha, \beta\}; \{\alpha\beta \to \lambda, \beta\alpha \to \lambda\}).$$

In particular, this shows that H is the free group of rank one. □

The general result above has several consequences. First of all when applied to the free presentation $\langle \Sigma; \emptyset \rangle$ of a free group and a finite set of prefix-rules P_U such that $P := P_U \cup P_{S_0}$ is p-canonical, the above construction yields a free presentation for the subgroup H generated by P_U.

The class of groups that admit a finite presentation of the form $(\Sigma; S)$, where S is a special and canonical string-rewriting system on Σ, is exactly the class of groups that are free products of finitely many finite and infinite cyclic groups [Coc76]. Since this class of groups is closed under the operation of taking finitely generated subgroups, each such subgroup can be presented through a finite presentation involving a special canonical string-rewriting system. By Corollary 5.7 for each subgroup of this form a finite set of prefix-rules can be constructed such that the resulting prefix-rewriting system is p-canonical. Hence, Proposition 6.5 yields a finite presentation for this subgroup. Actually, the following result holds.

Proposition 6.7. [Cre95]
Let $(\Sigma; S)$ be a finite, special, and canonical presentation of a group G, let U be a finite set of strings from Σ^+, and let $P := P_U \cup P_S$ be a p-canonical prefix-rewriting system for $\sim_U$. Then the construction of Proposition 6.5 yields a finite presentation $(\Gamma; T)$ for the subgroup $\langle U \rangle$ of G such that the string-rewriting system T is special and canonical.

Using a slightly different approach N. Kuhn shows that the presentation $(\Gamma; T)$ of $\langle U \rangle$ can be obtained in polynomial time from $(\Sigma; S)$ and U [Kuh91].

The construction of Proposition 6.5 also applies to virtually free presentations because of Proposition 5.11. By analyzing it in detail the following result has been obtained.

Proposition 6.8. [CO94]
Given a virtually free presentation $(\Sigma; S)$ of a group G and a finite set of generators $U \subseteq \Sigma^+$, a virtually free presentation $(\Gamma; T)$ for the subgroup $\langle U \rangle$ of G can be constructed in polynomial time.

For a finitely generated subgroup H of a polycyclic group G that is given through a finite convergent PCP2-presentation $(\Sigma; S)$, Proposition 5.18 yields a finite set of prefix-rules P_U such that the prefix-rewriting system $P := P_U \cup P_S$ is noetherian, p-interreduced, and λ-confluent. Since P is in general not confluent, Proposition 6.5 does not apply. However, since P_U corresponds to a canonical base Ω of H, a finite PCP2-presentation $(\Gamma; T)$ for H can be constructed from P_U. This PCP2-presentation is even confluent, that is, we have the following result.

Proposition 6.9. [KMO94]
Given a finite PCP2-presentation of a polycyclic group G and a finite set U of generators, a finite convergent PCP2-presentation for the subgroup $\langle U\rangle$ of G can be constructed effectively.

In the remaining part of this section we review in short the results that have been obtained for various classes of finite presentations of groups that involve monadic string-rewriting systems. For these classes of presentations a different approach has been shown to be advantageous. This approach is based on automata-theoretical constructions.

¿From a finite, monadic, and confluent presentation $(\Sigma; S)$ of a group G and a finite set $U \subseteq \Sigma^+$ that is closed under inverses a deterministic finite-state acceptor A is constructed for $\Delta_S^*(U^*)$. ¿From A a finite set REP is extracted that forms a partial set of coset representatives for $\langle U\rangle$ in G. By applying the Reidemeister-Schreier rewriting process to $(\Sigma; S)$ and $\langle U\rangle$ using REP, a finite monadic presentation $(\Gamma; T)$ is obtained for $\langle U\rangle$. If the given presentation $(\Sigma; S)$ is two-monadic, then the resulting presentation $(\Gamma; T)$ can be transformed into a two-monadic confluent presentation of $\langle U\rangle$ [Kuh91].

In [KMO94] this procedure is carried over to the class of all finite monadic and λ-confluent presentations of groups that have inverses of length one. Here a monadic and λ-confluent presentation is obtained for each finitely generated subgroup. In fact, for both these cases the presentation for the subgroup is obtained in polynomial time.

7 Automatic monoids

An automatic structure for a monoid-presentation $(\Sigma; S)$ can be interpreted as a finite description of the multiplication table of the monoid M_S. We will see that under certain restrictions there exists a close correspondence between automatic structures and infinite canonical prefix-rewriting systems for $(\Sigma; S)$. In order to define these structures we need the following definition as we will be dealing with infinite sets of pairs of strings that are to be recognized by finite-state acceptors (fsa's).

Let Σ be a finite alphabet, and let $\# \notin \Sigma$ be an additional "padding" symbol. Then by $\Sigma_\#$ we denote the following finite alphabet:

$$\Sigma_\# := ((\Sigma \cup \{\#\}) \times (\Sigma \cup \{\#\})) \setminus \{(\#, \#)\}.$$

This alphabet is called the *padded extension* of Σ. A mapping $\nu : \Sigma^* \times \Sigma^* \to \Sigma_\#^*$ is now defined as follows:
if $u := a_1 a_2 \cdots a_n$ and $v := b_1 b_2 \cdots b_m$, where $a_1, \ldots, a_n, b_1, \ldots, b_m \in \Sigma$, then

$$\nu(u, v) := \begin{cases} (a_1, b_1)(a_2, b_2) \cdots (a_m, b_m)(a_{m+1}, \#) \cdots (a_n, \#), & \text{if } m < n, \\ (a_1, b_1)(a_2, b_2) \cdots (a_m, b_m), & \text{if } m = n, \\ (a_1, b_1)(a_2, b_2) \cdots (a_n, b_n)(\#, b_{n+1}) \cdots (\#, b_m) & \text{if } m > n. \end{cases}$$

A *prefix-rewriting system* P on Σ is called *synchronously regular*, *s-regular* for short, if $\nu(P)$ is accepted by some fsa over $\Sigma_\#$. Obviously, if P is s-regular, then $\mathrm{dom}(P)$ and $\mathrm{range}(P)$, and therewith also $\mathrm{RED}(P)$ and $\mathrm{IRR}(P)$, are regular languages.

An *automatic structure* for a finitely generated monoid-presentation $(\Sigma; S)$ consists of a fsa W over Σ, a fsa $M_=$ over $\Sigma_\#$, and fsa's M_a ($a \in \Sigma$) over $\Sigma_\#$ satisfying the following conditions:

(0.) $L(W) \subseteq \Sigma^*$ is a complete set of (not necessarily unique) representatives for the monoid M_S, that is, $L(W) \cap [u]_S \neq \emptyset$ holds for each $u \in \Sigma^*$,

(1.) $L(M_=) = \{\nu(u,v) \mid u,v \in L(W) \text{ and } u \leftrightarrow_S^* v\}$, and

(2.) for all $a \in \Sigma$, $L(M_a) = \{\nu(u,v) \mid u,v \in L(W) \text{ and } ua \leftrightarrow_S^* v\}$.

Actually, one may require that the set $L(W)$ is a cross-section for M_S, in which case we say that we have an *automatic structure with uniqueness* [Eps92]. In this situation the fsa $M_=$ is trivial, and hence, it will not be mentioned explicitly.

A monoid-presentation is called *automatic* if it has an automatic structure, and a monoid is called *automatic* if it has an automatic presentation. Automatic monoids have word problems that are decidable in quadratic time based on the automatic structure. For automatic groups many additional nice properties have been obtained, while for automatic monoids in general the situation is not quite as nice [CRRT97, OSKM98, Ott98a]. Here we are interested in automatic structures with uniqueness, for which the set of representatives considered is in addition prefix-closed. It is an open problem whether or not every automatic group does have an automatic structure with this additional property.

Recall that the set $\mathrm{IRR}(P)$ of strings that are irreducible with respect to a prefix-rewriting system P is prefix-closed. Finally, we say that the prefix-rewriting system P on Σ is equivalent to a string-rewriting system S on the same alphabet Σ, if the relations $\Leftrightarrow_P^*$ and $\leftrightarrow_S^*$ coincide.

The following observation is rather straightforward.

Lemma 7.1. *If there exists an s-regular canonical prefix-rewriting system P on Σ that is equivalent to the string-rewriting system S, then $C := \mathrm{IRR}(P)$ is part of an automatic structure with uniqueness for $(\Sigma; S)$.*

On the other hand, the following result can be proved by taking P to be the prefix-rewriting system $P := \{(ua, v) \mid u,v \in L(W), a \in \Sigma, ua \leftrightarrow_S^* v, \text{ but } ua \neq v\}$.

Proposition 7.2. *Let $(W, A_a(a \in A))$ be an automatic structure with uniqueness for $(\Sigma; S)$ such that the set $L(W)$ is in addition prefix-closed. Then there exists an s-regular canonical prefix-rewriting system P on Σ that is equivalent to S such that $\mathrm{IRR}(P) = L(W)$.*

Together these two facts yield the following characterization.

Corollary 7.3. *Let $(\Sigma; S)$ be a finitely generated monoid-presentation. Then the following two statements are equivalent:*

(a) There exists an automatic structure $(W, A_a(a \in \Sigma))$ with uniqueness for $(\Sigma; S)$ such that the set $L(W)$ is prefix-closed.

(b) There exists an s-regular canonical prefix-rewriting system P on Σ that is equivalent to S.

Is there a corresponding characterization for automatic structures (with uniqueness), where $L(W)$ is **not** prefix-closed?

There exists a group with a finite convergent presentation, which does not admit an automatic structure [Ger92]. Hence, no finitely generated presentation of this group has an s-regular canonical prefix-rewriting system that defines the corresponding Thue congruence.

The monoid N of [OSKM98] has an automatic structure that is based on a regular cross-section that is the set of irreducible strings modulo some infinite left-regular convergent string-rewriting system. Hence, this set is certainly prefix-closed and so Proposition 7.2 shows that this presentation of N admits an s-regular canonical prefix-rewriting system. However, N does not admit any finite convergent presentation. These observations yield the following result.

Corollary 7.4. *The class of finitely presented monoids that admit a finite convergent presentation and the class of finitely presented monoids that admit an s-regular canonical prefix-rewriting system are incomparable under set inclusion.*

8 Coset enumeration and Gröbner bases

In this section we will point out a close correspondence between the Todd-Coxeter coset enumeration method for finitely generated subgroups of finitely presented groups as presented in Section 3 and the computation of prefix Gröbner bases of finitely generated binomial right ideals in the corresponding free group ring. It is based on a recent paper by B. Reinert, K. Madlener, and T. Mora [RMM98a].

Let $\langle \Sigma; S\rangle$ be a finite group-presentation of a group G, where we assume without loss of generality that S is a special string-rewriting system, that is, $\mathrm{dom}(S)$ is the defining set of relators for the group. Let $U \subseteq \underline{\Sigma}^+$ be a finite set generating a subgroup H of G, and let F denote the free group generated by Σ, that is, $F = \langle \Sigma; \emptyset\rangle \cong (\underline{\Sigma}; S_0)$. The elements of F are represented by the set $\mathrm{IRR}(S_0)$ of freely reduced strings.

By $\mathbb{K}[F]$ we denote the *free group ring* of F, where $\mathbb{K}$ is a field. The elements of $\mathbb{K}[F]$ are the formal polynomials of the form $\sum_{i=1}^{k} \alpha_i \cdot w_i$, where $\alpha_i \in \mathbb{K} \setminus \{0\}$ and $w_i \in F$. Here $\cdot$ denotes the scalar multiplication, while $*$ will be used to denote the multiplication in the ring $\mathbb{K}[F]$. On $\underline{\Sigma}$ we fix the precedence $a_1 < a_2 < \cdots < a_n < \bar{a}_1 < \cdots < \bar{a}_n$, where $\Sigma = \{a_1, a_2, \ldots, a_n\}$, which induces the length-lexicographical ordering $\geq_{\ell\ell}$ on F. This ordering is linear and well-founded, but it is not compatible with the group structure of F. Nevertheless, this ordering can be lifted to $\mathbb{K}[F]$ and used to distinguish the largest term of a polynomial $f \in \mathbb{K}[F]$ as its *head term* $HT(f)$, this term's coefficient as its *head coefficient* $HC(f)$, and the *head monomial* $HM(f) = HC(f) \cdot HT(f)$. Further, for a subset $Q \subseteq \mathbb{K}[F]$, $HT(Q) := \{HT(f) \mid f \in Q\}$.

As each element of F is identified with its freely reduced representative, we can define the following concept of reduction on $\mathbb{K}[F]$ based on prefixes of strings: For two non-zero polynomials $p, f \in \mathbb{K}[F]$ we say that f *prefix-reduces* p *to* q *at a monomial* $\alpha \cdot w$ of p, where $\alpha \in \mathbb{K} \setminus \{0\}$ and $w \in F$, in a single step, denoted by $p \Rightarrow_f q$, if there exists a string $z \in \mathrm{IRR}(S_0)$ such that $w = HT(f)z$, and $q = p - \alpha \cdot HC(f)^{-1} \cdot f * z$. If $Q \subseteq \mathbb{K}[F]$, then $p \Rightarrow_Q q$ denotes the fact that $p \Rightarrow_f q$ holds for some $f \in Q$. In the reduction process the monomial $\alpha \cdot w$ is replaced by a sum of smaller monomials, which means that the prefix-reduction relation $\Rightarrow_Q$ on $\mathbb{K}[F]$ is noetherian.

A basis G of a right ideal i of $\mathbb{K}[F]$ is called a *prefix Gröbner basis* of i, if $HT(i) = \{uz \mid u \in HT(G), z \in F\}$. In this case every non-zero polynomial $p \in i$ is prefix-reducible by G, which implies immediately that $p \Rightarrow_G^* 0$ holds for each $p \in i$. Since it is even true that $p \Rightarrow_G^* 0$ if and only if $p \in i$, prefix Gröbner bases can be used to decide the membership problem for i by reduction. The set G is called *reduced* if no polynomial of G is prefix-reducible by any other polynomial of G, that is, the elements of $HT(G)$ are incomparable under the prefix relation. More on prefix Gröbner bases in monoid and group rings can be found in [MR93, MR98a, MR98b]. Here we only need that they are finite and computable for finitely generated right ideals in $\mathbb{K}[F]$ (see also [Ros93]).

As in the commutative case congruences on the free group F can be modelled by certain ideals of $\mathbb{K}[F]$. A subset $B \subseteq \mathbb{K}[F]$ is called a *binomial basis* of an ideal $i \subseteq \mathbb{K}[F]$ if it is a basis that consists only of polynomials of the form $u - v$, where $u, v \in F$ and $u >_{\ell\ell} v$. An ideal will be called *binomial* if it admits a binomial basis. These ideals are closely related to the word problem in groups (see [MR98a, Rei95]). Prefix Gröbner bases of finitely

generated binomial right ideals can be computed by a procedure prefix_Gröbner_basis in polynomial time when starting with an arbitrary binomial basis.

In the following we will show how prefix Gröbner bases of binomial ideals can be used to do coset enumeration in a way directly related to the Todd-Coxeter coset enumeration method. In order to describe the input $\langle \Sigma; S \rangle$ and U of the Todd-Coxeter enumeration method through binomials we choose the sets $F_S := \{s - 1 \mid s \in \mathrm{dom}(S)\}$ and $F_U := \{u - 1 \mid u \in U\}$. The initial goal is to check whether the subgroup of the free group F generated by $U \cup N(S)$ is finitely generated. This is done in an incremental fashion. Using prefix Gröbner bases we can solve the membership problem for a finitely generated subgroup of the free group F, and by adding polynomials that are obtained by multiplying the generating elements of the subgroup considered with suitably chosen group elements from the left we approximate the normal subgroup $N(S)$ of F.

Next we want to provide the theoretical foundation of these ideas.

Proposition 8.1. [MR93]
Let U be a finite subset of $\underline{\Sigma}^+$, and let $w \in \underline{\Sigma}^+$. Then w defines an element of the subgroup $\langle U \rangle$ of the free group $F = \langle \Sigma; \emptyset \rangle$ if and only if $w \Rightarrow_G^* 1$, where G is the monic prefix Gröbner basis for the right ideal of $\mathbb{K}[F]$ that is generated by the set $\{u-1 \mid u \in U\}$.

As the prefix-rewriting systems in Section 4, the monic prefix Gröbner bases are related to Nielsen reduced sets.

Proposition 8.2. [Rei95]
Let U be a finite subset of $\underline{\Sigma}^+$, and let G be the monic prefix Gröbner basis for the right ideal of $\mathbb{K}[F]$ that is generated by the set $\{u - 1 \mid u \in U\}$. Then the set $X_G := \{uv^{-1} \mid (u - v) \in G\}$ is a Nielsen reduced set of generators for the subgroup $\langle U \rangle$ of F.

However, here we are interested in the general case that the subgroup H is generated by the set $U \cup N(S)$, where the set S of defining relations is not empty. Later we will see how this possibly infinite set can be approximated in a finitary manner.

What we are aiming at is a procedure with the following specification: Given a finite group-presentation $\langle \Sigma; S \rangle$, where S is a special system, and a finite set $U \subseteq \underline{\Sigma}^+$, our procedure produces the following output:

(i) if $S = \emptyset$, that is, the group G presented by $\langle \Sigma; S \rangle$ is the free group F generated by Σ, then our procedure terminates, and it produces the monic prefix Gröbner basis G for the right ideal of $\mathbb{K}[F]$ generated by the set $\{u - 1 \mid u \in U\}$;

(ii) if $S \neq \emptyset$, then our procedure enumerates cosets of the subgroup of the free group F generated by the set $U \cup N(S)$, and if it terminates, it returns a complete set of coset representatives and the non-trivial part of the coset table encoded in the prefix Gröbner basis.

In contrast to the Todd-Coxeter enumeration method we need not require that each generator does actually occur in at least one defining relation.

Informally the procedure works as follows. The input $\langle \Sigma; S \rangle$ and U are encoded as sets of binomials $F_S := \{s - 1 \mid s \in \mathrm{dom}(S)\}$ and $F_U := \{u - 1 \mid u \in U\}$, and computations are performed in the group ring $\mathbb{K}[F]$. The following additional sets will be used:

(1.) A set $N \subseteq F$ of potential coset representatives of the subgroup $H := \langle U \cup N(S) \rangle$ in F.

(2.) A set $B \subseteq F$ that serves as a test set for possible coset representatives.

(3.) A set $D \subseteq \mathbb{K}[F]$ that is used to increment the generating set considered in order to obtain a generating set for H.

(4.) A monic, reduced prefix Gröbner basis $G \subseteq \mathbb{K}[F]$ that is used to decide whether or not the elements in B are indeed coset representatives of H.

First the procedure checks whether or not the set of defining relations S is empty. If it is, then a monic prefix Gröbner basis is computed for the right ideal of $\mathbb{K}[F]$ that is generated by F_U. Based on Proposition 8.2 this yields a Nielsen reduced set of generators for the subgroup H. If the set S is not empty, then N is initialized as the set containing the empty string only, which is the coset representative of the subgroup itself. During the computation N will always be prefix-closed. The set B is initialized as $B := \{a \mid a \in \underline{\Sigma}\}$, and then G is computed as the monic prefix Gröbner basis for the right ideal of $\mathbb{K}[F]$ that is generated by $F_S \cup F_U$. Hence, G corresponds to the subgroup of F that is generated by $\mathrm{dom}(S) \cup U$. This completes the initialization phase.

Now as long as there still are elements in the set B the following actions are performed. The smallest element is chosen from B (with respect to the length-lexicographical ordering $\geq_{\ell\ell}$). Call it τ. It is removed from B, and if τ is not prefix-reducible by G, then it is added to N and all freely reduced elements of the form τa are added to B, where $a \in \underline{\Sigma}$. Next $D := \{\tau * (s-1) \mid s \in \mathrm{dom}(S)\}$ is determined, which in TC corresponds to the process of marking the first and the last slot of each relator table with the newly found coset representative τ. Finally the monic prefix Gröbner basis of the set $G \cup D$ is computed, which corresponds to the subgroup of F that is generated by $X_G \cup \{\tau \cdot s \cdot \tau^{-1} \mid s \in \mathrm{dom}(S)\}$. Hence, we approximate the potentially infinite generating set of the subgroup $\langle U \cup N(S)\rangle$ of F. Based on the new prefix Gröbner basis some elements of N may become prefix-reducible. These have to be removed from N, as they are no longer coset representatives. This corresponds to the collaps of cosets in TC. Here is the complete description of the procedure.

Procedure 8.3. Extended TC simulation [RMM98a].

INPUT: $F_S = \{s-1 \mid s \in \mathrm{dom}(S)\}$, and $F_U = \{u-1 \mid u \in U\}$.

begin $N \leftarrow \emptyset$;
  if $S = \emptyset$ **then** $G \leftarrow$ prefix_Gröbner_basis (F_U)
  else begin $N \leftarrow \{\lambda\}$;
    $B \leftarrow \underline{\Sigma}$;
    $G \leftarrow$ prefix_Gröbner_basis $(F_S \cup F_U)$;
    while $B \neq \emptyset$ **do**
    begin $\tau \leftarrow \min_{\leq_{\ell\ell}}(B)$, $B \leftarrow B \setminus \{\tau\}$;
      if τ is not prefix-reducible by G **then**
      begin $N \leftarrow N \cup \{\tau\}$;
        $B \leftarrow B \cup \{\tau a \mid a \in \underline{\Sigma}, \tau a \in \mathrm{IRR}(S_0)\}$;
        $D \leftarrow \{\tau * (s-1) \mid s \in \mathrm{dom}(S)\}$;
        $G \leftarrow$ prefix_Gröbner_basis $(G \cup D)$;
        $M \leftarrow \{w \in N \mid w$ is prefix-reducible by $G\}$;
        $N \leftarrow N \setminus M$
      end
    end
  end
end.

The correctness of the procedure follows from the following proposition.

Proposition 8.4. [RMM98a]
Let $\langle \Sigma; S \rangle$ be a finite group-presentation, and let $U \subseteq \underline{\Sigma}^+$ be a finite set.

(a) If Procedure 8.3 terminates on input (F_S, F_U), then the subgroup of the free group F that is generated by the set $U \cup N(S)$ is finitely generated.

(b) If the subgroup of F generated by $U \cup N(S)$ has finite index in F, then Procedure 8.3 terminates on input (F_S, F_U). In this case the set N computed is a complete set of coset representatives.

The procedure has been implemented in the MRC package for computing Gröbner bases in monoid and group rings [ReZe98]. Since its description differs very much from the original table based method of Todd and Coxeter, there are new possibilities for creating new cosets. Right now new strategies involving different algorithms for the computation of the prefix Gröbner bases, different orderings on $\mathbb{K}[F]$ which have an effect on the selection of the next τ, and new data structures for representing the cosets are studied. We are aware that representing cosets by words is very space consuming, but we are looking for *knowledge* from prefix string-rewriting theory which then could be integrated into other Todd-Coxeter coset enumeration procedures.

In [RMM98a] it is further shown how this result leads to a completion-based procedure for prefix-rewriting systems that emulates the Todd-Coxeter coset enumeration. This procedure turned out to be similar to one given in [La90]. Another approach by Sims in [Sim94] to simulate Todd-Coxeter coset enumeration by a modification of the Knuth-Bendix algorithm for string-rewriting systems can also be compared to this approach, although in some cases additional efforts are necessary to make it terminating for subgroups of finite index. A thorough comparison of Todd-Coxeter enumeration methods can be found in [RMM98b].

9 Concluding remarks

As we have seen prefix-rewriting is a general method that is well suited to dealing with subgroup problems. Nielsen's process of transforming a set of generators of a subgroup of a free group into a free generating set can easily be interpreted as a special instance of prefix-completion, and in fact by prefix-completion a generalized notion of Nielsen reduced sets has been obtained (Section 4). On the other hand, as prefix-rewriting yields Gröbner bases for right ideals in the free group ring, Nielsen reduced sets are also obtained from prefix Gröbner bases of right ideals (Section 8). In Section 8 we have seen that also the Todd-Coxeter coset enumeration method can be simulated by a procedure that is based on computing prefix Gröbner bases in the free group ring. Further, prefix-rewriting methods provide unique coset representatives for finitely generated subgroups of some classes of groups even if the index of the subgroup considered is not finite (Section 5). Finally, for some classes of groups finite presentations for finitely generated subgroups can be obtained from a prefix-rewriting system for the subgroup (Section 6).

The question arises of whether these results extend to some other classes of groups. In particular for the class of automatic groups it is not yet clear how far the methods based on prefix-rewriting will lead. Recently in [HH98] the concept of an automatic group has been generalized to a group that is automatic with respect to a specified subgroup. Automatic coset systems are then used to solve the subgroup problem and to compute

subgroup presentations. The relation between prefix-rewriting and these methods has not yet been studied. Further it remains to investigate the extend to which these methods apply to the submonoid problem, that is, in how far can they be adopted to the problem of deciding whether a given element belongs to a given finitely generated submonoid of a given monoid. Observe that in [MR98a] a correspondence between the submonoid problem in monoids and the subalgebra problem in the corresponding monoid ring is described.

References

[ABS87] J.-M. Autebert, L. Boasson, and G. Senizergues. Groups and NTS languages. *J. Computer System Sciences*, 35:243–267, 1987.

[AM84] J. Avenhaus and K. Madlener. The Nielsen reduction and p-complete problems in free groups. *Theoretical Computer Science*, 32:61–76, 1984.

[AMO86] J. Avenhaus, K. Madlener, and F. Otto. Groups presented by finite two-monadic Church-Rosser Thue systems. *Transactions American Mathematical Society*, 297:427–443, 1986.

[Bau81] G. Bauer. *Zur Darstellung von Monoiden durch konfluente Regelsysteme.* Doctoral diss., Fachbereich Informatik, Universität Kaiserslautern, 1981.

[BBN59] G. Baumslag, W.W. Boone, and B.H. Neumann. Some unsolvable problems about elements and subgroups of groups. *Math. Scand.*, 7:191–201, 1959.

[BCM77] G. Baumslag, F.B. Cannonito, and C.F. Miller III. Infinitely generated subgroups of finitely presented groups. *Mathematische Zeitschrift*, 153:117–134, 1977.

[BKR87] B. Benninghofen, S. Kemmerich, and M.M. Richter. *Systems of Reductions.* Lecture Notes in Computer Science 277. Springer-Verlag, Berlin, 1987.

[BO93] R.V. Book and F. Otto. *String-Rewriting Systems.* Springer-Verlag, New York, 1993.

[Büc79] H. Bücken. Reduction-systems and small cancellation theory. In *Proceedings 4th Workshop on Automated Deduction*, pages 53–59, 1979.

[CO94] R. Cremanns and F. Otto. Constructing canonical presentations for subgroups of context-free groups in polynomial time. In J. von zur Gathen and M. Giesbrecht, editors, *Proceedings ISSAC'94*, pages 147–153. ACM, New York, 1994.

[Coc76] Y. Cochet. Church-Rosser congruences on free semigroups. *Colloquia Mathematica Societatis János Bolyai*, 20:51–60, 1976.

[Cre95] R. Cremanns. *Finiteness conditions for rewriting systems.* Doctoral diss., Fachbereich Mathematik/Informatik, Universität Kassel, 1995.

[CRRT97] C.M. Campbell, E.F. Robertson, N. Ruškuc, and R.M. Thomas. *Automatic semigroups.* Technical Report No. 1997/29, Dep. of Mathematics and Computer Science, University of Leicester, 1997.

[Deh11] M. Dehn. Über unendliche diskontinuierliche Gruppen. *Math. Ann.*, 71:116–144, 1911.

[Deh12] M. Dehn. Transformation der Kurven auf zweiseitigen Flächen. *Math. Ann.*, 72:413–421, 1912.

[Eps92] D.B.A. Epstein. *Word Processing In Groups.* Jones and Bartlett Publishers, Boston, 1992.

[Ger92] S.M. Gersten. Dehn functions and l1-norms of finite presentations. In G. Baumslag and C.F. Miller III, editors, *Algorithms and Classification in Combinatorial Group Theory*, Math. Sciences Research Institute Publ. 23, pages 195–224. Springer-Verlag, New York, 1992.

[HH98] D.F. Holt and D.F. Hurt. Computing automatic coset systems and subgroup presentations. *J. Symbolic Computation*, 25:1–19, 1998.

[HK91] T. Harju and J. Karhumäki. The equivalence problem of multitape finite automata. *Theoretical Computer Science*, 78:347–355, 1991.

[Joh76] D.L. Johnson. *Presentation of Groups*, volume 22 of *London Mathematical Society Lecture Notes Series*. Cambridge University Press, Cambridge, 1976.

[KB70] 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, New York, 1970.

[KM89] N. Kuhn and K. Madlener. A method for enumerating cosets of a group presented by a canonical system. In *Proc. ISSAC'89*, pages 338–350. ACM Press, New York, 1989.

[KMO90] N. Kuhn, K. Madlener, and F. Otto. A test for λ-confluence for certain prefix rewriting systems with applications to the generalized word problem. In S. Watanabe and M. Nagata, editors, *Proceedings ISSAC'90*, pages 8–15. ACM, New York, 1990.

[KMO94] 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.

[KN85] D. Kapur and P. Narendran. The Knuth-Bendix completion procedure and Thue systems. *SIAM J. Computing*, 14:1052–1072, 1985.

[KRW90] A. Kandri-Rody and V. Weispfennig. Non-commutative Gröbner bases in algebras of solvable type. *J. Symbolic Computation*, 9:1–26, 1990.

[Kuh91] N. Kuhn. *Zur Entscheidbarkeit des Untergruppenproblems für Gruppen mit kanonischen Darstellungen.* Doctoral diss., Fachbereich Informatik, Universität Kaiserslautern, 1991.

[La90] G. Labonté. An algorithm for the construction of matrix representations for finitely presented non-comutative algebras. *J. Symbolic Computation*, 9:27–38, 1990.

[LeC86] P. LeChenadec. *Canonical Forms in Finitely Presented Algebras.* Research Notes in Theoretical Computer Science. Pitman, London, 1986.

[LS77] R.C. Lyndon and P.E. Schupp. *Combinatorial Group Theory.* Springer-Verlag, Berlin, 1977.

[Mik58] K.A. Mikhailova. The occurrence problem for direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958.

[Mil71] C.F. Miller. *On group-theoretic decision problems and their classification*, volume 68 of *Annals of Mathematical Studies.* Princeton University Press, Princeton, 1971.

[MKS76] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial Group Theory.* Second revised edition. Dover, New York, 1976.

[MO87] K. Madlener and F. Otto. Using string-rewriting for solving the word problem for finitely presented groups. *Information Processing Letters*, 24:281–284, 1987.

[MO89] K. Madlener and F. Otto. About the descriptive power of certain classes of finite string-rewriting systems. *Theoretical Computer Science*, 67:143–172, 1989.

[MO91] K. Madlener and F. Otto. Decidable sentences for context-free groups. In C. Choffrut and M. Jantzen, editors, *Proceedings STACS'91*, Lecture Notes in Computer Science 480, pages 160–171. Springer-Verlag, Berlin, 1991.

[MR93] K. Madlener and B. Reinert. Computing Gröbner bases in monoid and group rings. In M. Bronstein, editor, *Proc. ISSAC'93*, pages 254–263. ACM, New York, 1993.

[MR98a] K. Madlener and B. Reinert. Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings. *Theoretical Computer Science*, 208:3–31, 1998.

[MR98b] 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.

[MR98c] K. Madlener and B. Reinert. A generalization of Gröbner basis algorithms to polycyclic group rings. *J. Symbolic Computation*, 25:23–45, 1998.

[MS83] D.E. Muller and P.E. Schupp. Groups, the theory of ends, and context-free languages. *J. Computer System Sciences*, 26:295–310, 1983.

[OK97] F. Otto and Y. Kobayashi. Properties of monoids that are presented by finite convergent string-rewriting systems - a survey. In D.Z. Du and K. Ko, editors, *Advances in Algorithms, Languages and Complexity*, pages 226–266. Kluwer Academic Publ., Dordrecht, 1997.

[OSKM98] F. Otto, A. Sattler-Klein, and K. Madlener. Automatic monoids versus monoids with finite convergent presentations. In T. Nipkow, editor, *Rewriting Techniques and Applications, Proceedings RTA'98*, Lecture Notes in Computer Science 1379, pages 32–46. Springer-Verlag, Berlin, 1998.

[Ott86] F. Otto. On deciding whether a monoid is a free monoid or is a group. *Acta Informatica*, 23:99–110, 1986.

[Ott98a] F. Otto. *On Dehn functions of finitely presented bi-automatic monoids.* Mathematische Schriften Kassel 8/98, Universität Kassel, July 1998.

[Ott98b] F. Otto. *On s-regular prefix-rewriting systems and automatic structures.* Mathematische Schriften Kassel 9/98, Universität Kassel, September 1998.

[Rei95] B. Reinert. *On Gröbner Bases in Monoid and Group Rings.* Doctoral diss., Fachbereich Informatik, Universität Kaiserslautern, 1995.

[RMM98a] B. Reinert, K. Madlener, and T. Mora. A note on Nielsen reduction and coset enumeration. In *Proceedings ISSAC'98*, pages 171–178. ACM, New York, 1998.

[RMM98b] B. Reinert, K. Madlener, and T. Mora. *Coset enumeration - a comparison of methods.* Technical report, Universität Kaiserslautern, 1998.

[ReZe98] B. Reinert and D. Zeckzer. MRC: A System for Computing Gröbner Bases in Monoid and Group Rings, In *6th Rhine Workshop on Computer Algebra*, Sankt Augustin, 1998.

[Ros93] A. Rosenmann. An algorithm for constructing Gröbner and free Schreier bases in free group algebras. *J. Symbolic Computation*, 16:523–549, 1993.

[Sim94] C.C. Sims. *Computation With Finitely Presented Groups*, volume 48 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, New York, 1994.

[Sny89] W. Snyder. Efficient ground completion: an $O(n \log n)$ algorithm for generating reduced sets of ground rewrite rules equivalent to a set of ground equations E. In N. Deshowitz, editor, *Rewriting Techniques and Applications, Proceedings RTA'89*, Lecture Notes in Computer Science 355, pages 419–433. Springer-Verlag, Berlin, 1989.

[SOK94] C.C. Squier, F. Otto, and Y. Kobayashi. A finiteness condition for rewriting systems. *Theoretical Computer Science*, 131:271–294, 1994.

[TC36] J.A. Todd and H.S.M. Coxeter. A practical method for enumerating cosets of a finite abstract group. *Proc. Edinburgh Math. Soc.*, 5:26–34, 1936.

[Wiß89] D. Wißmann. *Anwendung von Rewrite-Techniken in polyzyklischen Gruppen.* Doctoral diss., Fachbereich Informatik, Universität Kaiserslautern, 1989.

List of papers published in the Reports on Computer Algebra series

[RCA:22] K. Madlener and O. Friedrich. Some Applications Of Prefix-Rewriting In Monoids, Groups, And Rings. Nov 1998.

[RCA:21] G.-M. Greuel, G. Pfister, and H. Schönemann. Singular version 1.2 user manual. June 1998.

[RCA:20] B. Reinert and D. Zeckzer. MRC – A System for Computing Gröbner Bases in Monoid and Group Rings. July 1998.

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

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

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

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

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

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

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

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

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

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

[RCA:09] B. Reinert. Introducing reduction to polycyclic group rings – a comparison of methods. October 1996.

[RCA:08] T. Siebert. On strategies and implementations for computations of free resolutions. September 1996.

[RCA:07] G.M. Greuel. Description of SINGULAR: A computer algebra system for singularity theory, algebraic geometry, and commutative algebra. 1996.

[RCA:06] G.M. Greuel and G. Pfister. Advances and improvements in the theory of standard bases and szyzygies. 1996.

[RCA:05] O. Bachmann, S. Gray, and H. Schönemann. MPP: A Framework for Distributed Polynomial Computations. 1996.

[RCA:04] O. Bachmann and H. Schönemann. A Manual for the MPP Dictionary and MPP Library. 1996.

[RCA:03] R. Stobbe. FACTORY: a C++ class library for multivariate polynomial arithmetic. 1996.

[RCA:02] H. Schönemann. Algorithms in singular. June 1996.

[RCA:01] 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. July 1996.