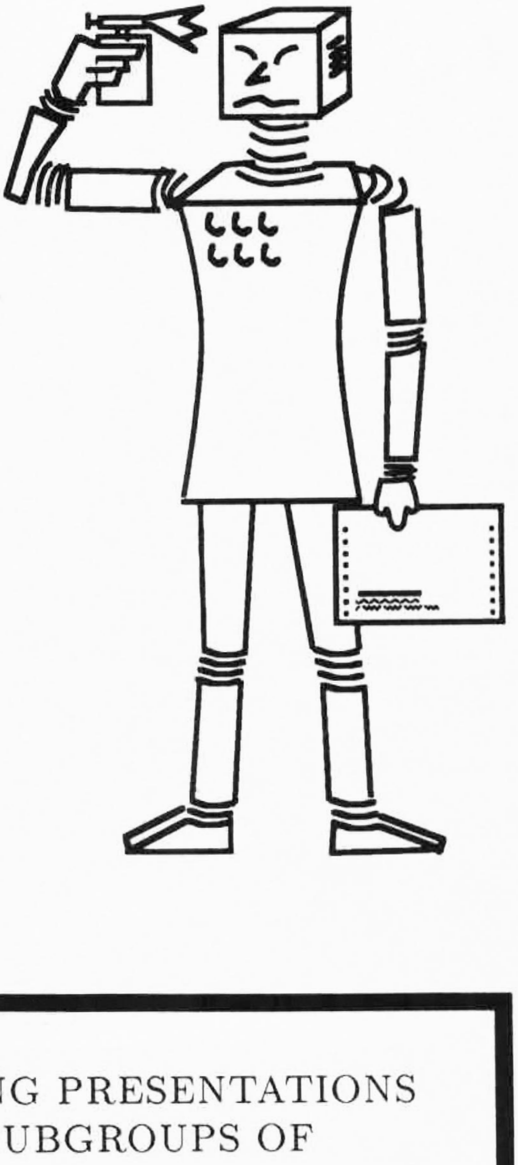
Fachbereich Informatik
Universität Kaiserslautern
Postfach 3049
D-6750 Kaiserslautern

SEKI - REPORT



COMPUTING PRESENTATIONS FOR SUBGROUPS OF POLYCYCLIC GROUPS AND OF CONTEXT-FREE GROUPS

Norbert Kuhn, Klaus Madlener and Friedrich Otto

SEKI Report SR-92-07

COMPUTING PRESENTATIONS FOR SUBGROUPS OF POLYCYCLIC GROUPS AND OF CONTEXT-FREE GROUPS

Nòrbert Kuhn
DFKI, 6600 Saarbrücken

Klaus Madlener
Fachbereich Informatik, Universität Kaiserslautern
6750 Kaiserslautern

Friedrich Otto*
Fachbereich Mathematik/Informatik, Gesamthochschule Kassel
3500 Kassel

February 25, 1992

Abstract

Finitely generated context-free groups can be presented by finite, monadic, and λ-confluent string-rewriting systems. Due to their nice algorithmic properties these systems provide a way to effectively solve many decision problems for context-free groups. Since finitely generated subgroups of context-free groups are again context-free, they can be presented in the same way. Here we describe a process that, from a finite, monadic, and λ-confluent string-rewriting system presenting a context-free group G and a finite subset U of G, determines a presentation of this form for the subgroup $\langle U\rangle$ of G that is generated by U. For finitely presented polycyclic groups we obtain an analogous result, when we use finite confluent PCP2-presentations to describe these groups.

[*] This work was performed while this author was visiting at the Fachbereich Informatik, Universität Kaiserslautern.

1 Introduction

The systematic study of decision problems for finitely presented groups like the word problem, the conjugacy problem, and the generalized word problem has by now a long tradition. While all these problems are undecidable in general, they have been solved successfully for many restricted instances [12].

Each finitely presented group G has infinitely many finite presentations of the form $\langle \Sigma; R \rangle$. Here Σ is a finite alphabet (set of generators), $^- : \Sigma \rightarrow \Sigma$ is a bijection that is involutory, and R is a finite string-rewriting system (set of defining relations) containing the trivial relations $\{a\bar{a} \rightarrow \lambda, \bar{a}a \rightarrow \lambda \mid a \in \Sigma\}$, where λ denotes the empty word. If Pr is a decision problem, e.g. the word problem, then we say that Pr is decidable for a group G if, for some finite presentation $\langle \Sigma; R \rangle$ of G, there exists an algorithm that solves Pr for this presentation. For many decision problems such an algorithm can in theory be carried over to each other finite presentation $\langle \Gamma; S \rangle$ of G based on an isomorphism between the two presentations; unfortunately, such an isomorphism can in general not be constructed effectively. In fact, given two finite presentations it is undecidable in general whether they define the same group. Therefore, one is often particularly interested in certain uniform versions of these decision problems.

Let C be a class of finite presentations $\langle \Sigma; R \rangle$ that satisfy some syntactic restriction. The **uniform word problem** for C is then the following decision problem:

INSTANCE: A finite presentation $\langle \Sigma; R \rangle$ from C, and two words $u, v \in \Sigma^*$.
QUESTION: Do u and v present the same element of the group defined by $\langle \Sigma; R \rangle$?

Analogously, the uniform versions of the other decision problems are defined. For example, the word problem is decidable for the class of presentations that involve a single non-trivial relation (i.e., the so-called one-relator groups [12]), and it is decidable for the class of finite presentations that involve a noetherian and confluent string-rewriting system. However, for the latter the generalized word problem is still undecidable [18]. Finally, for the class of finite presentations $\langle \Sigma; R \rangle$ with R monadic and confluent, the generalized word problem is decidable [5]. In fact, given a finite presentation $\langle \Sigma; R \rangle$ of this form and a finite set $U \subset \Sigma^*$, a prefix-rewriting system $P := P_U \cup P_R$ can be constructed effectively such that the prefix-rewriting relation $\Longrightarrow_P$ defined by P is confluent, and the right congruence $\Longleftrightarrow_P^*$ induced by $\Longrightarrow_P$ coincides with the relation $\sim_U$, which is defined as follows: $x \sim_U y$ iff $xy^{-1} \in \langle U \rangle$ [10]. Here $\langle U \rangle$ denotes the subgroup of the group presented by $\langle \Sigma; R \rangle$ that is generated by U. Thus, w belongs to this subgroup if and only if $w \Longrightarrow_P^* \lambda$, i.e., the generalized word problem can be solved by prefix-rewriting. Actually, since $\Longrightarrow_P$ is confluent, the irreducible words mod $\Longrightarrow_P$ form a set of coset representatives for the subgroup $\langle U \rangle$, and given a word w, prefix-rewriting will reduce w to the representative of its coset. Finally, it should be mentioned that a group G has a presentation $\langle \Sigma; R \rangle$ involving a finite, monadic, and confluent string-rewriting system R if and only if G is a "plain" group, i.e., G is isomorphic to the free product of a free group of finite rank and finitely many finite groups [2].

In this paper we are mainly interested in the class of finitely presented polycyclic groups and the class of context-free groups, which properly contains the plain groups. It is known that a finitely presented group is polycyclic if and only if it can be presented through a finite confluent PCP2-presentation [22]. A group G given through a finite presentation $\langle \Sigma; R \rangle$ is called **context-free** if the congruence class $[\lambda]_R$ is a context-free language. It is known that a group is context-free if and only if it is a finitely generated virtually free group [19], i.e., it contains a free subgroup of finite index. On the other hand, a group is context-free if and only if it has a presentation of the form $\langle\Sigma; R\rangle$ such that R is finite, monadic, and λ-confluent [1]. For these presentations many decision problems, among them the word problem and the generalized word problem, can be solved efficiently [16]. Therefore, they are particularly useful when dealing with decision problems for context-free groups. Accordingly, a specialized completion procedure has been proposed that, given a finite monadic presentation $\langle\Sigma; R\rangle$ as input, tries to transform this presentation into a finite presentation $\langle\Sigma; S\rangle$ such that S is monadic and λ-confluent [13]. Unfortunately, even if the group presented by $\langle\Sigma; R\rangle$ is context-free, this procedure may not succeed.

Here we are concerned with finitely generated subgroups of polycyclic groups and context-free groups. Our work is motivated by the observation that many algebraically defined classes of groups are closed under the operation of taking finitely generated subgroups. For example, each subgroup of a free group is free, and each subgroup of an abelian group is abelian. Now this also holds for the class of polycyclic groups and the class of context-free groups. Since the polycyclic groups, respectively the context-free groups, are presented through the finite confluent PCP2-presentations, respectively through the finite, monadic, and λ-confluent presentations, this observation leads to the following task:

INSTANCE: A finite confluent PCP2-presentation $\langle\Sigma; R\rangle$, respectively a finite, monadic, and λ-confluent presentation $\langle\Sigma; R\rangle$, and a finite subset $U \subset \Sigma^*$.

TASK: Determine a finite presentation $\langle\Gamma; T\rangle$ of the same type as $\langle\Sigma; R\rangle$ for the subgroup $\langle U\rangle$!

Reidemeister and Schreier have dealt with this task in a general setting [17]. Let $\langle\Sigma; R\rangle$ be a finite presentation, and let $U \subset \Sigma^*$ be a finite set. Based on a set of minimal representatives for all the cosets of $\langle U\rangle$ the process described by Reidemeister and Schreier yields a presentation for $\langle U\rangle$. Unfortunately, this presentation is finite in general only in case $\langle U\rangle$ has finite index in the group G presented by $\langle\Sigma; R\rangle$. In fact, there are finitely presented groups with finitely generated subgroups that are not finitely presented [12]. Also for each coset a unique representative is required, and there must be an effective process that, given a word $w \in \Sigma^*$ as input, determines the representative of the coset containing w. Here we will solve the above task without the aid of these restrictions.

In Section 3 we restate some results of [3,22] in short on how to associate a prefix-rewriting system $P = P(\Omega) \cup P_R$ with each finitely generated subgroup H of a finitely presented polycyclic group such that the prefix-rewriting relation $\Longrightarrow_P$ is λ-confluent, i.e., $w \in H$ if and only if $w \Longrightarrow_P^* \lambda$. Exploiting these results we then effectively construct a finite confluent PCP2-presentation for the subgroup H. In Section 4 we describe a construction that, given a presentation $\langle\Sigma; R\rangle$ involving a finite, monadic, and λ-confluent string-rewriting system R and a finite set $U \subset \Sigma^*$, results in a prefix-rewriting system $P = P_U \cup P_R$ such that $\Longleftrightarrow_P^* = \sim_U$, and such that the prefix-rewriting relation $\Longrightarrow_P$ is λ-confluent. This gives an alternate way for solving the generalized word problem in this setting. This construction is analogous to a construction presented in [9] for the class of finite presentations that involve length-reducing and confluent string-rewriting systems. However, since finite, length-reducing, and confluent presentations only present a proper subclass of the context-free groups [15], the situation considered here is more general. In addition, we present a rewrite process $\sigma : \langle U\rangle \longrightarrow U^*$ that transforms each word $w \in \langle U\rangle$ into an equivalent word $\sigma(w)$ in the given generators U.

Then, based on some ideas that Gilman describes for the class of groups presented by finite, monadic, and confluent string-rewriting systems [8], we adopt the Reidemeister-Schreier process to the class of finite, monadic, and λ-confluent presentations of context-free groups. We present a construction that consists of three major steps. First, from $\langle\Sigma; R\rangle$ and U we construct a deterministic finite-state acceptor (dfsa) A such that $\Delta_R^*(U^*) \subseteq L(\mathbf{A}) \subseteq \langle U\rangle$, where $\Delta_R^*(U^*)$ denotes the set of descendants of products from U^* mod R, and $L(\mathbf{A})$ denotes the language accepted by A. From A we extract a finite set REP that forms a partial and ambiguous set of coset representatives for $\langle U\rangle$. Applying the process of Reidemeister and Schreier to $\langle\Sigma; R\rangle$ and U using the set REP of coset representatives then yields a finite monadic presentation $\langle\Gamma; S\rangle$ for the subgroup $\langle U\rangle$. In general, the string-rewriting system S is not λ-confluent; however, by normalizing this system [14] we obtain an equivalent finite system T that is monadic and λ-confluent. Thus, $\langle\Gamma; T\rangle$ is the intended presentation of $\langle U\rangle$. A nice aspect of this construction is the fact that the presentation $\langle\Gamma; T\rangle$ is obtained from $\langle\Sigma; R\rangle$ and U in polynomial time. Along with $\langle\Gamma; T\rangle$ a mapping $\tau : \langle U\rangle \longrightarrow \Gamma^*$ is constructed that rewrites each word $w \in \langle U\rangle$ as a word in the new generators such that w and $\tau(w)$ describe the same element of the group $\langle U\rangle$. This construction is presented in Section 5.

Finally, in the concluding section we discuss related results from Kuhn's doctoral dissertation [9] about the task of constructing presentations of finitely generated subgroups for other restricted classes of presentations.

2 Definitions and notation

Here we restate in short the definitions and results on string-rewriting systems, prefix-rewriting and context-free groups that this paper is based upon.

Let Σ be a finite alphabet. Then Σ^* denotes the set of words over Σ including the empty word λ. The length of a word w is written as $\mid w \mid$, and the concatenation of two words u and v is simply written as uv.

A **string-rewriting system** R on Σ is a subset of $\Sigma^* \times \Sigma^*$. Its elements are refered to as (**rewrite**) **rules**, and they are often written in the form $(l \rightarrow r)$. By $dom(R)$, respectively $range(R)$, we denote the set of words that occur as the left-hand side, respectively the right-hand side, of a rule of R. The system R is called **length-reducing**, if $\mid l \mid > \mid r \mid$ holds for each rule $(l \rightarrow r) \in R$, and it is called **monadic** if $range(R) \subseteq \Sigma \cup \{\lambda\}$ and $l > r$ holds for each rule $(l \rightarrow r) \in R$, where $>$ denotes the length-lexicographical ordering induced by a fixed linear ordering on Σ.

The **single-step reduction relation** $\longrightarrow_R$ is the following relation on Σ^*:

$$u \longrightarrow_R v \text{ if and only if } \exists x, y \in \Sigma^* \exists (l \rightarrow r) \in R : u = xly \text{ and } v = xry.$$

Its reflexive transitive closure $\longrightarrow_R^*$ is the **reduction relation** induced by R, and its reflexive, symmetric, and transitive closure $\longleftrightarrow_R^*$ is the **Thue congruence** generated by R. For $w \in \Sigma^*$, $[w]_R$ denotes the **congruence class** $\{u \in \Sigma^* \mid u \longleftrightarrow_R^* w\}$. The factor monoid $\Sigma^* / \longleftrightarrow_R^*$ is denoted by M_R, and whenever a monoid M is isomorphic to M_R, the ordered pair $(\Sigma; R)$ is called a (**monoid-**) **presentation** of M with **generators** Σ and **defining relations** R.

If the monoid M_R presented by $(\Sigma; R)$ is a group, then one can determine a set of words $\{u_a \mid a \in \Sigma\}$ effectively such that, for each $a \in \Sigma$, $au_a \longleftrightarrow_R^* \lambda \longleftrightarrow_R^* u_a a$ holds [20]. This gives a function $^{-1} : \Sigma^* \rightarrow \Sigma^*$ such that w^{-1} is a **formal inverse** of w, i.e., $ww^{-1} \longleftrightarrow_R^* \lambda \longleftrightarrow_R^* w^{-1}w$ holds for each word w. However, in combinatorial group theory groups are usually presented through group-presentations rather than through monoid-presentations.

Let Σ be a finite alphabet, and let $^- : \Sigma \rightarrow \Sigma$ be a bijection such that $\bar{\bar{a}} = a$ for all $a \in \Sigma$. We define a function $^{-1} : \Sigma^* \rightarrow \Sigma^*$ through $\lambda^{-1} := \lambda, (wa)^{-1} := \bar{a}w^{-1}$ $(w \in \Sigma^*, a \in \Sigma)$.

Further, let R be a string-rewriting system on Σ that includes the "trivial rules" $\{a\bar{a} \rightarrow \lambda \mid a \in \Sigma\}$. Then, for each letter $a \in \Sigma$, $\bar{a} \in \Sigma$ is a "formal inverse" of length one for a, and so the monoid M_R presented by $(\Sigma; R)$ is a group. Accordingly, the ordered pair $\langle\Sigma; R\rangle$ is called a **group-presentation.**

Since group-presentations are a special class of monoid-presentations, we state the following definitions only in terms of the latter. In the following, whenever we restrict our attention to group-presentations, we will explicitly say so.

Let G be a group given through the presention $(\Sigma; R)$, and let U be a finite subset of Σ^*. By $\langle U\rangle$ we denote the **subgroup** of G that is **generated by** U. A word $w \in \Sigma^*$ belongs to $\langle U\rangle$ if there exist $u_1, \ldots, u_n \in U$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$ such that $w \longleftrightarrow_R^* u_1^{\varepsilon_1} \cdots u_n^{\varepsilon_n}$. The **generalized word problem** for G can then be stated as follows:

INSTANCE: A finite subset $U \subset \Sigma^*$, and a word $w \in \Sigma^*$.
QUESTION: Does w belong to the subgroup $\langle U\rangle$ of G ?

To simplify the notation we will usually assume that the finite set U is **closed under taking inverses**, i.e., for each $u \in U$, there exists a word $v \in U$ such that $v \longleftrightarrow_R^* u^{-1}$. We consider the following binary relation $\sim_U$ on Σ^* :

$$x \sim_U y \text{ if and only if } \exists u \in \langle U\rangle : x \longleftrightarrow_R^* uy.$$

This relation is a right-congruence on Σ^*, and for $w \in \Sigma^*$, $[w]_U$ denotes the equivalence class of w mod $\sim_U$. Obviously, $[\lambda]_U = \langle U\rangle$, i.e., $w \in \langle U\rangle$ if and only if $w \sim_U \lambda$.

We can express this relation in a different way. To this end we associate a prefix-rewriting system $P := P_U \cup P_R$ with $(\Sigma; R)$ and U. Let

$$P_U := \{(u, v) \mid \exists w \in U : uv^{-1} \longleftrightarrow_R^* w\}$$

be a finite set such that, for each $w \in U$, P_U contains at least one pair (u, v) satisfying $uv^{-1} \longleftrightarrow_R^* w$, and let

$$P_R := \{(xl, xr) \mid x \in \Sigma^* \text{ and } (l \rightarrow r) \in R\}.$$

Then the **single-step prefix-reduction relation** $\Longrightarrow_P$ on Σ^* is defined as follows:

$$u \Longrightarrow_P v \text{ if and only if } \exists (x, y) \in P \exists z \in \Sigma^* : u = xz \text{ and } v = yz.$$

The reflexive transitive closure $\Longrightarrow_P^*$ of $\Longrightarrow_P$ is the **prefix-reduction relation** induced by P, and the reflexive, symmetric, and transitive closure $\Longleftrightarrow_P^*$ is the right-congruence induced by P.

Lemma 2.1 [10]. *For every finite set $U \subset \Sigma^*$ and every set of prefix-rules $P := P_U \cup P_R$ associated with $(\Sigma; R)$ and U, the right-congruences $\sim_U$ and $\Longleftrightarrow_P^*$ coincide.*

A string-rewriting system R is called

- **noetherian** if there is no infinite sequence of the form $u_0 \longrightarrow_R u_1 \longrightarrow_R \ldots$;
- **confluent** if, for all $u, v, w \in \Sigma^*$, $u \longrightarrow_R^* v$ and $u \longrightarrow_R^* w$ imply that $v \longrightarrow_R^* z$ and $w \longrightarrow_R^* z$ for some $z \in \Sigma^*$;
- **λ-confluent** if, for all $u \in \Sigma^*$, $u \longleftrightarrow_R^* \lambda$ implies that $u \longrightarrow_R^* \lambda$.

These notions immediately carry over to prefix-rewriting systems. If the prefix-rewriting system $P = P_U \cup P_R$ is noetherian and (λ-) confluent, then a word w belongs to the subgroup $\langle U \rangle$ if and only if λ is the only irreducible descendant of w mod $\Longrightarrow_P$.

For a string-rewriting system R on Σ, $IRR(R)$ is the **set of irreducible words**. If R is finite, then $IRR(R)$ is a regular set. For $u \in \Sigma^*$, $\Delta_R^*(u)$ is the **set of descendants** of u, i.e., $\Delta_R^*(u) = \{v \mid u \longrightarrow_R^* v\}$, and for $L \subseteq \Sigma^*$, $\Delta_R^*(L) = \bigcup_{u \in L} \Delta_R^*(u)$. For a prefix-rewriting system P, $IRR(\Longrightarrow_P)$ is the set of irreducible words mod $\Longrightarrow_P$. Again, in the situation considered here this set is regular.

Next we turn to the context-free groups. Let R be a finite string-rewriting system on Σ such that the monoid M_R is a group. This group is called **context-free** if the congruence class $[\lambda]_R \subset \Sigma^*$ is a context-free language. An algebraic characterization for the class of context-free groups has been given by Muller and Schupp.

Proposition 2.2 [19].
A finitely generated group is context-free if and only if it is virtually free.

A group G is **virtually free** if it contains a free subgroup of finite index. Autebert, Boasson, and Senizergues have obtained the following important result on presentations of context-free groups.

Proposition 2.3 [1]. *A group G has a presentation of the form $(\Sigma; R)$, where R is a finite monadic string-rewriting system on Σ that is λ-confluent if and only if G is a finitely generated context-free group.*

While in general a finite, monadic, and λ-confluent string-rewriting system has an undecidable word problem [21], for those systems of this form that present groups many decision problems can be solved efficiently [16]. Underlying these decidability results is the following fundamental technical result.

Proposition 2.4 [16]. *Let R be a finite monadic string-rewriting system on Σ such that R is λ-confluent, and the monoid M_R is a group. Then, for each regular set $L \subseteq \Sigma^*$, the set $I_R(L) = [L]_R \cap IRR(R)$ of irreducible words that are congruent to some element of L is regular. In addition, from R and a nondeterministic finite-state acceptor (nfsa) for the set L, an nfsa for $I_R(L)$ can be constructed in polynomial time.*

As a consequence it is shown in [16] that Book's technique of linear sentences [5] applies to context-free groups. Since this technique can be used to solve the generalized word problem, we have the following result.

Corollary 2.5 [16]. *For context-free groups given through finite monadic string-rewriting systems that are λ-confluent, the generalized word problem is uniformly solvable in polynomial time.*

Finally, we consider the polycyclic groups. A group G is called **polycyclic** if there exist a finite sequence of normal subgroups

$$G = G_1 \rhd G_2 \rhd \ldots \rhd G_m \rhd G_{m+1} = \{1\}$$

and elements $g_1, g_2, \ldots, g_m \in G$ such that, for all $i = 1, \ldots, m$,

$$G_i = \langle \{g_i\} \cup G_{i+1} \rangle,$$

i.e., G_i is the subgroup of G that is generated by the subgroup G_{i+1} and the element g_i.

Wißmann [22] has shown that finitely presented polycyclic groups can be presented by finite, noetherian, and confluent string-rewriting systems of a very special form.

Let $\Sigma = \{a_1, \overline{a}_1, \ldots, a_n, \overline{a}_n\}$, let $\Sigma_i = \{a_i, \overline{a}_i, \ldots, a_n, \overline{a}_n\}$ for $i = 1, 2, \ldots, n$, and let $\Sigma_{n+1} = \emptyset$. We define several particular classes of rules over Σ. A rule $(l \rightarrow r)$ is called

- a **CP2-rule** if $l = a_j^\delta a_i^\varepsilon$ 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 $l = a_i^k$ and $r \in \Sigma_{i+1}^*$ for some $i \in \{1, \ldots, n\}$ and $k > 0$,
- a **negative P-rule** if $l = \overline{a}_i$ 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 over Σ 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 $\overline{a}_i$, or S contains no rule with left-hand side from $\{a_i, \overline{a}_i\}^*$,
- 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 $a_j^\delta a_i^\varepsilon$.

Now a presentation $\langle \Sigma; R \rangle$ is called a **PCP2-presentation** if $R = R_0 \cup P \cup C$, where R_0 is the set of trivial rules $R_0 = \{a_i \overline{a}_i \rightarrow \lambda, \overline{a}_i a_i \rightarrow \lambda \mid i = 1, \ldots, n\}$, P is a P-system, and C is a CP2-system.

Using a particular ordering Wißmann shows that, if $\langle \Sigma; R \rangle$ is a PCP2-presentation, then the string-rewriting system R is noetherian. Further, a finitely presented group G can be presented through a PCP2-presentation if and only if G is a polycyclic group [22]. In fact, Wißmann proves the following result using a specialized form of the Knuth-Bendix completion procedure.

Proposition 2.6 [22]. *Given a finite PCP2-presentation $\langle \Sigma; S \rangle$ of a polycyclic group G, another finite PCP2-presentation $\langle \Sigma; R \rangle$ can be constructed effectively such that R and S are equivalent, and R is confluent.*

Here two string-rewriting systems on the same alphabet are called **equivalent** if they generate the same Thue congruence. We close this section with a characterization of the set of irreducible strings with respect to a PCP2-presentation.

Let $\langle \Sigma; R \rangle$ be a PCP2-presentation. We define certain sets $ORD(\Sigma_i)$ of **ordered strings**, $i = 1, \ldots, n+1$, recursively as follows:

$$\begin{array}{lcl} ORD(\Sigma_{n+1}) & := & \{\lambda\}, \text{ and} \\ ORD(\Sigma_i) & := & \{x \in \Sigma_i^* \mid x = uv \text{ for some } u \in \{a_i\}^* \cup \{\overline{a}_i\}^* \text{ and } v \in ORD(\Sigma_{i+1})\}. \end{array}$$

Next we define some **constants** $\varepsilon_R(i), i \in \{1, \ldots, n\}$:

$$\varepsilon_R(i) := \begin{cases} \infty & \text{if R contains no P-rule} (\ell, r) \text{ with } \ell \in \{a_i\}^*, \\ k & \text{if R contains a positive P-rule} (a_i^k, r) \text{ for some (unique) } k > 0. \end{cases}$$

Obviously, the strings in $ORD(\Sigma) := ORD(\Sigma_1)$ are irreducible with respect to the trivial rules R_0 as well as with respect to the CP2-rules in R, while each string a_i^k is irreducible with respect to the P-rules in R, if $\varepsilon_R(i) = \infty$ or if $\varepsilon_R(i) < \infty$ and $0 \leq k < \varepsilon_R(i)$. This shows that the set IRR(R) of irreducible strings with respect to R can be described as follows:

$$\begin{aligned} IRR(R) &= \{x \in ORD(\Sigma) \mid \forall i \in \{1,\ldots,n\} : \text{if}\, \varepsilon_R(i) < \infty, \text{then}\, 0 \leq |x|_{a_i} < \varepsilon_R(i)\, \text{and}\, |x|_{\bar{a}_i} = 0\} \\ &= \{a_1^{j_1} a_2^{j_2} \ldots a_n^{j_n} \mid j_1, j_2, \ldots, j_n \in \mathbb{Z}, \text{and, for all}\, i = 1,\ldots,n, \text{if}\, \varepsilon_R(i) < \infty, \text{then}\, 0 \leq j_i < \varepsilon_R(i)\}. \end{aligned}$$

3 Prefix-rewriting systems and PCP2-presentations for subgroups of polycyclic groups

Let $\langle \Sigma; R\rangle$ be a finite confluent PCP2-presentation of a polycyclic group G, let V be a finite subset of Σ^*, and let H denote the subgroup of G that is generated by V, i.e., $H = \langle V\rangle$. We are interested in particular sets of generators for H. To define these we need the following technical notions.

Let $v = a_1^{\tau(1)} a_2^{\tau(2)} \cdots a_n^{\tau(n)} \in IRR(R) - \{\lambda\}$, i.e., for $i = 1,\ldots,n$, if $\varepsilon_R(i) < \infty$, then $0 \leq \tau(i) < \varepsilon_R(i)$. Then we define the following functions:

- $AB(v) := a_i$, if $\tau(i) \neq 0$ and $\tau(j) = 0$ for all $j = 1,\ldots,i-1$,
- $IAB(v) := i$, if $\tau(i) \neq 0$ and $\tau(j) = 0$ for all $j = 1,\ldots,i-1$,
- $KO(v,i) := \tau(i)$ for all $i = 1,\ldots,n$,
- $KOAB(v) := KO(v, IAB(v))$,
- $AT(v) := AB(v)^{KOAB(v)}$,
- $REST(v) := a_{i+1}^{\tau(i+1)} \cdots a_n^{\tau(n)}$ if $IAB(v) = i$,
- $AT^{-1}(v) := AT((v^{-1})\downarrow)$, where $w\downarrow$ denotes the irreducible descendant of w mod R,
- $REST^{-1}(v) := REST((v^{-1})\downarrow)$.

Thus, for $v \in IRR(R) - \{\lambda\}$, $AT(v)$ is the first nonempty syllable of v, and $REST(v)$ is v without this syllable.

If $\varepsilon_R(i) < \infty$, where $i = IAB(v)$, then there exists a positive integer p such that $IAB((v^p)\downarrow) > IAB(v)$. By $EXP1(v)$ we denote the smallest positive integer with this property. It is easily seen that

$$EXP1(v) = lcm(KOAB(v), \varepsilon_R(i))/KOAB(v),$$

where $lcm(i,j)$ denotes the least common multiple of i and j. Finally, if $\varepsilon_R(i) = \infty$, we take $EXP1(v) := \infty$. Using these technical notions we can now state the following definition which is fundamental to our treatment of subgroups of polycyclic groups.

Definition 3.1 .
Let $\Omega = (u_1,\ldots,u_s)$, where $u_1,\ldots,u_s \in IRR(R) - \{\lambda\}$. Then Ω is a **canonical base** *for the subgroup H of G, if the following four conditions are satisfied:*

1. *$\forall v \in H\, \exists i_1,\ldots,i_s \in \mathbb{Z}$: $v \leftrightarrow_R^* u_1^{i_1} \cdots u_s^{i_s}$, where $EXP1(u_j) < \infty$ implies that $0 \leq i_j < EXP1(u_j)$, $j = 1,\ldots,s$,*
2. *$IAB(u_i) < IAB(u_{i+1})$, $i = 1,\ldots,s-1$,*
3. *$KOAB(u_i) > 0$, $i = 1,\ldots,s$, and*
4. *if $IAB((u_i^m)\downarrow) = IAB(u_i)$, then $KOAB(u_i) \leq |KOAB((u_i^m)\downarrow)|$ for all $i = 1,\ldots,s$ and $m \in \mathbb{Z}$.*

From this definition the following properties of a canonical base can be derived in a fairly straightforward manner.

Lemma 3.2 .
Let $\langle\Sigma; R\rangle$ *be a finite confluent PCP2-presentation of* G*, and let* $\Omega = (u_1, \ldots, u_s)$ *be a canonicel base for the subgroup* H *of* G.

(a) $AT((u_i^{\tau(i)}u_{i+1}^{\tau(i+1)} \cdots u_s^{\tau(s)}) \downarrow) = AT(u_i)^{\tau(i)}$ *for all* $i \in \{1, \ldots, s\}$, $\tau(i) \in \mathbb{Z} - \{0\}$ *and* $\tau(i+1), \ldots, \tau(s) \in \mathbb{Z}$, *proviaed* $0 < \tau(i) < EXP1(u_i)$ *if* $EXP1(u_i) < \infty$.

(b) *For all* $i \in \{1, \ldots, s\}$, $\Omega_i := (u_i, \ldots, u_s)$ *is a canonical base for the subgroup* $H_i := \langle u_i, \ldots, u_s\rangle$ *of* G.

(c) *For all* $i \in \{1, \ldots, s-1\}$, $j \in \{i+1, \ldots, s\}$ *and* $\delta, \varepsilon \in \{1, -1\}$, $u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta} \in H_{i+1}$.

(d) *For all* $i \in \{1, \ldots, s-1\}$, *if* $EXP1(u_i) < \infty$, *then* $u_i^{EXP1(u_i)} \in H_{i+1}$.

From part (a) of the above lemma we can draw the following conclusion concerning the way in which the elements of a subgrouj H are presented through a canonical base.

Corollary 3.3 .
Let $\langle\Sigma; R\rangle$ *be a finite confluent PCP2-presentation of a group* G*, and let* $\Omega = (u_1, \ldots, u_s)$ *be a canonical base for the subgroup* H *of* G*. If* $u_1^{j_1}u_2^{j_2} \cdots u_s^{j_s} \leftrightarrow_R^* u_1^{k_1}u_2^{k_2} \cdots u_s^{k_s}$, *where* $EXP1(u_i) < \infty$ *implies that* $0 \leq j_i, k_i < EXP1(u_i)$, $1 \leq i \leq s$, *then* $j_i = k_i$ *for all* $i = 1, \ldots, s$.

Proof. Assume that $j_1 > 0$. Then by Lemma 3.2 (a)

$$AT(u_1)^{j_1} = AT((u_1^{j_1} \cdots u_s^{j_s}) \downarrow) = AT((u_1^{k_1} \cdots u_s^{k_s}) \downarrow),$$

which implies that $k_1 = j_1$. Hence, $u_2^{j_2} \cdots u_s^{j_s} \leftrightarrow_R^* u_2^{k_2} \cdots u_s^{k_s}$, and proceding inductively we obtain $j_i = k_i$ for all $j = 1, \ldots, s$. □

Thus, the presentation of an element of the subgroup H through the elements of a canonical base, as described in Definition 3.1 (1), is unique.

One of the main results of [22] states that, given a finite confluent PCP2-presentation $\langle\Sigma; R\rangle$ of a polycyclic group G and a finite set V of generators of a subgroup H of G, a canonical base $\Omega = (u_1, \ldots, u_s)$ for the subgroup H can be constructed effectively by employing a specialized completion procedure. With Ω we associate a finite set of prefix-rules as follows:

$$\begin{array}{rcl} P(\Omega) & := & \{AT(u_i) \to ((REST(u_i))^{-1}) \downarrow \mid i = 1, \ldots, s\} \\ & \cup & \{AT^{-1}(u_i) \to ((REST^{-1}(u_i))^{-1}) \downarrow \mid i \in \{1, \ldots, s\} \text{ and } EXP1(u_i) = \infty\}. \end{array}$$

It is then easily seen that $u \Longleftrightarrow^*_{P(\Omega)\cup P_R} v$ holds if and only if $Hu = Hv$, i.e., if u and v define the same right-coset of G mod H. In particular, this implies that $u \Longleftrightarrow^*_{P(\Omega)\cup P_R} \lambda$ if and only if $u \in H$. Furthermore, in the setting considered the reduction relation $\Longrightarrow_{P(\Omega)\cup P_R}$ is noetherian and λ-confluent.

Thus, the relation $\Longrightarrow_{P(\Omega)\cup P_R}$ yields a way to decide the generalized word problem for the subgroup H. In addition, if $u \in H$, then a string $v \in (\Omega \cup \{u_i^{-1} \mid u_i \in \Omega\})^*$ satisfying $u \leftrightarrow_R^* v$ can easily be extracted from a reduction sequence $u = u_0 \Longrightarrow_{P(\Omega)\cup P_R} u_1 \Longrightarrow_{P(\Omega)\cup P_R} \cdots$

$\Longrightarrow_{P(\Omega)\cup P_R} \lambda$, i.e., we also have an effective rewrite process with respect to the canonical base for H. It remains to show how to extract a PCP2-presentation for H from $\langle\Sigma; R\rangle$ and Ω.

For $i = 1, 2, \ldots, s$, let H_i denote the subgroup of G that is generated by the set $\Omega_i := \{u_i, \ldots, u_s\}$. Then Ω_i is a canonical base for H_i. Hence, by the above remark we have an effective rewrite process $\sigma_i : H_i \to (\Omega_i \cup \{u_i^{-1}, \ldots, u_s^{-1}\})^*$ such that, for each $w \in \Sigma^*$, if $w \in H_i$, then $w \leftrightarrow_R^* \sigma_i(w)$. From $\langle\Sigma; R\rangle, \Omega$ and these rewrite processes $\sigma_1, \sigma_2, \ldots, \sigma_s$ we now construct a monoid-presentation $\langle\Gamma; S\rangle$ for the subgroup H as follows.

Let $\Gamma = \{b_1, \ldots, b_s, \overline{b}_1, \ldots, \overline{b}_s\}$ be a new alphabet, and let $S_0 := \{b_j\overline{b}_j \to \lambda, \overline{b}_j b_j \to \lambda \mid j = 1, \ldots, s\}$.

By Lemma 3.2(c) $u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta} \in H_{i+1}$ for all $i \in \{1, \ldots, s-1\}$, $j \in \{i+1, \ldots, s\}$ and $\delta, \varepsilon \in \{1, -1\}$, and so $\sigma_{i+1}(u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta}) \in (\Omega_{i+1} \cup \{u_{i+1}^{-1}, \ldots, u_s^{-1}\})^*$. Let $\eta_{i+1}(u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta}) \in \{b_{i+1}, \ldots, b_s, \overline{b}_{i+1}, \ldots, \overline{b}_s\}^*$ be the word that is obtained from $\sigma_{i+1}(u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta})$ by replacing each factor u_k^{γ} $(k \in \{i+1, \ldots, s\}, \gamma \in \{1, -1\})$ by the letter b_k^{γ}. Then we take S_C to be the following set of CP2-rules on Γ :

$$S_C := \{b_j^{\varepsilon}b_i^{\delta} \to b_i^{\delta}\eta_{i+1}(u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta}) \mid i \in \{1, \ldots, s-1\}, j > i, \delta, \varepsilon \in \{1, -1\}\},$$

i.e., S_C is a CP2-system on Γ.

By Lemma 3.2(d) $u_i^{EXP1(u_i)} \in H_{i+1}$ for all $i \in \{1, \ldots, s-1\}$, for which $EXP1(u_i) < \infty$ holds, and so $\sigma_{i+1}(u_i^{EXP1(u_i)}) \in (\Omega_{i+1} \cup \{u_{i+1}^{-1}, \ldots, u_s^{-1}\})^*$. We let S_P denote the following set of P-rules on Γ :

$$\begin{array}{rcl} S_P & := & \{b_i^{EXP1(u_i)} \to \eta_{i+1}(u_i^{EXP1(u_i)}), \overline{b}_i \to b_i^{EXP1(u_i)-1}(\eta_{i+1}(u_i^{EXP1(u_i)}))^{-1} \mid \\ & & \qquad i \in \{1, \ldots, s\} \text{ such that } EXP1(u_i) < \infty\}. \end{array}$$

Then S_P is a P-system on Γ. Thus, if S denotes the finite string-rewriting system $S := S_0 \cup S_C \cup S_P$, then $\langle\Gamma; S\rangle$ is a finite PCP2-presentation. Hence, the group K presented by $\langle\Gamma; S\rangle$ is polycyclic. Observe that this presentation has been constructed effectively from $\langle\Sigma; R\rangle$ and Ω.

Lemma 3.4 .
The presentation $\langle\Gamma; S\rangle$ describes the subgroup H of G, i.e., K is isomorphic to H.

Proof. We define a mapping $\alpha : \Gamma^* \to \Sigma^*$ through $b_i \mapsto u_i$ and $\overline{b}_i \mapsto u_i^{-1}$, $1 \le i \le s$. Since

$$\alpha(b_j^{\varepsilon}b_i^{\delta}) = u_j^{\varepsilon}u_i^{\delta} \leftrightarrow_R^* u_i^{\delta}u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta} \leftrightarrow_R^* u_i^{\delta}\sigma_{i+1}(u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta}) = \alpha(b_i^{\delta}\eta_{i+1}(u_i^{-\delta}u_j^{\varepsilon}u_i^{\delta})),$$

and since

$$\alpha(b_i^{EXP1(u_i)}) = u_i^{EXP1(u_i)} \leftrightarrow_R^* \sigma_{i+1}(u_i^{EXP1(u_i)}) = \alpha(\eta_{i+1}(u_i^{EXP1(u_i)}))$$

and

$$\begin{array}{rcl} \alpha(\overline{b}_i) = u_i^{-1} & \leftrightarrow_R^* & u_i^{-1}u_i^{EXP1(u_i)}(\sigma_{i+1}(u_i^{EXP1(u_i)}))^{-1} \\ & \leftrightarrow_R^* & u_i^{EXP1(u_i)-1}(\sigma_{i+1}(u_i^{EXP1(u_i)}))^{-1} \\ & = & \alpha(b_i^{EXP1(u_i)-1}(\eta_{i+1}(u_i^{EXP1(u_i)}))^{-1}), \end{array}$$

we have $\alpha(\ell) \leftrightarrow_R^* \alpha(r)$ for all rules $(\ell, r) \in S$, i.e., α induces a group-homomorphism from the group K onto the subgroup H of G. It remains to verify that this homomorphism is injective.

Since $\langle \Gamma; S \rangle$ is a PCP2-presentation, the string-rewriting system S is noetherian. Let $w \in \Gamma^*$ be irreducible mod S.

Claim. If $w \neq \lambda$, then $\alpha(w) \not\leftrightarrow_R^* \lambda$.
Proof. Assume that $w \neq \lambda$. We have $w = b_1^{j_1} \cdots b_s^{j_s}$, where $EXP1(u_i) < \infty$ implies that $0 \leq j_i < EXP1(u_i)$, since $\varepsilon_S(i) = EXP1(u_i)$, $i = 1, \ldots, s$. Hence, $\alpha(w) = u_1^{j_1} \cdots u_s^{j_s}$, where $EXP1(u_i) < \infty$ implies that $0 \leq j_i < EXP1(u_i)$. Let $k := min\{i \mid j_i \neq 0\}$. Since $w \neq \lambda$, we have $k \in \{1, \ldots, s\}$. Then

$$AT(\alpha(w)\downarrow) = AT((u_k^{j_k} u_{k+1}^{j_{k+1}} \cdots u_s^{j_s})\downarrow) = AT(u_k)^{j_k}$$

by Lemma 3.2(a), which means that $\alpha(w)\downarrow \neq \lambda$. Thus, $\alpha(w) \not\rightarrow_R^* \lambda$, and hence, $\alpha(w) \not\leftrightarrow_R^* \lambda$, since R is confluent. □

Thus, the homomorphism $\alpha : K \to H$ is indeed injective, and therefore K and H are isomorphic, i.e., $\langle \Gamma; S \rangle$ is a PCP2-presentation for the subgroup H of G. □

The above proof shows even more. If $w \in \Gamma^*$, then there is a string $w_0 = b_1^{j_1} \cdots b_s^{j_s}$ such that $w \to_S^* w_0$, where $EXP1(u_i) < \infty$ implies that $0 \leq j_i < EXP1(u_i)$, $i = 1, \ldots, s$. Thus, $\alpha(w) \leftrightarrow_R^* \alpha(w_0) = u_1^{j_1} \cdots u_s^{j_s}$. Now let $v \in \Gamma^*$ be such that $w \leftrightarrow_S^* v$. Then $v \to_S^* v_0 = b_1^{k_1} \cdots b_s^{k_s}$, where $EXP1(u_i) < \infty$ implies that $0 \leq k_i < EXP1(u_i)$, $i = 1, \ldots, s$, and hence,

$$u_1^{j_1} \cdots u_s^{j_s} = \alpha(w_0) \leftrightarrow_R^* \alpha(w) \leftrightarrow_R^* \alpha(v) \leftrightarrow_R^* \alpha(v_0) = u_1^{k_1} \cdots u_s^{k_s}.$$

By Corollary 3.3 we can conclude that $j_i = k_i$, $i = 1, \ldots, s$, which means that $w \to_S^* b_1^{j_1} \cdots b_s^{j_s} \leftarrow_S^* v$. Hence, the string-rewriting system S is confluent. We can thus summarize our results as follows.

Theorem 3.5 . *There is an algorithm that solves the following task:*

INPUT : *A finite PCP2-presentation $\langle \Sigma; R \rangle$ of a group G, and a finite subset $V \subset \Sigma^*$.*

OUTPUT : *A finite confluent PCP2-presentation $\langle \Gamma; S \rangle$ for the subgroup H of G that is generated by V.*

Thus, finite (confluent) PCP2-presentations do not only give a nice combinatorial characterization for the class of finitely presented polycyclic groups, but they also give a means to effectively perform calculations of subgroups of these groups. This completes our investigation of polycyclic groups. We now turn to the context-free groups.

4 Prefix-rewriting systems for context-free groups

Let R be a finite, monadic, and λ-confluent string-rewriting system on Σ such that the monoid M_R is a group, and let $U \subset \Sigma^*$ be a finite set of words that is closed under taking inverses. Further, let $P = P_U \cup P_R$ be a prefix-rewriting system associated with $(\Sigma; R)$ and U such that $u > v$ holds for each rule $(u, v) \in P$, where $>$ again denotes the length-lexicographical ordering on Σ^*. Then the prefix-rewriting system P is noetherian. If, in addition, P is λ-confluent, then $\langle U\rangle \cap IRR(\Longrightarrow_P) = [\lambda]_U \cap IRR(\Longrightarrow_P) = \{\lambda\}$, and hence, membership in $\langle U\rangle$ can simply be decided by prefix-rewriting mod P.

In [11] the authors present a test for λ-confluence of prefix-rewriting systems of this form for the particular case that the underlying string-rewriting system R is finite, length-reducing, and confluent, and that it presents a group. This test reduces the problem of deciding λ-confluence of P to the problem of verifying the equality of certain regular sets. It can be carried over to the case considered here, but it gets much more complicated due to the fact that the underlying system R is not confluent. However, another much simpler test for λ-confluence of P can be devised based on Proposition 2.4.

Lemma 4.1 . *Let R be a finite, monadic, and λ-confluent string-rewriting system on Σ such that the monoid M_R is a group, let $U \subset \Sigma^*$ be a finite set that is closed under taking inverses, and let $P := P_U \cup P_R$ be a noetherian prefix-rewriting system that is associated with $(\Sigma; R)$ and U. Then this prefix-rewriting system is λ-confluent if and only if $I_R(U^*) \cap IRR(\Longrightarrow_{P_U}) = \{\lambda\}$.*

Proof. If P is λ-confluent, then $w \Longrightarrow_P^* \lambda$ holds for each word $w \in \langle U\rangle = [\lambda]_U$. Thus, each word $w \in I_R(U^*) = [U^*]_R \cap IRR(R) = \langle U\rangle \cap IRR(R)$ reduces to λ mod P, and so each word $w \in I_R(U^*) - \{\lambda\}$ must have a non-empty prefix that is the left-hand side of a rule (u, v) of P_U.

Conversely, assume that $I_R(U^*) \cap IRR(\Longrightarrow_{P_U}) = \{\lambda\}$, and let $w \in \langle U\rangle$. Then $w \longrightarrow_R^* w_0$ for some $w_0 \in I_R(U^*)$, since R is noetherian. If $w_0 \neq \lambda$, then $w_0 \notin IRR(\Longrightarrow_{P_U})$, i.e., a prefix-rule $(u, v) \in P_U$ applies to w_0, and so $w_0 \Longrightarrow_{P_U} w_1$. Since $\Longleftrightarrow_P^* = \sim_U$, we have $w_1 \in \langle U\rangle$, and hence, $w_1 \longrightarrow_R^* w_2$ for some word $w_2 \in IRR(U^*)$. Continuing in this way we obtain a sequence $w \longrightarrow_R^* w_0 \Longrightarrow_P w_1 \longrightarrow_R^* w_2 \Longrightarrow_P \ldots$, which terminates, since P is noetherian. Hence, we have a reduction $w \Longrightarrow_P^* \lambda$. Thus, P is λ-confluent. □

From $(\Sigma; R)$ and U we can construct an nfsa for the set $I_R(U^*)$ in polynomial time. If $P_U = \{(x_1, y_1), \ldots, (x_m, y_m)\}$, then $IRR(\Longrightarrow_{P_U}) = \Sigma^* - \bigcup_{i=1}^m x_i \cdot \Sigma^*$. Hence, we obtain an nfsa for the set $I_R(U^*) \cap IRR(\Longrightarrow_{P_U})$ in polynomial time. This gives the following decidability result.

Theorem 4.2 . *The following problem is decidable in polynomial time:*

INSTANCE: *A finite, monadic, and λ-confluent string-rewriting system R on Σ such that M_R is a group, a finite set $U \subset \Sigma^*$ that is closed under taking inverses, and a noetherian prefix-rewriting system $P = P_U \cup P_R$ that is associated with $(\Sigma; R)$ and U.*

QUESTION: *Is P λ-confluent?*

Based on the above test for λ-confluence we could now develop a Knuth-Bendix-style completion procedure that, given a prefix-rewriting system $P = P_U \cup P_R$ that is not λ-confluent as input, tries to construct an equivalent system that is λ-confluent by adding certain rules to P_U. However, a λ-confluent prefix-rewriting system P associated with $(\Sigma; R)$ and U can immediately be extracted from an nfsa for the set $I_R(U^*)$. For the case of groups presented by finite, length-reducing, and confluent string-rewriting systems this has been observed by Kuhn [9].

Let R be a finite monadic string-rewriting system on Σ such that R is λ-confluent, and M_R is a group, and let $U \subset \Sigma^*$ be a finite set that is closed under taking inverses. From R and U we first construct an nfsa $B = (Q, \Sigma, q_0, \delta, F)$ that accepts the set $I_R(U^*) =$

$\{w \in IRR(R) \mid \exists n \geq 0 \, \exists u_1, \ldots, u_m \in U : w \longleftrightarrow_R^* u_1 \cdots u_m\}$. To simplify the following discussion we identify the nfsa B with its state graph, and we can talk about "paths" in B. From B we extract a set P_1 of prefix-rules as follows.

(i) For every simple path in B 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_1, where x is the label along the path considered.

(ii) For every path p in B from the initial state 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_1x_2, x_1) into P_1, where x_i is the label along the path p_i $(i = 1, 2)$.

Obviously, P_1 can be constructed effectively from B, and for all rules $(x, y) \in P_1$, $\mid x \mid > \mid y \mid$ holds.

Lemma 4.3 . *The system P_1 has the following properties:*

(a) For all $(x, y) \in P_1$, $xy^{-1} \in \langle U \rangle$,

(b) $\Longleftrightarrow_P^* = \sim_U$, where $P = P_1 \cup P_R$, and

(c) $\Longrightarrow_P$ is λ-confluent.

Proof.
(a) Let $(x, y) \in P_1$. If $y = \lambda$, then x is the label along a simple path in B from q_0 to some $q_f \in F$ by (i). Hence, $x \in L(B) = I_R(U^*)$ implying that $xy^{-1} = x \in \langle U \rangle$. If $y \neq \lambda$, then by (ii) $x = yz$ for some nonempty word z, and there is a nonempty word v such that $xv = yzv$ and yv are both accepted by B. Thus, $yzv, yv \in \langle U \rangle$, and so $xy^{-1} = yzy^{-1} \longleftrightarrow_R^* yzv \cdot v^{-1}y^{-1} = (yzv) \cdot (yv)^{-1} \in \langle U \rangle$.

(c) Let $w \in \langle U \rangle$. We claim that $w \Longrightarrow_P^* \lambda$. Since R is noetherian, there is a word $w_0 \in IRR(R)$ such that $w \longrightarrow_R^* w_0$, and so $w_0 \in I_R(U^*)$. If $w_0 = \lambda$, nothing remains to be shown; otherwise, there is a path p in B from q_0 to some final state with label w_0. If p is a simple path that does not pass through any final state, then $(w_0, \lambda) \in P_1$ by (i); otherwise, there is a proper initial part p_1 of p that is simple, that ends at a final state, and that does not pass through a final state, or there is a proper initial part p_1, p_2 of p such that p_1 is simple, p_2 is a simple loop, and p_1, p_2 does not pass through a final state. In the former case $w_0 = x_1x_2$ for some rule $(x_1, \lambda) \in P_1$, in the latter $w_0 = x_1x_2x_3$ for some rule $(x_1x_2, x_1) \in P_1$. In either case, $w_0 \Longrightarrow_{P_1} w_1$ for some $w_1 \in \Sigma^*$ satisfying $\mid w_1 \mid < \mid w_0 \mid$. By (a) $w_0 \sim_U w_1$, and so by induction on $\mid w \mid$ we obtain $w \Longrightarrow_P^* \lambda$.

(b) Because of (a) we have $u \sim_U v$, whenever $u \Longleftrightarrow_P^* v$. To prove the converse implication assume that $u \sim_U v$. Then $uv^{-1} \in \langle U \rangle$, and hence, $u \longleftrightarrow_R^* uv^{-1} \cdot v \Longrightarrow_P^* v$ from the proof of (c), i.e., $u \Longleftrightarrow_P^* v$. □

In general, it can happen that, for some $u \in U$, the set of rules P_1 does not contain a rule (x, y) satisfying $xy^{-1} \longleftrightarrow_R^* u$. In order to also fulfill this formal requirement, we could then simply add the rule (u, λ) to P_1. Thus, we have the following result.

Theorem 4.4 . *For each finite, monadic, and λ-confluent string-rewriting system R on Σ that presents a group, and for each finite subset $U \subset \Sigma^*$, there exists a finite, length-reducing* *set of prefix-rewrite rules P_U such that the prefix-rewriting system $P = P_U \cup P_R$ presents the right-congruence $\sim_U$, and is λ-confluent. In fact, P_U can be constructed effectively from $(\Sigma; R)$ and U.*

The complexity of this construction is closely related to the number of simple paths and simple loops in the nfsa B for the set $I_R(U^*)$. Whenever this number is bounded by a polynomial, then P_U is obtainable in polynomial time. Once we have the system P_U, the membership problem for $\langle U \rangle$ can be solved in polynomial time by prefix-rewriting mod $P = P_U \cup P_R$.

Given a subset $U \subset \Sigma^*$ and a word $w \in \Sigma^*$, one is not only interested in deciding whether or not w belongs to the subgroup $\langle U \rangle$, but in the affirmative one also wants to "rewrite" w as a product of the given generators U, i.e., determine words $u_1, \ldots, u_m \in U$ such that $w \overset{*}{\longleftrightarrow}_R u_1 \cdots u_m$. In the following we present such a "rewrite process". This process will consist of two phases. In phase 1 a word $w \in \langle U \rangle$ is transformed into a congruent word $v \in \Delta_R^*(U^*) \cap IRR(R)$, and in phase 2 a word $u \in U^*$ is determined such that $u \longrightarrow_R^* v$. Then $w \longleftrightarrow_R^* u$, and hence, u can be taken as the result of rewriting w.

So let $w \in \langle U \rangle$. By Proposition 2.4 the set $I_R(w) = [w]_R \cap IRR(R)$ is regular, and from R and w an nfsa B_1 for $I_R(w)$ can be constructed in polynomial time. The set U^* is regular, and hence, so is the set of descendants $\Delta_R^*(U^*)$. Again, from R and U an nfsa B_2 for $\Delta_R^*(U^*)$ can be constructed in polynomial time (cf. [5]). Since $w \in \langle U \rangle$, there are words $u_1, \ldots, u_m \in U$ such that $w \longleftrightarrow_R^* u_1 \cdots u_m$, and so each irreducible descendant of $u_1 \cdots u_m$ belongs both to $\Delta_R^*(U^*)$ and to $I_R(w)$. Thus, the intersection $I_R(w) \cap \Delta_R^*(U^*)$ is nonempty, and from B_1 and B_2 we can extract the minimal word $v(w)$ with respect to the length-lexicographical ordering that belongs to this intersection. The word $v(w)$ is uniquely determined, and hence, we can define a mapping $\sigma_1 : \langle U \rangle \rightarrow \Delta_R^*(U^*) \cap IRR(R)$ through $w \mapsto v(w)$ $(w \in \langle U \rangle)$. Observe that, given $(\Sigma; R)$, U, and $w \in \langle U \rangle$ as input, the word $\sigma_1(w)$ is computed in polynomial time.

Now let $v \in \Delta_R^*(U^*)$. We want to compute a word $u \in U^*$ such that $u \longrightarrow_R^* v$. Let $\nabla_R^*(v) := \{y \in \Sigma^* \mid y \longrightarrow_R^* v\}$. Since R is monadic, the set $\nabla_R^*(v)$ is context-free [6], and from R and v a context-free grammar $G_1(v)$ for this set can be easily determined. Since $v \in \Delta_R^*(U^*)$, we know that the intersection $\nabla_R^*(v) \cap U^*$ is nonempty. From the grammar $G_1(v)$ and an nfsa for U^* we can construct a context-free grammar $G_2(v)$ for this intersection, and from $G_2(v)$ we can determine a word $u(v) \in \nabla_R^*(v) \cap U^*$. In this way we obtain a mapping $\sigma_2 : \Delta_R^*(U^*) \rightarrow U^*$ such that, for $v \in \Delta_R^*(U^*), \sigma_2(v) \longrightarrow_R^* v$. Unfortunately, since the construction of the grammar $G_2(v)$ from the grammar $G_1(v)$ and U involves the task of determining the Greibach normal form of $G_1(v)$, we see currently no way to perform this process in polynomial time.

Combining the mappings σ_1 and σ_2 we obtain an effective rewrite process $\sigma : \langle U \rangle \rightarrow U^*$. Thus, we have the following result.

Theorem 4.5 . *Let R be a finite, monadic, and λ-confluent string-rewriting system that presents a group. Given a finite subset $U \subset \Sigma^*$, a rewrite process $\sigma : \langle U \rangle \rightarrow U^*$ satisfying $\sigma(w) \longleftrightarrow_R^* w$ can be constructed effectively.*

5 Presentations of subgroups of context-free groups

Let $\langle \Sigma; R \rangle$ be a finite group-presentation such that the string-rewriting system R is monadic and λ-confluent, and let $U = \{u_1, \ldots, u_m\}$ be a finite set of words from Σ^*. Then the subgroup $\langle U \rangle$ of M_R generated by U is a context-free group [19], and hence, it can be presented by some finite, monadic, and λ-confluent string-rewriting system T on some alphabet Γ. In this section we present a construction that yields a presentation of this form for $\langle U \rangle$. As outlined in the introduction this construction consists of three steps. First we derive a dfsa A from the group-presentation $\langle \Sigma; R \rangle$ and the set U.

Construction 5.1 . *A dfsa A for a subset of* $\langle U \rangle$*:*

```
INPUT:  A finite, monadic, and $\lambda$-confluent string-rewriting system $R$ on $\Sigma$
        such that $\langle \Sigma; R \rangle$ is a group-presentation, and a finite set of words
        $U = \{u_1, \ldots, u_m\} \cup \{u_1^{-1}, \ldots, u_m^{-1}\} \subset \Sigma^*$;
comment: Since $\langle \Sigma; R \rangle$ is a group-presentation, each letter $a \in \Sigma$ has an inverse
of length 1, and $R$ contains the rules $\{a\bar{a} \rightarrow \lambda \mid a \in \Sigma\}$. The formal inverses
$u_1^{-1}, \ldots, u_m^{-1}$ are included in $U$ to simplify the notation in what follows.
begin
(0)     an nfsa $A'_0 = (Q_0, \Sigma, q_0, \delta_0, \{q_0\})$ is constructed by adding a loop from
        $q_0$ to $q_0$ with label $u_i$ for each $i \in \{1, \ldots, m\}$, and by adding state $q_j$ to
        $\delta_0(q_i, \bar{a})$ whenever $q_i \in \delta_0(q_j, a)$;
        $i := 0$;
        comment: $A'_0$ is an nfsa with $L(A'_0) = U^*$;
(1)     while   $\exists q \in Q_i \exists a \in \Sigma$: $|\ \delta_i(q, a)\ | > 1$ do
        begin   choose $q, q_1, q_2 \in Q_i$ and $a \in \Sigma$ such that $q_1, q_2 \in \delta_i(q, a)$,
                $q_1 \neq q_2$, and $q_2 \neq q_0$;
                $Q_i := Q_i - \{q_2\}$;
                replace $q_2$ by $q_1$ in $\delta_i$
        end;
        comment: After a finite number of iterations this while-loop termi-
        nates with a dfsa $A_i = (Q_i, \Sigma, q_0, \delta_i, \{q_0\})$, since during each iteration
        the number of states is reduced by one;
(2)     if $\exists q \in Q_i \exists (l \rightarrow r) \in R$: $\delta_i(q, l)$ is defined and $\delta_i(q, l) \neq \delta_i(q, r)$ then
        begin
                if $r \in \Sigma$ and $\delta_i(q, r) = \emptyset$ then
                begin
                        $Q_{i+1} := Q_i$;
                        $\delta_{i+1} := \delta_i \cup \{((q, r), \delta_i(q, l)), ((\delta_i(q, l), \bar{r}), q)\}$;
                        comment: Together with the transition $q \longrightarrow^{r} q'$
                        also the transition $q' \longrightarrow^{\bar{r}} q$ is introduced
                end
                else
                if $r \in \Sigma$ and $\delta_i(q, r)$ is defined then
                begin
                        if $\delta_i(q, r) = q_0$   then   $\{q_1 := \delta_i(q, r)$;
                                                          $q_2 := \delta_i(q, l)\}$
                                                   else   $\{q_1 := \delta_i(q, l)$;
                                                          $q_2 := \delta_i(q, r)\}$;
                        $Q_{i+1} := Q_i - \{q_2\}$;
                        $\delta_{i+1} := \delta_i |_{replace\, q_2\, by\, q_1}$
                end
                else     {comment: $r = \lambda$ and $\delta_i(q,l) \neq q$}
                begin    if $\delta_i(q,l) = q_0$ then {$q_2$    $q$;
                                                       $q := q_0$}
                                            else   $q_2 := \delta_i(q,l)$;
                         $Q_{i+1} := Q_i - \{q_2\}$;
                         $\delta_{i+1} := \delta_i |_{replace\, q_2\, by\, q}$
                end;
                comment: $A'_{i+1} = (Q_{i+1}, \Sigma, q_0, \delta_{i+1}, \{q_0\})$ is an nfsa;
                $i := i + 1$;
                goto (1)
        end;
(3)     $A := A_i$;
        OUTPUT: $A = (Q, \Sigma, q_0, \delta, \{q_0\})$
end.
```

In general step (2) will introduce some nondeterminism into A'_{i+1}, which is then removed subsequently by the **while**-loop (1). In each iteration of the **goto**-loop two transitions $q \longrightarrow^{r} q'$ and $q' \longrightarrow^{\bar{r}} q$ are added, which can happen only if $\delta(q,r)$ was undefined before, or a state is deleted. Thus, the above construction terminates eventually. In fact, it computes a dfsa $A = (Q, \Sigma, q_0, \delta, \{q_0\})$ from $\langle \Sigma; R \rangle$ and U in polynomial time.

Before we can go to the second step of our construction, we must establish certain facts about the dfsa A.

Lemma 5.2 . *For all $q \in Q$ and all $a \in \Sigma$, if $\delta(q,a)$ is defined, then $\delta(\delta(q,a),\bar{a}) = q$.*

Proof. This property is true for the initial nfsa A'_0 after step (0). Obviously, it is preserved by the **while**-loop (1) as well as by step (2). □

Lemma 5.3 .

(a) $\Delta^*_R(U^*) \subseteq L(A)$.

(b) $L(A) \subseteq \langle U \rangle$.

Proof. We have $L(A'_0) = U^*$. The dfsa A is obtained from A'_0 through a finite sequence of elementary transformations, i.e., we have a sequence of finite-state acceptors $A'_0, A_0, A'_1, \ldots, A_k = A$ such that, for each $i \in \{0, 1, \ldots, k\}$, the dfsa A_i is obtained from A'_i by an execution of the **while**-loop (1), and the nfsa A'_{i+1} is obtained from A_i by step (2). We now establish some claims by induction on i.

Claim 1. For all $i = 0, 1, \ldots, k-1$, $L(A'_i) \subseteq L(A_i) \subseteq L(A'_{i+1}) \subseteq L(A_{i+1})$.
Proof. This is obvious from the construction. □

Claim 2. Let $w \in L(A)$, and let $u \in \Sigma^*$ be such that $w \longrightarrow_R u$. Then $u \in L(A)$, i.e., $L(A)$ is closed under the operation of taking descendants mod R.
Proof. Since $w \longrightarrow_R u$, we have $w = xly \longrightarrow_R xry = u$ for some rule $(l \rightarrow r) \in R$. Further, since $w \in L(A)$, there are states $q_1, q_2 \in Q$ such that we have the following transitions in A:

$$q_0 \longrightarrow^{x} q_1 \longrightarrow^{l} q_2 \longrightarrow^{y} q_0.$$

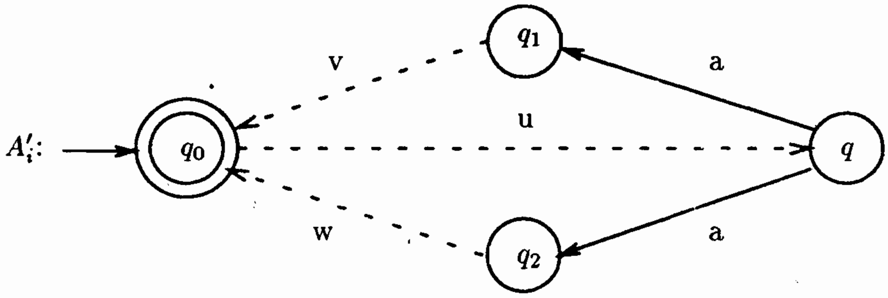
By the condition in (2) we have $\delta(q_1, r) = \delta(q_1, l) = q_2$, i.e., we also have the following transitions in A:

$$q_0 \longrightarrow^x q_1 \longrightarrow^r q_2 \longrightarrow^y q_0,$$

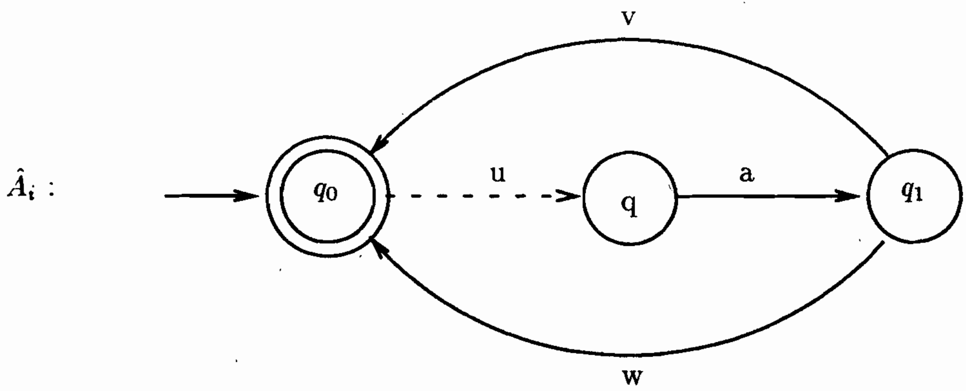
which means that $u = xry \in L(A)$. □

Since $L(A'_0) = U^*$, Claims 1 and 2 imply that $\Delta^*_R(U^*) \subseteq L(A)$.

Claim 3. For each $i \in \{0, 1, \ldots, k\}$, if $L(A'_i) \subseteq \langle U \rangle$, then $L(A_i) \subseteq \langle U \rangle$, too.
Proof. Suppose that $L(A'_i) \subseteq \langle U \rangle$ holds for some $i \in \{0, 1, \ldots, k\}$. If A'_i happens to be deterministic, then $A_i = A'_i$, and there is nothing to show. So assume that there are states $q, q_1, q_2 \in Q_i$ and a letter $a \in \Sigma$ such that $q_1 \neq q_2$, $q_2 \neq q_0$, and $q_1, q_2 \in \delta_i(q, a)$. From the construction we know that each state of A'_i is accessible as well as coaccessible, i.e., there exist words $u, v, w \in \Sigma^*$ such that $q \in \delta_i(q_0, u)$, $q_0 \in \delta_i(q_1, v)$, and $q_0 \in \delta_i(q_2, w)$. Graphically we can depict this situation as follows:



An execution of the body of the **while**-loop (1) identifies q_1 and q_2, i.e., we obtain the following situation:

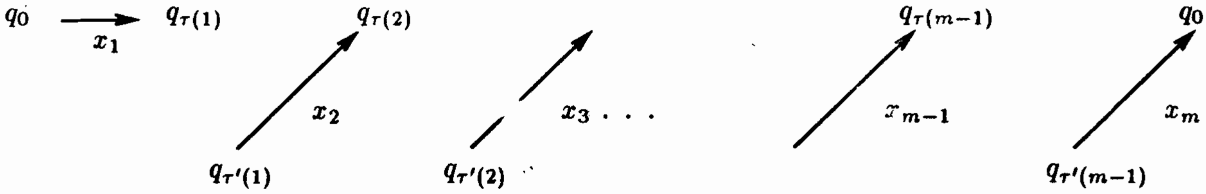


We claim that $L(\hat{A}_i) \subseteq \langle U \rangle$. Through induction on the number of times the body of the **while**-loop is executed we then obtain Claim 3.

So let $x \in L(\hat{A}_i)$, i.e., in $\hat{A}_i$ we have a path of the following form:

$$q_0 \longrightarrow_{x_1} q_1 \longrightarrow_{x_2} q_1 \longrightarrow_{x_3} \cdots \longrightarrow_{x_{m-1}} q_1 \longrightarrow_{x_m} q_0,$$

where $x = x_1 x_2 \ldots x_m$ is a factorization of x, and each occurrence of q_1 is displayed. In A'_i this path corresponds to a sequence of paths of the following form:



where $\tau(j), \tau'(j) \in \{1,2\}$, $j = 1,\dots,m-1$.

If, for some j, $\tau(j) = \tau'(j)$, then the path ending at $q_{\tau(j)}$ and the path beginning at $q_{\tau'(j)}$ form a single path in A_i'.

If, for some j, $\tau(j) = 1$ and $\tau'(j) = 2$, then

$$q_{\tau'(j-1)} \longrightarrow_{x_j} q_1 \longrightarrow_{vua} q_2 \longrightarrow_{x_{j+1}} q_{\tau(j+1)}$$

is a path in A_i', and if, for some j, $\tau(j) = 2$ and $\tau'(j) = 1$, then

$$q_{\tau'(j-1)} \longrightarrow_{x_j} q_2 \longrightarrow_{wua} q_1 \longrightarrow_{x_{j+1}} q_{\tau(j+1)}$$

is a path in A_i'. Thus, for $j = 1,\dots,m-1$, we define a word y_j as follows:

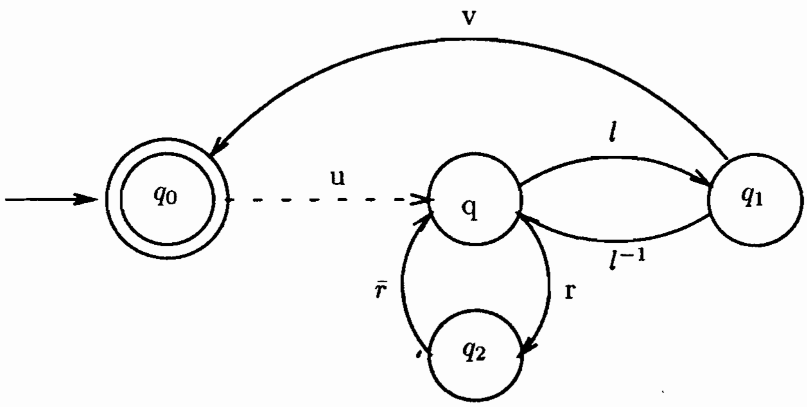
$$y_j := \begin{cases} v & if \quad \tau(j) = 1, \\ w & if \quad \tau(j) = 2. \end{cases}$$

Then $x_1y_1, uax_2y_2, \dots, uax_{m-1}y_{m-1}, uax_m \in L(A_i') \subseteq \langle U \rangle$, and $uay_1, uay_2, \dots, uay_{m-1} \in L(A_i') \subseteq \langle U \rangle$. Hence,

$$\begin{array}{rcl} x & = & x_1x_2\dots x_m \\ & \overset{*}{\longleftrightarrow}_R & (x_1y_1)\cdot(y_1^{-1}a^{-1}u^{-1})\cdot(uax_2y_2)\cdots(uax_{m-1}y_{m-1})\cdot(y_{m-1}^{-1}a^{-1}u^{-1})\cdot(uax_m) \\ & = & (x_1y_1)\cdot(uay_1)^{-1}\cdot(uax_2y_2)\cdots(uax_{m-1}y_{m-1})\cdot(uay_{m-1})^{-1}\cdot(uax_m) \in \langle U \rangle. \end{array}$$

Thus, $L(\hat{A}_i) \subseteq \langle U \rangle$. □

Claim 4. For each $i \in \{0,1,\dots,k-1\}$, if $L(A_i) \subseteq \langle U \rangle$, then $L(A_{i+1}') \subseteq \langle U \rangle$, too.
Proof. In A_i we have the following situation for some rule $(l \rightarrow r) \in R$:



(i) If $\delta_i(q,r)$ is undefined, then $r \in \Sigma$, and A'_{i+1} is obtained from A_i by simply adding the following two transitions:

$$q \longrightarrow^{r} q_1 \text{ and } q_1 \longrightarrow^{\bar{r}} q.$$

Thus, if $w \in L(A'_{i+1})$, then by replacing each transition $q \longrightarrow^{r} q_1$ in an accepting path in A'_{i+1} with label w by the path $q \longrightarrow \cdots^{l} \cdots \longrightarrow q_1$, and by replacing each transition $q_1 \longrightarrow^{\bar{r}} q$ by the path $q_1 \longrightarrow \cdots^{l^{-1}} \cdots \longrightarrow q$, we obtain an accepting path in A_i with label u such that $u \longleftrightarrow_R^* w$. By the hypothesis, $u \in \langle U \rangle$, and so $w \in \langle U \rangle$.

(ii) If $\delta_i(q,r)$ is defined, but $\delta_i(q,r) \neq \delta_i(q,l)$, then A'_{i+1} is obtained from A_i by identifying the states q_1 and q_2. Now $L(A'_{i+1}) \subseteq \langle U \rangle$ is shown similar to the proof of Claim 3. Observe that A_i contains the paths

$$q_2 \longrightarrow^{\bar{r}} q \longrightarrow^{l} q_1 \text{ and } q_1 \longrightarrow^{l^{-1}} q \longrightarrow^{r} q_2,$$

and that $\bar{r}l \longleftrightarrow_R^* \bar{r}r \longleftrightarrow_R \lambda$ and $l^{-1}r \longleftrightarrow_R l^{-1}l \longleftrightarrow_R^* \lambda$ hold. □

Since $L(A'_0) = U^* \subseteq \langle U \rangle$, Claims 3 and 4 together yield that $L(A) = L(A_k) \subseteq \langle U \rangle$. This completes the proof of Lemma 5.3. □

Now using breadth-first search on the graph underlying the dfsa A, and starting with the state q_0, we determine, for each state $q \in Q$, the minimal word $r(q)$ with respect to the length-lexicographical ordering that labels a path from q_0 to q. Since each state is accessible, we thus obtain a word $r(q)$ for each state $q \in Q$. By REP we denote the set $REP = \{r(q) \mid q \in Q\}$. Observe that, for each $q \in Q$, $\delta(q_0, r(q)) = q$, that $\delta(q, (r(q))^{-1}) = q_0$ by Lemma 5.2, and that $r(q_0) = \lambda$.

Lemma 5.4 . *For all $x, y \in \Sigma^*$, if $\delta(q_0, x)$ and $\delta(q_0, y)$ are defined and equal, then $x \sim_U y$.*

Proof. Let q denote the state $q = \delta(q_0, x) = \delta(q_0, y)$. Since $\delta(q, (r(q))^{-1}) = q_0$, we have $x(r(q))^{-1}, y(r(q))^{-1} \in L(A) \subseteq \langle U \rangle$. Thus, $xy^{-1} \longleftrightarrow_R^* (x(r(q))^{-1}) \cdot (r(q)y^{-1}) = (x(r(q))^{-1}) \cdot (y(r(q))^{-1})^{-1} \in \langle U \rangle$, i.e., $x \sim_U y$. □

Hence, each word $r(q) \in REP$ represents a coset of $\langle U \rangle$ in M_R. However, different words $r(q)$ and $r(q')$ may represent the same coset, and in general, there will be cosets that are not presented by any of these words. The following technical observation will be useful in what follows.

Lemma 5.5 . *The set REP is closed under taking prefixes, i.e., if $uv \in REP$ for some $u \in \Sigma^*$ and $v \in \Sigma^+$, then $u \in REP$.*

Proof. If $uv = r(q_2)$, then there is a state q_1 such that $\delta(q_0, u) = q_1$ and $\delta(q_1, v) = q_2$. Since uv is the minimal word satisfying $\delta(q_0, uv) = q_2$, and since $v \neq \lambda$, we have $q_1 \neq q_2$.

Assume that $\delta(q_0, w) = q_1$ for some word w such that $u > w$. Then $\delta(q_0, wv) = \delta(q_1, v) = q_2$ and $uv > wv$, contradicting the minimality of $uv = r(q_2)$. Thus, $r(q_1) = u$ implying that $u \in REP$. □

The rewriting process of Reidemeister and Schreier uses a complete set of minimal representatives for all the cosets of $\langle U \rangle$ to construct a presentation for $\langle U \rangle$ [17]. Here we technically perform the same steps; however, we use the partial and ambiguous set of coset representatives REP.

First, we choose a new alphabet Γ as follows. For each state $q \in Q$ and each letter $a \in \Sigma$, if $\delta(q,a)$ is defined, then we introduce a letter $b_{q,a}$, i.e.,

$$\Gamma = \{b_{q,a} \mid q \in Q,\ a \in \Sigma \text{ such that } \delta(q,a) \text{ is defined}\}.$$

Further, we define a homomorphism $\alpha : \Gamma^* \to \Sigma^*$ through $b_{q,a} \mapsto r(q)a(r(\delta(q,a)))^{-1}$ for all $b_{q,a} \in \Gamma$. By Σ_U we denote the image $\alpha(\Gamma) \subset \Sigma^*$. We can establish the following properties for Σ_U.

Lemma 5.6 .

(a) $\Sigma_U \subset L(A)$.

(b) $\langle \Sigma_U \rangle = \langle U \rangle$, *i.e., for each* $u \in \langle U \rangle$, *there is some* $v \in \Gamma^*$ *such that* $u \xleftrightarrow{}^*_R \alpha(v)$.

Proof.
(a) Let $q \in Q$ and $a \in \Sigma$ be such that $\delta(q,a) = q_1 \in Q$. Then $b_{q,a} \in \Gamma$, and $\alpha(b_{q,a}) = r(q)a(r(\delta(q,a)))^{-1} \in \Sigma_U$. Now

$$\begin{aligned} \delta(q_0, r(q)a(r(\delta(q,a)))^{-1}) &= \delta(q_0, r(q)a(r(q_1))^{-1}) \\ &= \delta(q, a(r(q_1))^{-1}) \\ &= \delta(q_1, (r(q_1))^{-1}) \\ &= q_0, \end{aligned}$$

i.e., $\alpha(b_{q,a}) \in L(A)$. Thus, $\Sigma_U \subset L(A) \subseteq \langle U \rangle$.

(b) Let $u \in \langle U \rangle$. At the end of Section 4 we constructed a mapping $\sigma_1 : \langle U \rangle \to \Delta^*_R(U^*) \cap IRR(R)$ such that, for $w \in \langle U \rangle$, $w \xleftrightarrow{}^*_R \sigma_1(w)$. Since $\Delta^*_R(U^*) \subseteq L(A)$, we may thus assume without loss of generality that $u \in L(A)$.

We now describe a function $\tau : L(A) \to \Gamma^*$ such that, for all $u \in L(A)$, $u \xleftrightarrow{}^*_R \alpha(\tau(u))$. This will then prove our lemma. So let $u = a_1 \cdots a_m \in L(A)$, $a_1, \ldots, a_m \in \Sigma$. Since $u \in L(A)$, there is a path from q_0 to q_0 with label u. For $i = 1, \ldots, m-1$, let $q_i := \delta(q_0, a_1 \cdots a_i)$. Then $\delta(q_i, a_{i+1}) = q_{i+1}$ for all $i = 0, 1, \ldots, m-2$, and $\delta(q_{m-1}, a_m) = q_0$. Observe that this sequence of states is uniquely determined by u, since A is a deterministic finite-state acceptor. We define the word $\tau(u) \in \Gamma^*$ as follows:

$$\tau(u) := b_{q_0,a_1} b_{q_1,a_2} \cdots b_{q_{m-1},a_m}.$$

Then

$$\begin{aligned} \alpha(\tau(u)) &= \alpha(b_{q_0,a_1} b_{q_1,a_2} \cdots b_{q_{m-1},a_m}) \\ &= (r(q_0)a_1(r(q_1))^{-1}) \cdot (r(q_1)a_2(r(q_2))^{-1}) \cdots (r(q_{m-1})a_m(r(q_0))^{-1}) \\ &\xleftrightarrow{}^*_R a_1 a_2 \cdots a_m = u. \end{aligned}$$

□

Notice that the above function $\tau : L(A) \to \Gamma^*$ is computable in polynomial time. Further, by combining the three functions $\sigma_1 : \langle U \rangle \to L(A)$, $\tau : L(A) \to \Gamma^*$, and $\alpha : \Gamma^* \to \Sigma_U^*$ we can rewrite each word $u \in \langle U \rangle$ in polynomial time as a product of elements of Σ_U.

Finally, we define a string-rewriting system S on Γ. This system will consist of two subsystems S_1 and S_2, which are obtained as follows:

$$S_1 := \{b_{q,a} \rightarrow \lambda \mid q \in Q, a \in \Sigma \text{ satisfying } r(q)a \longleftrightarrow_R^* r(\delta(q,a))\}$$

and

$$S_2 := \{\tau_q(l) \rightarrow \tau_q(r) \mid (l \rightarrow r) \in R, q \in Q \text{ such that } \delta(q,l) \text{ is defined}\}.$$

Here, for $q \in Q$, τ_q is the partial mapping $\tau_q : \Sigma^* \hookrightarrow \Gamma^*$, which is defined as follows:

- $dom(\tau_q) = \{w \in \Sigma^* \mid \delta(q,w)$ is defined$\}$, and
- for $w = a_1 \cdots a_m \in dom(\tau_q)$, $(a_1, \ldots, a_m \in \Sigma)$, if $q_i := \delta(q, a_1 \cdots a_i)$, $i = 1, \ldots, m$, then $\tau_q(w) := b_{q,a_1} b_{q_1,a_2} \cdots b_{q_{m-1},a_m}$.

Thus, the mapping $\tau : L(A) \rightarrow \Gamma^*$ considered in the proof of the previous lemma is identical to the mapping τ_{q_0}. Obviously, $\mid \tau_q(w) \mid = \mid w \mid$ for all $q \in Q$ and all $w \in dom(\tau_q)$ Hence, $S := S_1 \cup S_2$ is a finite monadic string-rewriting system on Γ that is constructed in polynomial time from $\langle \Sigma; R \rangle$ and U.

If $b_{q,a} \in \Gamma$, then $\delta(q,a)$ is defined and $\delta(\delta(q,a),\bar{a}) = q$, i.e., $b_{p,\bar{a}} \in \Gamma$ as well, where $p = \delta(q,a)$. Since $(a\bar{a} \rightarrow \lambda) \in R$, this implies that $(\tau_q(a\bar{a}) \rightarrow \lambda) \in S_2$, i.e., $(b_{q,a} b_{p,\bar{a}} \rightarrow \lambda) \in S_2$, and analogously, $(b_{p,\bar{a}} b_{q,a} \rightarrow \lambda) \in S_2$. Thus, $\langle \Gamma; S \rangle$ is indeed a group-presentation. We claim that $\langle \Gamma; S \rangle$ is a presentation of the group $\langle U \rangle$. From the proof of Lemma 5.6 we already know that $\alpha : \Gamma^* \rightarrow \Sigma^*$ is a monoid-homomorphism from the free monoid Γ^* onto the subgroup $\langle U \rangle$ of M_R.

Lemma 5.7 . *For all $(u \rightarrow v) \in S$, $\alpha(u) \longleftrightarrow_R^* \alpha(v)$, i.e., α induces a homomorphism from the group M_S presented by $\langle \Gamma; S \rangle$ onto the group $\langle U \rangle$.*

Proof. Let $q \in Q$ and $a \in \Sigma$ be such that $\delta(q,a)$ is defined, and $r(q)a \longleftrightarrow_R^* r(\delta(q,a))$, i.e., $(b_{q,a} \rightarrow \lambda) \in S_1$. Then

$$\begin{array}{rcl} \alpha(b_{q,a}) & = & r(q)a(r(\delta(q,a)))^{-1} \\ & \longleftrightarrow_R^* & r(\delta(q,a)) \cdot (r(\delta(q,a)))^{-1} \\ & \longleftrightarrow_R^* & \lambda \\ & = & \alpha(\lambda). \end{array}$$

Now, let $q \in Q$ and $(l \rightarrow r) \in R$ be such that $\delta(q,l)$ is defined, i.e., $(\tau_q(l) \rightarrow \tau_q(r)) \in S_2$. From the construction of A we know that $\delta(q,l) = \delta(q,r)$. Suppose that $l = a_1 \cdots a_m$ $(a_1, \ldots, a_m \in \Sigma)$, and let $q_i := \delta(q, a_1 \cdots a_i)$, $i = 1, \ldots, m$. Then

$$\tau_q(l) = b_{q,a_1} b_{q_1,a_2} \cdots b_{q_{m-1},a_m},$$

and hence,

$$\begin{array}{rcl} \alpha(\tau_q(l)) & = & r(q)a_1(r(q_1))^{-1} \cdot r(q_1)a_2(r(q_2))^{-1} \cdots r(q_{m-1})a_m(r(q_m))^{-1} \\ & \longleftrightarrow_R^* & r(q)a_1 \cdots a_m(r(q_m))^{-1} \\ & = & r(q)l(r(q_m))^{-1} \\ & \longleftrightarrow_R & r(q)r(r(q_m))^{-1}. \end{array}$$

If $r = \lambda$, then $\tau_q(r) = \lambda$, and $q_m = \delta(q,l) = \delta(q,r) = \delta(q,\lambda) = q$ implying that

$$\alpha(\tau_q(l)) \longleftrightarrow_R^* r(q)r(r(q_m))^{-1} = r(q)(r(q))^{-1} \longleftrightarrow_R^* \lambda = \alpha(\tau_q(r)).$$

If $r \in \Sigma$, then $\tau_q(r) = b_{q,r}$, and

$$\alpha(\tau_q(r)) = \alpha(b_{q,r}) = r(q)r(r(\delta(q,r)))^{-1} = r(q)r(r(q_m))^{-1} \longleftrightarrow_R^* \alpha(\tau_q(l)).$$

This completes the proof of Lemma 5.7. □

It remains to show that the homomorphism $\alpha : M_S \to \langle U \rangle$ is injective. For this we need the following two technical lemmas.

Lemma 5.8 . *For all $u \in L(A)$, if $u \longrightarrow_R v$, then $\tau(u) \longrightarrow_{S_2} \tau(v)$.*

Proof. Let $u \in L(A)$ be such that $u \longrightarrow_R v$. Then $v \in L(A)$, and $u = xly \longrightarrow xry = v$ for some $x, y \in \Sigma^*$ and $(l \to r) \in R$. Since $u \in L(A)$, there are states $q_1, q_2 \in Q$ such that $\delta(q_0, x) = q_1$, $\delta(q_1, l) = q_2 = \delta(q_1, r)$, and $\delta(q_2, y) = q_0$. Hence, the rule $(\tau_{q_1}(l) \to \tau_{q_1}(r))$ belongs to S_2, and so

$$\tau(u) = \tau_{q_0}(x)\tau_{q_1}(l)\tau_{q_2}(y) \longrightarrow_S \tau_{q_0}(x)\tau_{q_1}(r)\tau_{q_2}(y) = \tau(v).$$

□

From Lemma 5.8 we immediately get the following consequence, since $\alpha(\Gamma^*) \subseteq L(A)$.

Corollary 5.9 . *For all $w \in \Gamma^*$, if $\alpha(w) \longleftrightarrow_R^* \lambda$, then $\tau(\alpha(w)) \longrightarrow_{S_2}^* \lambda$.*

Lemma 5.10 . *For all $b_{q,a} \in \Gamma$, $\tau(\alpha(b_{q,a})) \longrightarrow_{S_1}^* b_{q,a}$.*

Proof. Let $b_{q,a} \in \Gamma$, and let $p = \delta(q,a)$. Then $\alpha(b_{q,a}) = r(q)a(r(p))^{-1}$. Suppose that $r(q) = a_1 \cdots a_m$ and $(r(p))^{-1} = c_1 \cdots c_n$ $(a_i, c_j \in \Sigma)$. For $i = 1, \ldots, m-1$, let $q_i = \delta(q_0, a_1 \cdots a_i)$, and, for $j = 1, \ldots, n-1$, let $p_j = \delta(p, c_1 \cdots c_j)$. Then

$$\begin{aligned} \tau(\alpha(b_{q,a})) &= \tau(a_1 \cdots a_m a c_1 \cdots c_n) \\ &= b_{q_0,a_1} b_{q_1,a_2} \cdots b_{q_{m-1},a_m} \cdot b_{q,a} \cdot b_{p,c_1} \cdots b_{p_{n-1},c_n}. \end{aligned}$$

Since $r(q) = a_1 \cdots a_m \in REP$, we have $r(q_i) = a_1 \cdots a_i$, $i = 1, \ldots, m-1$, by Lemma 5.5. Hence, for each $i \in \{0, 1, \ldots, m-1\}$, $r(q_i)a_{i+1} = a_1 \cdots a_i a_{i+1} = r(q_{i+1})$ (where $q_m = q$), and therefore, $(b_{q_i,a_{i+1}} \to \lambda) \in S_1$ for all $i \in \{0, 1, \ldots, m-1\}$. Further, since $(r(p))^{-1} = c_1 \cdots c_n$, we have $r(p) = \bar{c}_n \cdots \bar{c}_1$. Again by Lemma 5.5 this gives $r(p_j) = \bar{c}_n \cdots \bar{c}_{j+1}$, $j = 1, \ldots, n-1$. Hence, for each $j \in \{0, 1, \ldots, n-1\}$, $r(p_j) = r(p_{j+1})\bar{c}_{j+1}$ (where $p = p_0$ and $q_0 = p_n$), and therefore, $r(p_j)c_{j+1} \longleftrightarrow_R^* r(p_{j+1}) = r(\delta(p_j, c_{j+1}))$ implying that $(b_{p_j,c_{j+1}} \to \lambda) \in S_1$ for all $j \in \{0, 1, \ldots, n-1\}$. Thus,

$$\tau(\alpha(b_{q,a})) = b_{q_0,a_1} b_{q_1,a_2} \cdots b_{q_{m-1},a_m} \cdot b_{q,a} \cdot b_{p,c_1} \cdots b_{p_{n-1},c_n} \longrightarrow_{S_1}^* b_{q,a}.$$

□

Combining Lemmas 5.7, 5.8, and 5.10 we can now derive the following result.

Theorem 5.11 . *$\langle \Gamma; S\rangle$ is a finite monadic presentation of the group $\langle U\rangle$.*

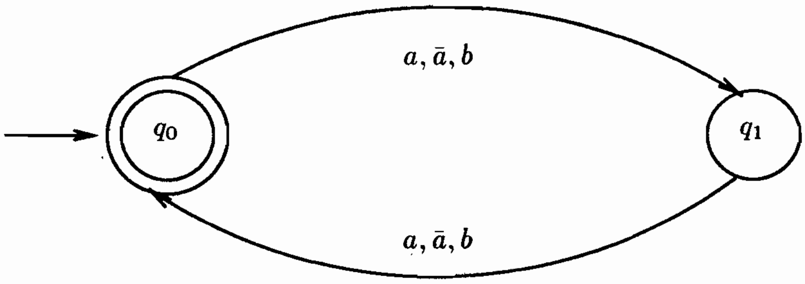
Proof. Because of Lemma 5.7 it remains to prove that, for all $w \in \Gamma^*$, if $\alpha(w) \longleftrightarrow^*_R \lambda$, then $w \longleftrightarrow^*_S \lambda$. So let $w \in \Gamma^*$ be such that $\alpha(w) \longleftrightarrow^*_R \lambda$. Then $\tau(\alpha(w)) \longrightarrow^*_{S_2} \lambda$ by Corollary 5.9, and by Lemma 5.10 $w \longleftarrow^*_{S_1} \tau(\alpha(w))$. Thus, $w \longleftrightarrow^*_S \lambda$, i.e., the homomorphism α from M_S onto $\langle U\rangle$ is injective, which means that $\langle \Gamma; S\rangle$ is in fact a presentation of the group $\langle U\rangle$. □

It is easily seen from the proof of Theorem 5.11 that the string-rewriting system S will in general not be λ-confluent. Thus, it remains to transform S into an equivalent finite monadic system that is λ-confluent. However, before continuing with this transformation, an example is in order. The following example is extremely simple; however, it suffices to illustrate the construction of a presentation for $\langle U\rangle$ described so far.

Example 5.12 . Let

$$\Sigma = \{a, \bar{a}, b\} \text{ and } R = \{a\bar{a} \to \lambda, \bar{a}a \to \lambda, b^2 \to \lambda, bab \to \bar{a}, b\bar{a}b \to a, aba \to b, \bar{a}b\bar{a} \to b\}.$$

Then R is a monadic and λ-confluent system, and hence, the group G presented by $\langle \Sigma; R\rangle$ is context-free. Let $U = \{a^2, ab, \bar{a}^2, b\bar{a}\}$. Using Construction 5.1 we get the following dfsa A:



By taking $a < \bar{a} < b$, we obtain $r(q_0) = \lambda$ and $r(q_1) = a$, and

$$\Gamma = \{b_{q_0,a}, b_{q_0,\bar{a}}, b_{q_0,b}, b_{q_1,a}, b_{q_1,\bar{a}}, b_{q_1,b}\}.$$

To simplify the notation we just write Γ as $\Gamma = \{b_1, b_2, b_3, b_4, b_5, b_6\}$. Further, we get

$$S_1 = \{b_1 \to \lambda, b_5 \to \lambda\},$$

and

$$\begin{aligned} S_2 = \{ & b_1b_5 \to \lambda, b_2b_4 \to \lambda, b_3b_6 \to \lambda, \\ & b_3b_4b_3 \to b_2, b_3b_5b_3 \to b_1, b_1b_6b_1 \to b_3, \\ & b_2b_6b_2 \to b_3, b_4b_2 \to \lambda, b_5b_1 \to \lambda, \\ & b_6b_3 \to \lambda, b_6b_1b_6 \to b_5, b_6b_2b_6 \to b_4, \\ & b_4b_3b_4 \to b_6, b_5b_3b_5 \to b_6\}. \end{aligned}$$

Thus, $\langle \Gamma; S_1 \cup S_2\rangle$ is a finite monadic presentation of $\langle U\rangle$, which, however, is not λ-confluent, since $b_6^2 \longleftrightarrow^*_S \lambda$, but b_6^2 is irreducible mod S. □

Let $\langle \Gamma; S\rangle$ be the presentation of the subgroup $\langle U\rangle$ constructed above. We define another string-rewriting system $\hat{S}$ on Γ by taking $\hat{S} := S \cup S_3$, where S_3 contains all the rules of the form $(x_1 \cdots x_m \to r)$ such that $x_1 \cdots x_m \neq \lambda$, and $(u_0 x_1 u_1 \cdots x_m u_m \to r) \in S_2$ for some $u_0, u_1, \ldots, u_m \in \Gamma^*$ satisfying $u_i \longrightarrow^*_{S_1} \lambda$, $i = 0, 1, \ldots, m$.

Lemma 5.13 . *The system $\hat{S}$ is equivalent to S, and $\hat{S}$ is λ-confluent.*

Proof. If $(uxv \to r) \in S_2$ and $x \longrightarrow^*_{S_1} \lambda$, then clearly $uv \longleftrightarrow^*_{S} r$. Thus, S and $\hat{S}$ are equivalent, i.e., they define the same Thue congruence on Γ^*.

To prove that $\hat{S}$ is λ-confluent, we need the following observation.

Claim. Let $(l \to b) \in S_2$ with $b \in \Gamma$. If $l \longrightarrow^*_{S_1} \lambda$, then $(b \to \lambda) \in S_1$.
Proof. If $l \longrightarrow^*_{S_1} \lambda$, then $b \longleftrightarrow^*_{S} \lambda$, and hence, $\alpha(b) = r(q)a(r(\delta(q,a)))^{-1} \longleftrightarrow^*_{R} \lambda$ by Lemma 5.7, where $b = b_{q,a}$ is taken. Thus, $r(q)a \longleftrightarrow^*_{R} r(\delta(q,a))$, which yields $(b \to \lambda) \in S_1$. □

Now let $w = b_1 \cdots b_m \in \Gamma^+$ be such that $w \longleftrightarrow^*_{S} \lambda$. Then

$$w = b_1 \cdots b_m \longleftarrow^*_{S_1} \tau(\alpha(w)) = u_0 b_1 u_1 \cdots b_m u_m \longrightarrow^*_{S_2} \lambda$$

for some words $u_0, u_1, \ldots, u_m \in \Gamma^*$ satisfying $u_i \longrightarrow^*_{S_1} \lambda$, $i = 0, 1, \ldots, m$ (cf. the proof of Theorem 5.11). If a rule $(\tilde{u}_{i-1} a_i u_i \cdots a_j u'_j \to r) \in S_2$ is applied to $\tau(\alpha(w))$, where $i \leq j$, $u_{i-1} = u'_{i-1}\tilde{u}_{i-1}$ and $u_j = u'_j \tilde{u}_j$, then the rule $(a_i \cdots a_j \to r)$ is in S_3. If a rule $(l \to r) \in S_2$ is applied within one of the factors u_i, then either $r = \lambda$ or $(r \to \lambda) \in S_1$ by the above claim, i.e., no letter b satisfying $b \not\longrightarrow_{S_1} \lambda$ is introduced here. Thus, using the appropriate rules of $S_2 \cup S_3$ we can construct a reduction $w \longrightarrow^*_{\hat{S}} \lambda$ that is essentially parallel to the reduction $\tau(\alpha(w)) \longrightarrow^*_{S_2} \lambda$. Hence, for all $w \in \Gamma^*$, if $w \longleftrightarrow^*_{\hat{S}} \lambda$, then $w \longrightarrow^*_{\hat{S}} \lambda$, i.e., $\hat{S}$ is indeed λ-confluent. □

The system $\hat{S}$ may not be noetherian, since it may contain "cycles" of the form

$$(b_1 \to b_2), (b_2 \to b_3), \ldots, (b_{m-1} \to b_m), (b_m \to b_1) \in \hat{S}$$

with $b_1, \ldots, b_m \in \Gamma$. For example, the system $\hat{S}$ obtained from the system S of Example 5.12 contains the rules $(b_3 \to b_6)$ and $(b_6 \to b_3)$. However, if $>$ is a fixed linear ordering on the alphabet Γ, then we can orient each rule of $\hat{S}$ according to the induced length-lexicographical ordering on Γ^*. If we also replace each letter b in the rules $(l \to r) \in \hat{S}$ with $\mid l \mid \geq 2$ by the smallest letter b' such that $b \longrightarrow^*_{\hat{S}} b'$, then the resulting finite monadic system $\hat{S}'$ is noetherian, and it is still λ-confluent.

A string-rewriting system T is called **normalized**, if, for each rule $(l \to r) \in T$, the right-hand side r is irreducible, and no rule from $T - \{l \to r\}$ is applicable to l. In [14] an algorithm *REDUCE-SYSTEM* is presented that, given a finite string-rewriting system T_1 on Σ and an admissible well-ordering $>$ on Σ^* as input such that $l > r$ holds for each rule $(l \to r) \in T_1$, constructs a finite normalized system T_2 that is equivalent to T_1, and that still satisfies $l > r$ for all its rules. In particular, if T_1 is monadic, then so is T_2, and if T_1 is λ-confluent presenting a group, then T_2 is also λ-confluent. Thus, we could apply the algorithm *REDUCE-SYSTEM* to the string-rewriting system $\hat{S}'$ using the fixed length-lexicographical ordering to obtain a finite, monadic, and λ-confluent system T such that T is normalized, and $\langle \Gamma; T\rangle$ is a presentation for the group $\langle U\rangle$. However, the steps leading from the system $S = S_1 \cup S_2$ to $\hat{S} = S \cup S_3$ to $\hat{S}'$ are already part of this algorithm. Thus, simply by fixing a linear ordering on Γ, and by applying the algorithm *REDUCE-SYSTEM* to the string-rewriting system S using the induced length-lexicographical ordering we obtain a system T in polynomial time that has all these properties. Hence, we have the following result.

Theorem 5.14 . *Given a finite group-presentation $\langle\Sigma; R\rangle$ such that R is monadic and λ-confluent, and a finite subset $U \subset \Sigma^*$, a group-presentation $\langle\Gamma; T\rangle$ for the subgroup $\langle U\rangle$ of M_R can be constructed in polynomial time such that T is monadic, normalized, and λ-confluent. In addition, we get a rewriting process $\tau : \langle U\rangle \to \Gamma^*$ that rewrites each word $u \in \langle U\rangle$ in polynomial time into a corresponding word in the new generators.*

We conclude with our example.

Example 5.12 *(continued).* Since $S_1 = \{b_1 \to \lambda, b_5 \to \lambda\}$, the algorithm *REDUCE-SYSTEM* applied to $S = S_1 \cup S_2$ yields the following system

$$\begin{aligned} T \;=\; & \{b_1 \to \lambda, b_5 \to \lambda, b_6 \to b_3, \\ & b_2b_4 \to \lambda, b_4b_2 \to \lambda, b_3^2 \to \lambda, \\ & b_3b_4b_3 \to b_2, b_3b_2b_3 \to b_4, \\ & b_2b_3b_2 \to b_3, b_4b_3b_4 \to b_3\} \end{aligned}$$

proving that M_R is isomorphic to its proper subgroup $\langle U\rangle$. □

6 Conclusion

The class of finitely presented polycyclic groups is exactly the class of groups that can be presented by finite (confluent) PCP2-presentations. Each finitely generated subgroup of such a group is itself polycyclic, and hence, it can also be presented by a group-presentation of this particular form. Exploiting results of [22] on the construction of prefix-rewriting systems that solve the generalized word problem in polycyclic groups, we have shown how to effectively derive a finite confluent PCP2-presentation for a finitely generated subgroup of a polycyclic group.

The class of context-free groups coincides with the class of groups that can be presented through finite, monadic, and λ-confluent group-presentations. Since each finitely generated subgroup of a context-free group is itself context-free, it can also be presented through a group-presentation of this particular form. Here we have described a construction that, given a finite, monadic, and λ-confluent group-presentation $\langle\Sigma; R\rangle$ and a finite subset $U \subset \Sigma^*$, yields a presentation of this very form for the subgroup $\langle U\rangle$ of M_R in polynomial time. This construction consists of three major steps:

1. From $\langle\Sigma; R\rangle$ and U, a dfsa $A = (Q, \Sigma, q_0, \delta, \{q_0\})$ is constructed such that $\Delta_R^*(U^*) \subseteq L(A) \subseteq \langle U\rangle$. Here the fact that the system R is monadic plays a crucial role.

2. From the dfsa A a finite monadic group-presentation $\langle\Gamma; S\rangle$ for the group $\langle U\rangle$ is obtained. This part is to a large extent the rewriting process of Reidemeister and Schreier. For it to work properly it is crucial that, for each letter $a \in \Sigma$, there exists an inverse of length one, i.e., that we have a group-presentation, and that the system R is λ-confluent.

3. Through the process of normalization we finally get a finite, monadic, and λ-confluent group-presentation $\langle\Gamma; T\rangle$ for $\langle U\rangle$ from $\langle\Gamma; S\rangle$. Here the fact that R is λ-confluent is again exploited.

Since the context-free groups are just the finite extensions of free groups, they can also be presented through finite string-rewriting systems that are noetherian and confluent [4]. Unfortunately, no syntactic characterization for those finite, noetherıan, and confluent systems that present context-free groups is known at this time; however, we do know that finite, length-reducing, and confluent systems do not suffice [15]. Accordingly, it is not known whether there is a general method to construct a finite, noetherian, and confluent presentation for $\langle U \rangle$ from the set U and a presentation of this form for a context-free group. However, in his doctoral dissertation Kuhn presents constructions of this form for certain classes of finite, length-reducing, and confluent presentations of groups [9].

A monadic string-rewriting system is called **two-monadic** if $| \ l \ | = 2$ holds for each rule $(l \rightarrow r)$. A group G can be presented by a finite, two-monadic, and confluent group-presentation if and only if G is a **plain** group, i.e., G is isomorphic to the free product of a free group of finite rank and finitely many finite groups [2]. The class of plain groups is also closed under taking finitely generated subgroups. Applied to a group-presentation of this form and a finite set U our construction yields a presentation of the same form for the subgroup $\langle U \rangle$. If we start with a finite, monadic, and (λ-) confluent monoid-presentation of a group G, i.e., if we do not have inverses of length one for all the given generators, then our construction can be adopted to still give a finite monadic presentation for the subgroup $\langle U \rangle$ generated by a given finite set U, but we have not yet found a way to always get a presentation for $\langle U \rangle$ that is (λ-) confluent. Only in case R is a confluent system that is **special**, i.e., each rule is of the form $(l \rightarrow \lambda)$, a presentation of the same form for $\langle U \rangle$ can always be obtained [9]. However, presentations of this form have just enough expressive power to present those groups that are isomorphic to free products of finitely many finite or infinite cyclic groups [7].

Finally, in [9] Kuhn describes a construction of a dfsa A for the set of descendants $\Delta_R^*(U^*)$ from a finite, length-reducing, and confluent group-presentation $\langle \Sigma; R \rangle$ and a finite set $U \subset \Sigma^*$. He proves that this construction terminates whenever the set $\Delta_R^*(U^*)$ is regular; however, it is still an open conjecture that the sets of this form are always regular in this setting. In case the construction terminates a finite length-reducing presentation for the subgroup $\langle U \rangle$ can be obtained from A as in our construction, but in general the process of normalization does not suffice to transform this presentation into a finite, length-reducing, and confluent one. Thus, with respect to the problem of constructing presentations of finitely generated subgroups, the class of finite, monadic, and λ-confluent group-presentations is particularly well-behaved.

7 References.

1. J. Autebert, L. Boasson, G. Senizergues; Groups and NTS languages; *Journal Computer System Sciences* 35 (1987) 243–267.

2. J. Avenhaus, K. Madlener; On groups defined by monadic Thue systems; in: *Algebra, Combinatorics and Logic in Computer Science*, Colloq. Math. Soc. Janos Bolyai 42 (Györ, 1983) 63–71.

3. J. Avenhaus, D. Wißmann; Using rewriting techniques to solve the generalized word problem in polycyclic groups; in: *Proceedings ISSAC'89*, 322–337.

4. G. Bauer; *Zur Darstellung von Monoiden durch konfluente Reduktionssysteme*, Doctoral dissertation (Fachbereich Informatik, Universität Kaiserslautern, 1981).

5. R.V. Book; Decidable sentences of Church-Rosser congruences; *Theoretical Computer Science* 23 (1983) 301–312.

6. R.V. Book, M. Jantzen, C. Wrathall; Monadic Thue systems; *Theoretical Computer Science* 19 (1982) 231–251.

7. Y. Cochet; Church-Rosser congruences on free semigroups; in: *Algebraic Theory of Semigroups*, Colloq. Math. Soc. Janos Bolyai 20 (North-Holland, Amsterdam, 1976) 51–60.

8. R.H. Gilman; Computations with rational subsets of confluent groups; in: J. Fitch (ed.), *Proceedings EUROSAM 84*, Lecture Notes in Computer Science 174 (Springer, Berlin, 1984) 207–212.

9. N. Kuhn; *Zur Entscheidbarkeit des Untergruppenproblems für Gruppen mit kanonischen Darstellungen*, Doctoral dissertation (Fachbereich Informatik, Universität Kaiserslautern, 1991).

10. N. Kuhn, K. Madlener; A method for enumerating cosets of a group presented by a canonical system; in: *Proceedings ISSAC'89*, 338–350.

11. N. Kuhn, K. Madlener, F. Otto; A test for λ-confluence for certain prefix rewriting systems with applications to the generalized word problem; in: *Proceedings ISSAC'90*, 8–15.

12. R. Lyndon, P. Schupp; *Combinatorial Group Theory* (Springer, Berlin, 1977).

13. K. Madlener, P. Narendran, F. Otto; A specialized completion procedure for monadic string-rewriting systems presenting groups; in: J.L. Albert, B. Monien, M.R. Artalejo (eds.), *Proceedings 18th ICALP*, Lecture Notes in Computer Science 510 (Springer, Berlin, 1991) 279–290.

14. K. Madlener, P. Narendran, F. Otto, L. Zhang; *On weakly confluent monadic string-rewriting systems*; Preprint No. 11/91 (Fachbereich Mathematik/Informatik, Gesamthochschule Kassel, 1991); also submitted for publication.

15. K. Madlener, F. Otto; About the descriptive power of certain classes of finite string-rewriting systems; *Theoretical Computer Science* 67 (1989) 143–172.

16. K. Madlener, F. Otto; Decidable sentences for context-free groups; in: C. Choffrut, M. Jantzen (eds.); *Proceedings STACS'91*, Lecture Notes in Computer Science 480 (Springer, Berlin, 1991) 160–171.

17. W. Magnus, A. Karrass, D. Solitar; *Combinatorial Group Theory* (Wiley-Interscience, New York, 1966).

18. C.F. Miller III; *On group-theoretic decision problems and their classification*, Annals of Math. Studies 68 (Princeton University Press, Princeton, 1971).

19. D.E. Muller, P.E. Schupp; Groups, the theory of ends and context-free languages; *Journal Computer System Sciences* 26 (1983) 295–310.

20. F. Otto; On deciding whether a monoid is a free monoid or is a group; *Acta Informatica* 23 (1986) 99–110.

21. F. Otto; Some undecidability results for weakly confluent monadic string-rewriting systems; in: H.F. Mattson, T. Mora, T.R.N. Rao (eds.); *Proceedings AAECC-9*, Lecture Notes in Computer Science 539 (Springer, Berlin, 1991) 292–303.

22. D. Wißmann; *Anwendung von Rewriting-Techniken in polyzyklischen Gruppen*, Doctoral dissertation (Fachbereich Informatik, Universität Kaiserslautern, 1989).