Algorithmic Problems on Inverse Monoids over Virtually-Free Groups

Volker Diekert, Markus Lohrey, and Nicole Ondrusch
Institut für Formale Methoden der Informatik (FMI),
Universität Stuttgart,
Universitätsstr. 38
D-70569 Stuttgart, Germany
{*diekert,lohrey,ondrusch*}*@fmi.uni-stuttgart.de*

Received (Day Month Year)
Revised (Day Month Year)

Communicated by [editor]

Let G be a finitely generated virtually-free group. We consider the Birget-Rhodes expansion of G, which yields an inverse monoid and which is denoted by $\mathrm{IM}(G)$ in the following. We show that for a finite idempotent presentation P, the word problem of a quotient monoid $\mathrm{IM}(G)/P$ can be solved in linear time on a RAM. The uniform word problem, where G and the presentation P are also part of the input, is EXPTIME-complete. With $\mathrm{IM}(G)/P$ we associate a relational structure, which contains for every rational subset L of $\mathrm{IM}(G)/P$ a binary relation, consisting of all pairs (x, y) such that y can be obtained from x by right multiplication with an element from L. We prove that the first-order theory of this structure is decidable. This result implies that the emptiness problem for boolean combinations of rational subsets of $\mathrm{IM}(G)/P$ is decidable, which, in turn implies the decidability of the submonoid membership problem of $\mathrm{IM}(G)/P$. These results were known previously for free groups, only. Moreover, we provide a new algorithmic approach for these problems, which seems to be of independent interest even for free groups.

We also show that one cannot expect decidability results in much larger frameworks than virtually-free groups because the subgroup membership problem of a subgroup H in an arbitrary group G can be reduced to a word problem of some $\mathrm{IM}(G)/P$, where P depends only on H. A consequence is that there is a hyperbolic group G and a finite idempotent presentation P such that the word problem is undecidable for some finitely generated submonoid of $\mathrm{IM}(G)/P$. In particular, the word problem of $\mathrm{IM}(G)/P$ is undecidable.

1. Introduction

Decidability and complexity questions concerning word problems for monoids are a classical topic in the interplay between logic, algebra, and complexity theory.

In this paper, we are interested in the class of inverse monoids. In the same way as groups can be represented by groups of permutations, inverse monoids can be represented by monoids of partial injections, see e.g. [21]. Algorithmic questions for inverse monoids have received increasing attention over the past few years, and inverse monoid theory has led to applications in combinatorial group theory, see e.g. [2,5,6,14,17,24,26,27]. Let us also refer to the survey [15].

Here, we will deal mainly with inverse monoids that are defined by the Birget-Rhodes expansion over a group G, see [3,4]. This expansion associates to G an inverse monoid

$\mathrm{IM}(G)$, where the elements are pairs of the form (U, g) such that U is a finite subset of G with $1, g \in U$. Multiplication is defined by the rule $(U, g)(V, h) = (U \cup gV, gh)$. The monoid $\mathrm{IM}(G)$ is denoted by $\widetilde{G}^{\mathcal{R}}$ in [3,4].

In fact, we take a slightly more general starting point where we consider pairs (U, g) such that U is a finite subset of a set $\mathcal{G}$ where G acts on the left. This more general viewpoint is more flexible and is done to have a basis to cope with the Margolis-Meakin expansion [13] as well, see below. We also refer to [28,9] for more background, which show that these constructions are not arbitrary, but play an important role in the theory of inverse monoids.

In Section 6.2 we consider quotient monoids of the form $\mathrm{IM}(G)/P$ where G is a finitely generated virtually-free group (i.e., G has a finitely generated free subgroup of finite index) and P is a finite set of equations between idempotent elements of $\mathrm{IM}(G)$. We call P a *finite idempotent presentation*. We prove that the word problem of $\mathrm{IM}(G)/P$ can be solved in linear time on a random access machine (RAM). In the case where F is a finitely generated free group, the decidability of the word problem of $\mathrm{IM}(F)/P$ has been shown by Margolis and Meakin in [14] by a reduction to the monadic second-order theory of the full infinite binary tree. This theory is decidable by Rabin's tree theorem [22], but its complexity is non-elementary. Hence, the approach from [14] results in a non-elementary algorithm for the word problem. An alternative proof using finite automata for the decidability of the word problem has been given in [26], but without any complexity bound. Using tree automata, it has been shown in [11] that the word problem of $\mathrm{IM}(F)/P$ (with F a free group, again) can be solved in polynomial time. In fact, after having announced the results in the present paper the authors of [11] observed that their techniques yield a linear time algorithm in the case of free groups on a RAM, too.

The algorithm presented here has at least two advantages: First, it is more general, since we may assume without any difficulty that G is a virtually-free group, and second, it yields a direct algorithm for the word problem. This second point is the primary focus in this paper. In contrast, in [11] the word problem is solved by translating via Rabin's tree theorem a fixed monadic second-order formula (which only depends on the fixed idempotent presentation P) into a fixed tree automaton. The tree automaton runs in linear time on a tree constructed from the input. Hence, the existence of a linear time algorithm is ensured, but the algorithm is not actually provided. It is hard to imagine that anybody will ever write a code for an actual implementation which runs through all these steps. Our algorithm uses simple data structures over the group, only, and an actual implementation is fairly easy.

If the idempotent presentation P is part of the input, then our algorithm has an exponential running time in the worst-case. This is unavoidable: In [11] it has been shown for free groups F that the uniform word problem for monoids of the form $\mathrm{IM}(F)/P$ is EXPTIME-complete.

For the case that G is not a virtually-free group, it turns out that the word problem of $\mathrm{IM}(G)/P$ might be undecidable, even if the word problem of G is easy. We show that the subgroup membership problem of a subgroup H in an arbitrary group G can be reduced to a word problem of some $\mathrm{IM}(G)/P$, where P depends only on H. Thus in general, the word problem of $\mathrm{IM}(G)/P$ is undecidable for hyperbolic groups, by a result of Rips [23]. In fact, we can construct a finitely generated submonoid of $\mathrm{IM}(G)/P$ where the word problem is undecidable.

The Birget-Rhodes expansion is quite similar to a construction of Margolis and Meakin [13,14]. Margolis and Meakin associate with a group G and a generating set Σ for G a monoid $M(G,\Sigma)$. The elements of $M(G,\Sigma)$ are pairs of the form (U,g), where U is a finite and connected subgraph of the Cayley graph $\mathcal{C}(G,\Sigma)$ of G with respect to Σ, which contains 1 and g. Multiplication of two such pairs is again defined by the rule $(U,g)(V,h) = (U \cup gV, gh)$. Here one has to notice that the group G acts freely on the Cayley graph $\mathcal{C}(G,\Sigma)$ by left multiplication.[a] This construction can be again generalized by giving up the restriction to connected subgraphs of the Cayley graph $\mathcal{C}(G,\Sigma)$. This results in an inverse monoid $\mathrm{SG}(G,\Sigma)$ (SG for subgraph). It turns out that our linear time solution of the word problem of $\mathrm{IM}(G)/P$ can be carried over to $\mathrm{SG}(G,\Sigma)/P$. However, in order to avoid an overload in technical notations we do not work out the details, see Section 6.6.

In Section 7 we associate with the monoid $\mathrm{IM}(G)/P$ a relational structure $\mathsf{R}(\mathrm{IM}(G)/P)$, which contains for every rational subset $L \subseteq \mathrm{IM}(G)/P$ a binary relation, consisting of all pairs (x,y) such that y can be obtained from x by right multiplication with an element from L. We prove that the first-order theory of this structure is decidable. As for the word problem, this result generalizes a corresponding result from [11] for free groups. We reduce the first-order theory of $\mathsf{R}(\mathrm{IM}(G)/P)$ to the monadic second-order theory of the Cayley graph of G with respect to some generating set of G. By a result of Muller and Schupp [19] this latter theory is decidable when G is virtually-free.

Our motivation for investigating the first-order theory of $\mathsf{R}(\mathrm{IM}(G)/P)$ is the fact that various algorithmic questions concerning rational subsets of $\mathrm{IM}(G)/P$, like for instance the emptiness problem for boolean combinations of rational sets or the submonoid membership problem, can be reduced to the first-order theory of $\mathsf{R}(\mathrm{IM}(G)/P)$. Hence, for a virtually free group G, these problems are decidable.

2. Inverse Monoids

Let M be a monoid and let M^* be the free monoid over the set M.

The *word problem* of M is the computational problem, which asks for two given words $u,v \in M^*$ whether $\pi(u) = \pi(v)$, where $\pi : M^* \to M$ is the canonical morphism. Here, one needs some finite description of elements of M; in particular, M has to be countable. In our paper these requirements will be fulfilled.

A monoid M is called an *inverse monoid*, if for every $x \in M$ there exists a unique element $x^{-1} \in M$ such that:

$$xx^{-1}x = x$$
$$x^{-1}xx^{-1} = x^{-1}$$

By Σ we denote a finite alphabet and we let $\Sigma^{-1} = \{a^{-1} \mid a \in \Sigma\}$ be a copy of Σ. By

[a] A group G acts freely on a set X, if for all $x \in X$ and $g \in G$, $gx = x$ implies $g = 1$.

Γ we denote the disjoint union of Σ and Σ^{-1}. Define $(a^{-1})^{-1} = a$; thus, $^{-1}$ becomes an involution on the alphabet Γ. We extend this involution to words from Γ^* by setting $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ for $a_1, \ldots, a_n \in \Gamma$.

Consider the free monoid Γ^* modulo the following defining equations (also called the *Vagner equations*):

$$xx^{-1}x = x$$
$$xx^{-1}yy^{-1} = yy^{-1}xx^{-1}$$

The quotient monoid of Γ^* modulo the Vagner equations for all $x, y \in \Gamma^*$ is an inverse monoid. Actually, it is the *free inverse monoid* generated by Σ. This observation involves a little computation, which can be found e.g. in the textbook [21] (as well as the following facts).

Remark 1.

(1) The idempotents of an inverse monoid (i.e., the elements e satisfying $e^2 = e$) are exactly the elements of the form xx^{-1}, and idempotents commute.
(2) For every set $\mathcal{G}$, its monoid of partially defined injections from $\mathcal{G}$ to $\mathcal{G}$ forms an inverse monoid; and vice versa: If M is any inverse monoid, then we can realize M as a submonoid of the monoid of partially defined injections from M to M.

Given an inverse monoid M, the quotient of M modulo the equations $xx^{-1} = 1$ is a group. It is the *maximal group image* of M, since every homomorphism from M to a group factorizes through this quotient. An inverse monoid is called *E-unitary*, if only idempotents are mapped to the identity of the maximal group image.

As an example consider the following construction. Let G be group with a left-action on a (non-empty) set $\mathcal{G}$, i.e., there is a mapping $\cdot : G \times \mathcal{G} \to \mathcal{G}$ with $1 \cdot x = x$ and $g \cdot (h \cdot x) = gh \cdot x$ for $g, h \in G$ and $x \in \mathcal{G}$. For $g \cdot x$ we will also write gx. For $g \in G$ and a finite set $U \subseteq \mathcal{G}$ we can define a partial injection $\iota_{(U,g)}$ as follows:

$$\iota_{(U,g)} : \mathcal{G} \setminus U \to \mathcal{G}, \quad x \mapsto g^{-1}x.$$

Thus, this injection is defined almost everywhere. The set of all partial injections of type $\iota_{(U,g)}$ forms an inverse monoid, because it is a submonoid in the monoid of partially defined injections from $\mathcal{G}$ to $\mathcal{G}$. A direct verification shows that multiplication is defined by

$$\iota_{(U,g)} \circ \iota_{(V,h)} = \iota_{(U \cup gV, gh)}. \tag{2}$$

Note that $\iota_{(U,g)} = \iota_{(V,h)}$ does not imply $g = h$ in general. However, in all cases of interest in this paper, G is an infinite group acting freely on the set $\mathcal{G}$. Then, $\iota_{(U,g)} = \iota_{(V,h)}$ implies $g = h$ and we obtain an E-unitary monoid. For the interested reader we state that the monoid of these $\iota_{(U,g)}$ is E-unitary if and only if for all $g \in G$ the set $\{ x \in \mathcal{G} \mid gx \neq x \}$ is either empty or infinite. In particular, if $\mathcal{G}$ is finite, but G acts non-trivially, then the the monoid is not E-unitary. Note that for a finite set $\mathcal{G}$ the empty function becomes part of this monoid, but this function behaves as a *zero*, so the maximal group image is trivial.

3. The inverse monoid $\mathrm{IM}(\mathcal{G})$

The starting point for our construction is guided by the example above: G is a group with a left-action on a non-empty set $\mathcal{G}$, moreover we fix an element $* \in \mathcal{G}$. Henceforth $\mathcal{G}$ is viewed as a pointed set. By slight abuse of language we write g as a shorthand for $g* \in \mathcal{G}$. Thus, depending on the context, g denotes either an element in the group G or in the set $\mathcal{G}$. But there will be no risk of confusion. In our applications $\mathcal{G}$ is just the vertex set of the Cayley graph of G and then $\mathcal{G} = G$.

We give a monoid structure to the set of pairs (U, g), where U is a finite subset of $\mathcal{G}$ and $g \in G$. The multiplication is defined in analogy to equation (2):

$$(U, g)(V, h) = (U \cup gV, gh).$$

Note that in this setting $(U, g) = (V, h)$ implies both, $U = V$ and $g = h$. Associativity of this operation and the Vagner equations can be verified easily by defining $(U, g)^{-1} = (g^{-1}U, g^{-1})$. The idempotents in this monoid are of the form $(U, 1)$. Thus, we have defined an inverse monoid where its maximal group image is G and the monoid is in fact E-unitary, because only idempotents become the identity in the maximal group image.

We use the point $* \in \mathcal{G}$ for the *localization* at the idempotent $(\{*\}, 1)$. This means that we are considering the subsemigroup of elements of the form

$$(\{*\}, 1)(U, g)(\{*\}, 1) = (U \cup \{ *, g* \}, g).$$

The localization has the effect that we always have $*, g* \in U$ for all elements (U, g) in the localization. According to our convention (to read $1, g \in U$ as $*, g* \in U$) we can also simply write $1, g \in U$. The localization yields an inverse monoid which we denote by $\mathrm{IM}(\mathcal{G})$. Note however that the monoid depends also on the element $*$.

We repeat: elements of $\mathrm{IM}(\mathcal{G})$ are pairs (U, g), where $U \subseteq \mathcal{G}$ is finite and $1,\ g \in U$. The neutral element is $(\{ 1 \}, 1)$. The inverse of (U, g) is $(g^{-1}U, g^{-1})$, and the idempotents are the pairs $(U, 1)$ with $1 \in U$.

If $\mathcal{G}$ is infinite and if G acts freely on $\mathcal{G}$, then (U, g) can be identified with the partial injection $\iota_{(U,g)}$ (where $1, g \in U$) as defined above. In particular, the inverse monoid $\mathrm{IM}(\mathcal{G})$ has a natural representation as monoid of partially defined functions over $\mathcal{G}$, and not only over the set $\mathrm{IM}(\mathcal{G})$ itself.

For the interested reader we add the following remark:

Remark 2. The inverse monoid $\mathrm{IM}(\mathcal{G})$ is E-unitary. Actually, it is an F-inverse monoid, which is a stronger assertion, see e.g. [16]: It is F-inverse, because every $(U, g) \in \mathrm{IM}(\mathcal{G})$ admits a canonical decomposition $(U, g) = (\{1, g\}, g)(g^{-1}U, 1)$ where $(g^{-1}U, 1)$ is idempotent and $(\{1, g\}, g)$ is the *greatest* element having the same image in the maximal group image as (U, g). It is the greatest element with respect to the natural order, which is defined for inverse monoids by letting $s \leq t$, if $s = te$ for some idempotent e.

Assume that the group G is generated by Σ. Then $\mathcal{G}$ becomes the vertex set of a directed graph with a distinguished vertex 1 and labeled directed edges (x, a, ax) with $x \in \mathcal{G}$ and $a \in \Sigma$. Thus, we can speak of connected subsets of $\mathcal{G}$. By $\mathrm{IM}(\mathcal{G}, \Sigma)$ we mean the inverse submonoid of $\mathrm{IM}(\mathcal{G})$ generated by the elements $(\{1, a\}, a)$ with $a \in \Sigma$. It is also the submonoid of $\mathrm{IM}(\mathcal{G})$ generated by the set $\{ (\{1, a\}, a) \mid a \in \Gamma \}$, where $\Gamma = \Sigma \cup \Sigma^{-1}$. Note that $(U, g) \in \mathrm{IM}(\mathcal{G}, \Sigma)$ implies that U is connected.

The above construction is very much in the spirit of a construction given by Birget and Rhodes [3,4]. We therefore call $\mathrm{IM}(\mathcal{G})$ the *Birget-Rhodes expansion* of $\mathcal{G}$. In fact, Birget and Rhodes consider $\mathcal{G} = G$ with its natural left-action and they denote the monoid $\mathrm{IM}(G)$ by $\widetilde{G}^{\mathcal{R}}$. For a given generating set Σ of G, Birget and Rhodes also consider the submonoid $\mathrm{IM}(G, \Sigma)$ (denoted by $\widetilde{G}^{\mathcal{R}}_{\Sigma}$ in [4] and called the cut-down of $\widetilde{G}^{\mathcal{R}}$ to Σ) generated by the pairs $(\{1, a\}, a)$ with $a \in \Gamma = \Sigma \cup \Sigma^{-1}$. If Σ is finite, then $\mathrm{IM}(G, \Sigma)$ is finitely generated. Clearly, for generating sets Σ_1, Σ_2 of G we have

$$\mathrm{IM}(G, \Sigma_1) \subseteq \mathrm{IM}(G, \Sigma_1 \cup \Sigma_2) \subseteq \mathrm{IM}(G).$$

If F is the free group generated by Σ, then $\mathrm{IM}(F, \Sigma)$ is the free inverse monoid generated by Σ, see [4,20].

The geometrical interpretation of $\mathrm{IM}(G, \Sigma)$ refers to the set of all pairs (U, g), where $1, g \in U$ and U is a finite and connected subset of the *Cayley graph* $\mathcal{C}(G, \Sigma)$ of G with respect to the set Σ, which is the directed graph

$$\mathcal{C}(G, \Sigma) = \left(G, \{ (g, h) \in G \times G \mid g^{-1}h \in \Sigma \}\right).$$

Note that an edge (g, h) can be labeled by $a = g^{-1}h \in \Sigma$ and it is no harm to imagine that for each edge (g, h) we have an implicit edge (h, g) labeled by $a^{-1} = h^{-1}g \in \Sigma^{-1}$.

Whether or not the word problem of $\mathrm{IM}(\mathcal{G})$ is decidable depends on $\mathcal{G}$ and G. It is clear however that the word problem of G is reducible to the word problem of $\mathrm{IM}(\mathcal{G})$; more precisely, it is reducible to the word problem of $\mathrm{IM}(\mathcal{G}, \Sigma)$. Indeed, let $g \in G$ be given by a word $a_1 \cdots a_n$ with $a_i \in \Gamma$. Then we have $g = 1$ in G if and only if $(U, g)(U, g) = (U, g)$, where $U = \{ a_1 \cdots a_i \mid 0 \le i \le n \}$. For the other way round, if G has a decidable word problem and if the presentation of the set $\mathcal{G}$ as well as the group action $\cdot : G \times \mathcal{G} \to \mathcal{G}$ is effective, then the word problem of $\mathrm{IM}(\mathcal{G})$ is decidable, too.

4. Finite idempotent presentations

An idempotent presentation P over $\mathrm{IM}(\mathcal{G})$ is given by a set of pairs (e, e') where $e = (E, 1)$ and $e' = (E', 1)$ are idempotents of $\mathrm{IM}(\mathcal{G})$. This defines a quotient monoid $\mathrm{IM}(\mathcal{G})/P$, where $e = e'$ are the defining relations over $\mathrm{IM}(\mathcal{G})$ for all $(e, e') \in P$. The maximal group image of $\mathrm{IM}(\mathcal{G})/P$ is still the group G. Thus, for a generating set Σ of G (and the choice of $* \in \mathcal{G}$) we obtain a sequence of canonical homomorphisms:

$$\Sigma^* \to (\Sigma \cup \Sigma^{-1})^* \to \mathrm{IM}(\mathcal{G}, \Sigma) \to \mathrm{IM}(\mathcal{G}) \to \mathrm{IM}(\mathcal{G})/P \to G.$$

4.1. *Confluent Rewriting over finite subsets*

In inverse monoids an equation $e = e'$ between idempotents is equivalent to the two equations $e = ee'$ and $e' = ee'$. Since idempotents commute in an inverse monoid, ee' is idempotent, too. Let $P \subseteq \mathrm{IM}(\mathcal{G}) \times \mathrm{IM}(\mathcal{G})$, where e and e' are idempotents for all $(e, e') \in P$. Thus, if P is a set of defining equations between idempotents we may assume that all elements of P have the form (e, ee').

In our context this means that $((E,1),(E',1)) \in P$ implies $E \subseteq E'$. Instead of writing $((E,1),(E',1)) \in P$ we simply write $(E,E') \in P$ henceforth, and we assume that $1 \in E \subseteq E'$.

The assumption $E \subseteq E'$ leads to a natural rewrite relation $\underset{P}{\Longrightarrow}$ over finite subsets of $\mathcal{G}$: For $U, U' \subseteq \mathcal{G}$ finite we define $U \underset{P}{\Longrightarrow} U'$, if there is some $g \in G$ and $(E,E') \in P$ with $gE \subseteq U$ and $U' = U \cup gE'$. By $\overset{*}{\underset{P}{\Longleftrightarrow}}$ we denote as usual the reflexive, symmetric, and transitive closure of the one-step rewrite relation $\underset{P}{\Longrightarrow}$. We have the following:

Lemma 3. *Let $U, U' \subseteq \mathcal{G}$, and $f, f' \in G$ with $1, f \in U$, $1, f' \in U'$. Let P be an idempotent presentation over $\mathrm{IM}(\mathcal{G})$. Then the following two assertions are equivalent:*

(a) $(U,f) = (U',f')$ *in* $\mathrm{IM}(\mathcal{G})/P$.
(b) $U \overset{*}{\underset{P}{\Longleftrightarrow}} U'$ *and* $f = f'$.

Proof. For $(a) \Rightarrow (b)$ assume that $(U,f) = (X,g)(E,1)(Y,h)$ and $(U',f') = (X,g)(E',1)(Y,h)$ for some $(E,E') \in P$. Clearly, $f = gh = f'$. Moreover, $U = X \cup gE \cup gY$ and $U' = X \cup gE' \cup gY$. In particular, $gE \subseteq U$ and $U' = U \cup gE'$. Hence $U \underset{P}{\Longrightarrow} U'$.

For $(b) \Rightarrow (a)$ assume that $U \underset{P}{\Longrightarrow} U'$. Then $gE \subseteq U$ and $U' = U \cup gE'$ for some $g \in G$ and $(E,E') \in P$. Since $1 \in E$ implies $g \in U$ we obtain

$$(U,f) = (U,g)(E,1)(g^{-1}U, g^{-1}f),$$

and

$$(U',f) = (U,g)(E',1)(g^{-1}U, g^{-1}f).$$

Hence $(U,f) = (U',f)$ in $\mathrm{IM}(\mathcal{G})/P$. $\square$

It turns out that the system $\underset{P}{\Longrightarrow}$ is strongly confluent. This means that whenever

$$U' \underset{P}{\Longleftarrow} U \underset{P}{\Longrightarrow} U'',$$

then there exists some $V \subseteq \mathcal{G}$ with

$$U' \underset{P}{\Longrightarrow} V \underset{P}{\Longleftarrow} U''.$$

Indeed it suffices to take $V = U' \cup U''$ and the result is immediate. Now strong confluence implies confluence [1], hence $U \overset{*}{\underset{P}{\Longleftrightarrow}} U'$ is equivalent to the existence of some V such that both $U \overset{*}{\underset{P}{\Longrightarrow}} V$ and $U' \overset{*}{\underset{P}{\Longrightarrow}} V$, where $\overset{*}{\underset{P}{\Longrightarrow}}$ denotes the reflexive and transitive closure of $\underset{P}{\Longrightarrow}$.

Lemma 4. *Let $U, U' \subseteq \mathcal{G}$. Then $U \overset{*}{\underset{P}{\Longleftrightarrow}} U'$ is equivalent to the following two conditions:*

(a) $\exists V : U \overset{*}{\underset{P}{\Longrightarrow}} V$ *and* $U' \subseteq V$.

(b) $\exists V' : U' \overset{*}{\underset{P}{\Longrightarrow}} V'$ *and* $U \subseteq V'$.

Proof. If $U \overset{*}{\underset{P}{\Longleftrightarrow}} U'$, then (a) and (b) hold due to confluence of the system $\underset{P}{\Longrightarrow}$.

Conversely, if (a) and (b) hold with V and V', then we have $U \overset{*}{\underset{P}{\Longrightarrow}} V \overset{*}{\underset{P}{\Longrightarrow}} V \cup V'$ due to $U' \subseteq V$. By symmetry we have $U' \overset{*}{\underset{P}{\Longrightarrow}} V' \overset{*}{\underset{P}{\Longrightarrow}} V \cup V'$, and hence $U \overset{*}{\underset{P}{\Longleftrightarrow}} U'$. □

Remark 5. Due to Lemmas 3 and 4 it is enough to focus on the following problem in order to solve the word problem for $\mathrm{IM}(\mathcal{G})/P$: Let P be a finite list of pairs (E, E') with $1 \in E \subseteq E' \subseteq \mathcal{G}$ and E, E' are finite. Decide for two given finite subsets $U, U' \subseteq \mathcal{G}$ whether there exists some $V \subseteq \mathcal{G}$ such that $U \overset{*}{\underset{P}{\Longrightarrow}} V$ and $U' \subseteq V$.

If $P \subseteq \mathrm{IM}(\mathcal{G}, \Sigma) \times \mathrm{IM}(\mathcal{G}, \Sigma)$, then we might consider the quotient monoid $\mathrm{IM}(\mathcal{G}, \Sigma)/P$, too. However, the inclusion $\mathrm{IM}(\mathcal{G}, \Sigma) \subseteq \mathrm{IM}(\mathcal{G})$ defines a canonical embedding $\mathrm{IM}(\mathcal{G}, \Sigma)/P \hookrightarrow \mathrm{IM}(\mathcal{G})/P$: Indeed, let $(U, g), (U', g) \in \mathrm{IM}(\mathcal{G}, \Sigma)$ such that $(U, g) = (U', g)$ in $\mathrm{IM}(\mathcal{G})/P$. Thus, there exists a finite $V \subseteq \mathcal{G}$ with $U \overset{*}{\underset{P}{\Longrightarrow}} V$ and $U' \overset{*}{\underset{P}{\Longrightarrow}} V$. Since U, U' and all sets occurring in P are connected, it follows that every subset, which appears in the derivation $U \overset{*}{\underset{P}{\Longrightarrow}} V$ or $U' \overset{*}{\underset{P}{\Longrightarrow}} V$ has to be connected, too. This implies $(U, g) = (U', g)$ in $\mathrm{IM}(\mathcal{G}, \Sigma)/P$. It follows that the word problem of $\mathrm{IM}(\mathcal{G}, \Sigma)/P$ can be directly reduced to the word problem of $\mathrm{IM}(\mathcal{G})/P$ and issues like connectedness do not play a central role anymore. Therefore we focus our intention on $\mathrm{IM}(\mathcal{G})/P$, rather than $\mathrm{IM}(\mathcal{G}, \Sigma)/P$.

Moreover, basically we are interested in $\mathcal{G} = G$, and for $\mathcal{G} = G$ the word problem of $\mathrm{IM}(G)/P$ can be stated as a word problem of $\mathrm{IM}(G, \Sigma)/P$ for some Σ as follows: Let $(U, g), (V, h) \in \mathrm{IM}(G)$ be given. Choose a generating set Σ for G which contains U, V, and all $E \cup E'$ with $((E, 1), (E', 1)) \in P$. (If G is finitely generated and P is finite, then Σ can be chosen to be finite.) Then, U and V are connected in $\mathcal{C}(G, \Sigma)$, i.e., $(U, g), (V, h) \in \mathrm{IM}(G, \Sigma)$. Thus, $(U, g) = (V, h)$ in $\mathrm{IM}(G)/P$ if and only if $(U, g) = (V, h)$ in $\mathrm{IM}(G, \Sigma)/P$.

Let us finish this section with another concept which is a main tool for the rest of the paper: For a subset W of the group G define the one-step rewrite relation $\underset{P,W}{\Longrightarrow}$ with $U \underset{P,W}{\Longrightarrow} U'$ for $U, U' \subseteq \mathcal{G}$ if there is some $g \in W$ and $(E, E') \in P$ such that $gE \subseteq U$ and $U' = U \cup gE'$. Note that $\underset{P,W}{\Longrightarrow}$ is a subset of $\underset{P}{\Longrightarrow}$. More precisely, we have:

$$\begin{aligned} \underset{P,W}{\Longrightarrow} \quad &\subseteq \quad \underset{P,W'}{\Longrightarrow} \quad \text{if } W \subseteq W', \text{ and} \\ \underset{P,G}{\Longrightarrow} \quad &= \quad \underset{P}{\Longrightarrow}\,. \end{aligned}$$

The relation $\underset{P,W}{\Longrightarrow}$ is still strongly confluent, but if W and P are finite, then in addition $\underset{P,W}{\Longrightarrow}$ is terminating in the sense that every chain $U \overset{*}{\underset{P,W}{\Longrightarrow}} U_1 \overset{*}{\underset{P,W}{\Longrightarrow}} U_2 \overset{*}{\underset{P,W}{\Longrightarrow}} \cdots$ becomes stationary.

This is clear because $U \subseteq U_i \subseteq U_{i+1}$ for all i. Hence every U_i in this chain is a subset of the finite set

$$U \cup \bigcup_{g \in W, (E,E') \in P} gE'.$$

Therefore, for finite sets U and W there is a unique finite subset $\widehat{U} \subseteq \mathcal{G}$ such that (i) $U \underset{P,W}{\overset{*}{\Longrightarrow}} \widehat{U}$ and (ii) $U \underset{P,W}{\overset{*}{\Longrightarrow}} U'$ implies $U' \underset{P,W}{\overset{*}{\Longrightarrow}} \widehat{U}$.

We also write $U \underset{P,W}{\overset{\max}{\Longrightarrow}} \widehat{U}$ to denote the fact that $\widehat{U} \underset{P,W}{\overset{*}{\Longrightarrow}} U'$ implies $U' = \widehat{U}$. The subset $\widehat{U}$ is a normal form with respect to the rewrite relation $\underset{P,W}{\Longrightarrow}$, i.e., with respect to inclusion $\widehat{U}$ is the largest set U' such that $U \underset{P,W}{\overset{*}{\Longleftrightarrow}} U'$.

5. Undecidability results

We cannot expect that the word problem of $\mathrm{IM}(G)/P$ is decidable, in general. In fact, we can reduce the *submonoid membership problem* of a group G to the word problem of $\mathrm{IM}(G)/P$ for some idempotent presentation P quite easily. Usually, the *subgroup membership problem* is of more interest than the submonoid membership problem, and we obtain an even better result, because we can replace $\mathrm{IM}(G)/P$ by $\mathrm{IM}(G,\Sigma)/P$ and the latter monoid is finitely generated (which is the natural setting when dealing with word problems). We will be more precise in a moment. Let us stress however that there are finitely generated groups, where the subgroup membership problem is decidable, but the submonoid membership problem is not, [12].

We start with a finitely generated group G and a finite set $\Theta \subseteq G$. By Θ^* we mean the submonoid in G generated by Θ; and by $\langle\Theta\rangle = (\Theta \cup \Theta^{-1})^*$ we mean the subgroup generated by Θ.

The submonoid (resp. subgroup) membership problem for Θ asks whether on input $g \in G$ we have $g \in \Theta^*$ (resp. $g \in \langle\Theta\rangle$). More natural uniform variants of these problems are obtained by putting the generating set Θ into the input. However, with respect to undecidability we get a stronger result if we consider the non-uniform setting as above. Note that the word problem of G is nothing but the subgroup membership problem for $\Theta = \emptyset$.

We choose a finite set Σ such that $\Theta \subseteq \Sigma$ and such that Σ generates G. Define the finite idempotent presentation $P(\Theta)$ by:

$$P(\Theta) = \{ (\{1\}, \{1,t\}) \mid t \in \Theta \}.$$

Recall that this means that we add defining equations of the form $(\{1\}, 1) = (\{1,t\}, 1)$ for all $t \in \Theta$.

For the subgroup membership problem we consider the finitely generated monoid $\mathrm{IM}(G,\Sigma)/P(\Theta \cup \Theta^{-1})$, but for submonoid membership problem we are forced to work in $\mathrm{IM}(G)/P(\Theta)$ which is not finitely generated, in general.

Theorem 6. *Let Θ and Σ as above.*

1.) If the finitely generated inverse monoid $\mathrm{IM}(G,\Sigma)/P(\Theta \cup \Theta^{-1})$ *has a decidable word problem, then we can decide on input* $g = a_1 \cdots a_m \in G$ *with* $a_i \in \Sigma$ *for* $1 \le i \le m$ *whether or not* $g \in \langle\Theta\rangle$.

2.) If the inverse monoid $\mathrm{IM}(G)/P(\Theta)$ *has a decidable word problem, then we can decide on input* $g = a_1 \cdots a_m \in G$ *with* $a_i \in \Sigma$ *for* $1 \le i \le m$ *whether or not* $g \in \Theta^*$. *More precisely, we have:*

$$g \in \Theta^* \iff (\{1, g\}, 1) = 1 \textit{ in } \mathrm{IM}(G)/P(\Theta).$$

Proof. Let $g \in G$. By the choice of $P(\Theta)$ and the techniques from Section 6.4 the following conditions are equivalent:

- $1 = (\{1, g\}, 1)$ in $\mathrm{IM}(G)/P(\Theta)$.
- There exists $U \subseteq G$ with $g \in U$ and $\{1\} \xRightarrow[P(\Theta)]{*} U$.
- $g \in \Theta^*$.

This proves the second item. Replacing $P(\Theta)$ by $P(\Theta \cup \Theta^{-1})$ we also get:

$$1 = (\{1, g\}, 1) \text{ in } \mathrm{IM}(G)/P(\Theta \cup \Theta^{-1}) \iff g \in \langle\Theta\rangle.$$

But the problem is that $(\{1, g\}, 1) \notin \mathrm{IM}(G,\Sigma)$, in general. We always have $(\{1, g\}, 1) \in \mathrm{IM}(G, \Sigma \cup \{g\})$, but this is not what we wish. So, we need a more subtle argument in order to prove the first item.

Assume that $\mathrm{IM}(G,\Sigma)/P(\Theta \cup \Theta^{-1})$ has a decidable word problem. Then, also G has a decidable word problem (for $g = a_1 \cdots a_m \in G$ with $a_i \in \Gamma$ we have $g = 1$ in G if and only if $(U, g)(U, g) = (U, g)$ in $\mathrm{IM}(G,\Sigma)/P(\Theta \cup \Theta^{-1})$, where $U = \{\, a_1 \cdots a_i \mid 0 \le i \le m \,\}$). By induction on the length m of the word $a_1 \cdots a_m$ we present an algorithm, which checks $a_1 \cdots a_m = g \in \langle\Theta\rangle$. For $m = 0$ we clearly have $1 = g \in \langle\Theta\rangle$. Now assume that $m \ge 1$. We let $V = \{\, a_1 \cdots a_i \in G \mid 0 \le i < m \,\}$. Note that V and $V \cup \{g\}$ are connected in the Cayley graph of G with respect to the generating set Σ. Since $m \ge 1$ we have $1 \in V$. Hence, we have $(V, 1), (V \cup \{g\}, 1) \in \mathrm{IM}(G,\Sigma)$. If $(V, 1) \ne (V \cup \{g\}, 1)$ in $\mathrm{IM}(G,\Sigma)/P(\Theta \cup \Theta^{-1})$ (which can be checked by assumption), then $g \notin \langle\Theta\rangle$. On the other hand, if $(V, 1) = (V \cup \{g\}, 1)$ in $\mathrm{IM}(G,\Sigma)/P(\Theta \cup \Theta^{-1})$, then by definition of $\xRightarrow[P(\Theta\cup\Theta^{-1})]{}$ there must exist $h \in V$ with $g \in h\langle\Theta\rangle$. Since V is finite and the word problem of G is decidable, we can find such an h effectively. Since $\langle\Theta\rangle$ is a subgroup of G, we have $g \in \langle\Theta\rangle$ if and only if $h \in \langle\Theta\rangle$. But, $h = a_1 \cdots a_i$ for some $0 \le i < m$ and hence, by induction, we can check $h \in \langle\Theta\rangle$. □

By a results of Rips [23], there exists a hyperbolic group G together with a finitely generated subgroup H of G such that the membership problem for H in G is undecidable. Using a refinement of Rips construction by Wise [29] we can choose the group G hyperbolic, torsion-free, and residually-finite. Thus, together with Theorem 6, we obtain:

Corollary 7. *There exists a torsion-free and residually-finite hyperbolic group G, a finite set $\Sigma \subseteq G$, and a finite idempotent presentation P over $\mathrm{IM}(G,\Sigma)$ such that the word problem of the finitely presented monoid $\mathrm{IM}(G,\Sigma)/P$ is undecidable.*

Even if the subgroup membership problem is decidable for G, as it is the case for the Abelian group $\mathbb{Z} \times \mathbb{Z}$, the word problem of $\mathrm{IM}(G)/P$ might be undecidable. This follows from a result of [17].

Proposition 8 ([17,7]). *There exists a finite idempotent presentation P over $\mathrm{IM}(\mathbb{Z} \times \mathbb{Z})$ such that $\mathrm{IM}(\mathbb{Z} \times \mathbb{Z})/P$ has an undecidable word problem.*

6. The word problem of $\mathrm{IM}(G)/P$ for virtually free groups G

6.1. *Virtually Free Groups*

Due to the undecidability results in Section 5 we cannot hope for to go far beyond free groups in order to generalize the results from [11,14,26]. The best we are able to do in the present paper are virtually free groups. Therefore for the rest of this paper, we assume that G is a finitely generated virtually free group. This means G has a finitely generated non-trivial free subgroup F of finite index. We fix a finite subset H of G such that $1 \in H$ and G can be written as the disjoint union

$$G = \bigcup_{h \in H} Fh. \tag{9}$$

We let Σ be a minimal set of generators for F and let $\Gamma = \Sigma \cup \{a^{-1} \mid a \in \Sigma\}$ as in Section 2. A word $u \in \Gamma^*$ is called *reduced*, if it contains no factor of the form aa^{-1} with $a \in \Gamma$. Clearly, the set of reduced words is in one-to-one correspondence with F. It follows that every element of G can uniquely be written in the form $\widehat{u}h$, where $\widehat{u} \in \Gamma^*$ is reduced and $h \in H$. It is easy to see, that this normal form can be computed in linear time. More precisely, the normal form can be computed with the help of a finite, confluent, and terminating string rewriting system over the alphabet $\Delta = \Gamma \cup H$, see also [25]:

$$\begin{aligned} aa^{-1} &\to 1 \quad \text{for } a \in \Gamma, \\ ha &\to u(h,a)g(h,a) \quad \text{for } h \in H, a \in \Gamma, \\ hh' &\to u(h,h')g(h,h') \quad \text{for } h,h' \in H. \end{aligned}$$

Here $u(h,a), u(h,h') \in \Gamma^*$ and $g(h,a), g(h,h') \in H$ are chosen such that $ha = u(h,a)g(h,a)$ and $hh' = u(h,h')g(h,h')$ hold in the group G. Moreover, either $1 \in H$ is identified with the empty word (by some additional rule), or we keep $1 \in H$ as a distinguished letter of Δ and we work with non-empty words over Δ only. The latter viewpoint is more suitable for our purposes.

Working form left to right on an input string over Δ, the above string rewriting system basically describes the work of a deterministic push-down automaton and some easy reflection yields the well-known fact that the word problem for the virtually free group G can be solved in linear time [18,25].

If the group G is not part of the input, then the sizes of Δ and the rewrite system above are viewed as constants. In particular if $w \in \Delta^*$ is a word of length n, then its normal form $\widehat{u}h \in \Gamma^* H$ has length at most $c \cdot n$ where c is a fixed constant depending on G only.

6.2. *Solving the word problem of* $\mathrm{IM}(G)/P$

We also fix the set $\mathcal{G}$ to be G itself, hence $\mathcal{G} = G$ with the left-regular action of G on G. This is not the most general framework, see Section 6.6, but it avoids an overloading of notations.

In order to have a concise representation of an element $(U, g) \in \mathrm{IM}(G)$ we use the following convention. The pair (U, g) is given by an alternating sequence

$$(a_1, b_1, \ldots, a_n, b_n),$$

with $n \geq 1$, $a_i \in \Delta$, $b_i \in \{0, 1\}$ for $1 \leq i \leq n$, and $a_1 = 1$, $b_1 = b_n = 1$. We read a word of Δ^* as an element of G and then we define $g = a_1 \cdots a_n$ and

$$U = \{a_1 \cdots a_i \mid \ 1 \leq i \leq n, \ b_i = 1\}.$$

Recall that in our setting U is not necessarily connected. This is why we use the bits b_i. Following our convention, the pair $(\{1\}, 1)$ becomes the sequence $(1, 1)$ where the left component is the $1 \in H$ as a letter of Δ and the right component is the bit $1 \in \{0, 1\}$ used as a flag to indicate that $1 \in H$ is in the sequence.

For a concise representation of a rule $(E, E') \in P$ with $E \subseteq E'$ we use an alternating sequence $(a_1, b_1, \ldots, a_n, b_n)$ with $n \geq 1$, $a_i \in \Delta$, $b_i \in \{0, 1, 2\}$ for $1 \leq i \leq n$, and $a_1 = 1$, $b_1 = 2$. Then we define:

$$E = \{a_1 \cdots a_i \mid \ b_i = 1, \ 1 \leq i \leq n\},$$
$$E' = \{a_1 \cdots a_i \mid \ b_i \geq 1, \ 1 \leq i \leq n\}.$$

From our concise representation of the pairs $(U_1, g_1), \ldots, (U_m, g_m)$, it is easy to compute in linear time a pair (U, g) such that $(U, g) = (U_1, g_1) \cdots , (U_m, g_m)$ in $\mathrm{IM}(G)$; we just have to concatenate the alternating sequences for the pairs $(U_1, g_1), \ldots, (U_m, g_m)$. Hence, by Remark 5 the word problem of $\mathrm{IM}(G)/P$ can be reduced in linear time to the following problem:

INPUT: Finite subsets $U, U' \subseteq G$, represented by alternating sequences.

QUESTION: Is there $V \subseteq G$ such that $U \xRightarrow[P]{*} V$ and $U' \subseteq V$?

We do not attack this problem directly, but we perform some preprocessing on the system P first.

6.3. *Preprocessing*

The preprocessing part transforms the input system P into another much larger system P_∞ which is then used to solve the word problem of $\mathrm{IM}(G)/P$. This leads to an optimal algorithm as we will discuss later.

The underlying undirected graph of the Cayley graph $\mathcal{C}(F, \Sigma)$ of the free group F is a tree. The nodes can be represented by reduced words from Γ^*. A subset $S \subseteq F$ is called suffix-closed if for all reduced words $uv \in S$ we have $v \in S$, too.

Let P be a finite list of pairs (E, E') as above. We insist $E \subseteq E'$, but the assumption $1 \in E$ is not needed anymore. In a first step of our preprocessing phase we compute a finite suffix-closed subset $S \subseteq F$ such that

$$\bigcup_{(E,E')\in P} HE' \subseteq SH,$$

where H is from (9). It is clear that the computation of a suitable set $S \subseteq F$ is possible in polynomial time with respect to the size of P. The important point is that whenever $x \in gE'$ for some $g \in G$ and $(E, E') \in P$, then $x \in FSH$: Indeed, let $g = fh$ with $f \in F$ and $h \in H$. Then $x \in fHE' \subseteq fSH$. As we will see this makes it possible to replace the relation $\underset{P}{\Longrightarrow}$ by some relation $\underset{P_\infty,F}{\Longrightarrow}$. Thus, most of our work can be performed over a tree-like structure: the Cayley graph of F.

We first define a system P_0 as follows:

$$P_0 = \{(B, B') \mid B \subseteq B' \subseteq SH,\ B \underset{P}{\Longrightarrow} B'\}.$$

Lemma 9. *Let $U, U' \subseteq G$. Then we have $U \underset{P}{\Longrightarrow} U'$ if and only if $U \underset{P_0,F}{\Longrightarrow} U'$.*

Proof. By definition, if $U \underset{P_0,F}{\Longrightarrow} U'$ then there is some $f \in F$ and $(B, B') \in P_0$ with $fB \subseteq U$ and $U' = U \cup fB'$. On the other hand, since $B \underset{P}{\Longrightarrow} B'$ there is some $g \in G$ and $(E, E') \in P$ with $gE \subseteq B$ and $B' = B \cup gE'$. Thus, we get $fgE \subseteq U$ because $fB \subseteq U$ and $gE \subseteq B$, and we get $U' = U \cup fgE'$ because $U' = U \cup fB'$, $B' = B \cup gE'$ and $fB \subseteq U$. Hence $U \underset{P}{\Longrightarrow} U'$.

For the other direction, let $U \underset{P}{\Longrightarrow} U'$. For some $f \in F$, $h \in H$, and $(E, E') \in P$ we obtain $fhE \subseteq U$ and $U' = U \cup fhE'$. We have $hE \subseteq hE' \subseteq SH$ by definition of S, and $hE \underset{P}{\Longrightarrow} hE'$. Hence $(hE, hE') \in P_0$ and therefore $U \underset{P_0,F}{\Longrightarrow} U'$. $\square$

In the following let $\Gamma_1 = \Gamma \cup \{1\}$. Thus, Γ_1 is the ball of radius 1 in the Cayley graph of F. Since Γ_1 is finite (in fact its size is a constant, if G is not part of the input) we have the notion of a normal form from the end of Section 4.1. Let $i \geq 0$ and P_i already defined as a system of pairs (B, B') with $B \subseteq B' \subseteq SH$. Recall that $B \overset{\max}{\underset{P_i,\Gamma_1}{\Longrightarrow}} \widehat{B}$ defines $\widehat{B}$ in terms of B with respect to P_i. Let us define P_{i+1} as follows:

$$P_{i+1} = \{(B, B') \mid B \subseteq SH,\ B' = \widehat{B} \cap SH,\ B \overset{\max}{\underset{P_i,\Gamma_1}{\Longrightarrow}} \widehat{B}\}.$$

Observe that there are exactly $2^{|SH|}$ rules in P_{i+1}. The computation of P_{i+1} (and its representation) is expensive, but still it can be performed in exponential time in the size of the original system P. Note also that if $(B, B') \in P_i$ then there is exactly one subset $B'' \subseteq SH$ such that $B' \subseteq B''$ and $(B, B'') \in P_{i+1}$. This follows because $1 \in \Gamma_1$.

Lemma 10. *Let $i \geq 0$ and $U, U' \subseteq G$ be finite subsets of G. Then the following statements are equivalent:*

- $\exists V :\ U \overset{*}{\underset{P}{\Longrightarrow}} V$ *and* $U' \subseteq V$.
- $\exists V' :\ U \overset{*}{\underset{P_i,F}{\Longrightarrow}} V'$ *and* $U' \subseteq V'$.

Proof. The equivalence holds for $i = 0$ by Lemma 9.

Thus, let $i \geq 0$ and assume first that $U \underset{P_i,F}{\overset{*}{\Longrightarrow}} V$ for some $U' \subseteq V$. We have to show that there is some V' with $U \underset{P_{i+1},F}{\overset{*}{\Longrightarrow}} V'$ and $U' \subseteq V'$. However, this is trivial, because for each $(B, B') \in P_i$ there is some $(B, B'') \in P_{i+1}$ with $B' \subseteq B''$.

It remains to show the other direction. Assume that $U \underset{P_{i+1},F}{\overset{*}{\Longrightarrow}} V'$ and $U' \subseteq V'$. It is enough to show that there is V with $V' \subseteq V$ and $U \underset{P_i,F}{\overset{*}{\Longrightarrow}} V$. Let for this purpose $\widehat{P} = \{(B, \widehat{B}) \mid B \subseteq SH, B \underset{P_i,\Gamma_1}{\overset{\max}{\Longrightarrow}} \widehat{B}\}$. Clearly for each $(B, B') \in P_{i+1}$ there is now some $(B, \widehat{B}) \in \widehat{P}$ with $B' \subseteq \widehat{B}$. Hence, for some subset V'' we have $U \underset{\widehat{P},F}{\overset{*}{\Longrightarrow}} V''$ and $V' \subseteq V''$. It is therefore enough to find some V with $U \underset{P_i,F}{\overset{*}{\Longrightarrow}} V$ and $V'' \subseteq V$. But this is again trivial because $(B, \widehat{B}) \in \widehat{P}$ implies $B \underset{P_i,F}{\overset{*}{\Longrightarrow}} \widehat{B}$. □

Recall that $(B, B') \in P_i$ implies the existence of some unique $(B, B'') \in P_{i+1}$ with $B \subseteq B' \subseteq B'' \subseteq SH$. There are at most exponentially many rules and each rule can change at most polynomially often when increasing the index i. Thus, after an exponential time computation we must find an index $i \geq 0$ such that $P_i = P_{i+1}$. In order to be precise we have $i \leq |SH|\, 2^{|SH|}$.

We stop the preprocessing phase here and define $P_\infty = P_i$. From our construction and Lemma 10, we immediately obtain:

Lemma 11. *The following assertions hold:*

- *For all $(B, B') \in P_\infty$ we have $B' = \widehat{B} \cap SH$, where $B \underset{P_\infty,\Gamma_1}{\overset{\max}{\Longrightarrow}} \widehat{B}$.*
- *$\exists V : U \underset{P}{\overset{*}{\Longrightarrow}} V$ and $U' \subseteq V$ if and only if $\exists V' : U \underset{P_\infty,F}{\overset{*}{\Longrightarrow}} V'$ and $U' \subseteq V'$.*

This finishes the preprocessing phase. By this phase we are left with the following problem:

INPUT: Finite subsets $U, U' \subseteq G$.

QUESTION: Is there V such that $U \underset{P_\infty,F}{\overset{*}{\Longrightarrow}} V$ and $U' \subseteq V$?

6.4. *Solving the word problem*

The basic idea is to replace the relation $\underset{P_\infty,F}{\overset{*}{\Longrightarrow}}$ in the problem above by some $\underset{P_\infty,W}{\overset{*}{\Longrightarrow}}$ where $W \subseteq F$ is finite. We fix for this section the following notation: Let P and P_∞ as above and consider two finite subsets $U, U' \subseteq G$. There is a finite suffix-closed set $S \subseteq F$ such that $(B, B') \in P_\infty$ implies $B \subseteq B' \subseteq SH$. We let $W \subseteq F$ be some finite subtree of the Cayley graph of F with

$$\{1\} \cup U \cup U' \subseteq WSH. \tag{15}$$

We let $\widehat{U}$ be defined by $U \underset{P_\infty,W}{\overset{\max}{\Longrightarrow}} \widehat{U}$.

We will prove the following theorem which reduces the word problem of $\mathrm{IM}(G)/P$ to the problem of computing $\widehat{U}$.

Theorem 12. *The following statements are equivalent:*

(a) $\exists V : U \xRightarrow[P]{*} V$ *and* $U' \subseteq V$*,*
(b) $U' \subseteq \widehat{U}$*.*

The direction from (b) to (a) has been seen in Lemma 10. The difficult part is to show the direction from (a) to (b). This will cover the rest of the section.

The following notation is crucial: For a subset $V \subseteq G$ and an element $f \in F$ define the derivation

$$V \circ f = V'$$

by $V' = V \cup fB'$, where $(B, B') \in P_\infty$ and $fB = V \cap fSH$.

Note that $V \circ f$ is defined for all $V \subseteq G$ and $f \in F$ since all subsets of SH appear as a left-hand side of some rule in P_∞. Clearly, $V \circ f = V'$ implies $V \xRightarrow[P_\infty, F]{} V'$, and $V \xRightarrow[P_\infty, F]{} V'$ implies $V' \subseteq V \circ f$ for some $f \in F$.

By Lemma 11, there is some V with $U \xRightarrow[P]{*} V$ and $U' \subseteq V$ if and only if there is a sequence $(f_1, \ldots, f_m)$ with $f_i \in F$ for $1 \le i \le m$ such that

$$U' \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m.$$

Since $U' \subseteq WSH$ by (15) it is therefore enough to prove the following lemma in order to show Theorem 12:

Lemma 13. *Let* $f_1, \ldots, f_m \in F$*. Then we have*

$$\widehat{U} \circ f_1 \circ \cdots \circ f_m \cap WSH \subseteq \widehat{U}.$$

First we restrict our attention to some special type of derivations which we call tree-like.

Definition 14. *A derivation* $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ *is called* tree-like*, if the following conditions hold:*

(1) $W = \{f_1, \ldots, f_n\}$ *for some* $n \le m$*.*
(2) $f_i \notin \{f_1, \ldots f_{i-1}\}$ *for* $1 \le i \le m$*.*
(3) For all $1 < i \le m$ *there is some* $j \in \{1, \ldots, i-1\}$ *and some* $a \in \Gamma$ *with* $f_j a = f_i$ *in* F*.*

The conditions above mean that $\{f_1, \ldots, f_i\}$ forms a subtree of size i in the Cayley graph of F for all i and which includes W for $n \le i \le m$. Moreover, we insist that $m \ge |W| = n$.

The next statement is the key lemma. It says that in a tree-like derivation, if a right-hand side of a rule appears in a subset, then this subset remains invariant. It cannot become larger by further applications of rules. More formally:

Lemma 15. *Let $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ be a tree-like derivation. For $1 \leq i \leq m$ define a subset $B(i)$ of SH by*

$$f_i B(i) = \widehat{U} \circ f_1 \circ \cdots \circ f_i \cap f_i SH.$$

Then $B(i)$ is a right-hand side of a rule in P_∞, and we have:

$$f_i B(i) = \widehat{U} \circ f_1 \circ \cdots \circ f_m \cap f_i SH.$$

Proof. The statement is trivial for $m = n$ because $\widehat{U} \circ f_1 \circ \cdots \circ f_n = \widehat{U}$, due to $W = \{f_1, \ldots, f_n\}$ and the fact $\widehat{U} \overset{\max}{\underset{P_\infty, W}{\Longrightarrow}} \widehat{U}$. Moreover, it is easy to see that $B(i)$ is a right-hand side of a rule in P_∞ for all i.

Now, let $m > n$ and $V = \widehat{U} \circ f_1 \circ \cdots \circ f_{m-1}$. Note that

$$V \subseteq \bigcup_{i<m} f_i SH \tag{21}$$

by the choice of W in (15). We have to show that

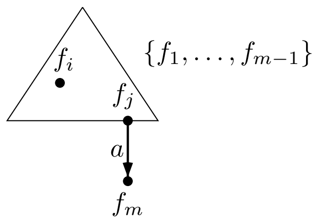
$$f_i B(i) = V \circ f_m \cap f_i SH$$

for all $1 \leq i \leq m$. By definition of $f_i B(i)$ this holds for $i = m$. By induction we may assume that $f_i B(i) = V \cap f_i SH$ for all $1 \leq i < m$.

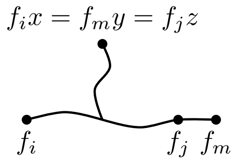
Choose $j \in \{1, \ldots, m-1\}$ and $a \in \Gamma$ such that $f_j a = f_m$ in F. Assume that $f_i SH \cap f_m SH \neq \emptyset$ for some $1 \leq i < m$. Then for some $x, y \in S$ we have:

$$f_i x = f_m y.$$

This is true because $\bigcup_{h \in H} Fh$ is a disjoint union. The situation looks as follows:



Since the Cayley graph of F is a tree, the geodesic from f_i to f_m passes through f_j. This means $f_i x = f_m y = f_j z$, where z is either a suffix of x or a suffix of y:



Since S is suffix-closed we deduce that $z \in S$ and hence $f_i SH \cap f_m SH \subseteq f_j SH$. By (21) it follows that

$$f_m SH \cap V \subseteq f_m SH \cap \bigcup_{i<m} f_i SH \subseteq f_j SH.$$

Hence, $f_m SH \cap V \subseteq f_j SH \cap V = f_j B(j) \subseteq V$. Therefore we have

$$V \circ f_m = V \ \cup \ (f_j B(j)) \circ f_m. \tag{24}$$

Now, $(f_j B(j)) \circ f_m = f_j(B(j) \circ a)$, because $f_m = f_j a$ with $a \in \Gamma$. Moreover, $B(j)$ is the right-hand side of some rule in P_∞. Thus, by Lemma 11:

$$B(j) \circ a \cap SH = B(j).$$

It follows

$$(f_j B(j)) \circ f_m \cap f_j SH = f_j(B(j) \circ a \cap SH) = f_j B(j)$$

and therefore

$$\begin{aligned} V \circ f_m \cap f_j SH &= (V \cup (f_j B(j)) \circ f_m) \cap f_j SH \qquad \text{(by (24))} \\ &= (V \cap f_j SH) \cup ((f_j B(j)) \circ f_m \cap f_j SH) \\ &= (V \cap f_j SH) \cup f_j B(j) \\ &= V \cap f_j SH \\ &= f_j B(j) \subseteq V. \end{aligned}$$

We obtain for $1 \leq i < m$:

$$\begin{aligned} V \circ f_m \cap f_i SH &= (V \cup (V \circ f_m \cap f_m SH)) \cap f_i SH \\ &= (V \cap f_i SH) \cup (V \circ f_m \cap f_i SH \cap f_m SH) \\ &\subseteq f_i B(i) \cup (V \circ f_m \cap f_i SH \cap f_j SH) \\ &\subseteq f_i B(i) \cup (f_i SH \cap V) \\ &= f_i B(i). \end{aligned}$$

Since $f_i B(i) \subseteq V \circ f_m \cap f_i SH$, it follows that $f_i B(i) = V \circ f_m \cap f_i SH$. $\square$

The following lemma shows that we can restrict to tree-like derivations.

Lemma 16. *Let $g_1, \ldots, g_k \in F$. Then there is a tree-like derivation $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ such that:*

$$\widehat{U} \circ g_1 \circ \cdots \circ g_k \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m.$$

Proof. Clearly for every $g \in F$ we have

$$\widehat{U} \circ g_1 \circ \cdots \circ g_k \subseteq \widehat{U} \circ g \circ g_1 \circ \cdots \circ g_k.$$

Hence we may replace $\{g_1, \ldots, g_k\}$ by some larger set. We add many new g on the left of the sequence $g_1, \ldots, g_k$. This enlarges the value k, but then we may assume that for some tree-like derivation $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ with $k \geq m$ we have $\{g_1, \ldots, g_k\} = \{f_1, \ldots, f_m\}$ and in fact $g_i = f_i$ for $1 \leq i \leq m$.

We show $\widehat{U} \circ g_1 \circ \cdots \circ g_k \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m$ by induction over k. The case $k = m$ is clear. Now assume that $k > m$. By induction, we have $\widehat{U} \circ g_1 \circ \cdots \circ g_{k-1} \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m$. Hence it is enough to show that

$$\widehat{U} \circ f_1 \circ \cdots \circ f_m \circ g_k \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m.$$

However $g_k = f_i$ for some $1 \leq i \leq m$.

Let $V = \widehat{U} \circ f_1 \circ \cdots \circ f_m$. We show $V \circ f_i = V$ for all $1 \leq i \leq m$. As in Lemma 15 let $f_i B(i) = \widehat{U} \circ f_1 \circ \cdots \circ f_i \cap f_i SH$. Then Lemma 15 says that $V \cap f_i SH = f_i B(i)$. Since $B(i)$ is a right-hand side of P_∞, we obtain

$$V \circ f_i = V \cup (f_i B(i) \circ f_i) = V \cup f_i B(i) = V. \qquad \square$$

We are now able to prove Lemma 13:

Proof of Lemma 13. By Lemma 16 we may assume that $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ is tree-like. In particular, $n \leq m$ and $W = \{f_1, \ldots, f_n\}$. Every element of WSH is contained in some $f_i SH$ for $1 \leq i \leq n$. By Lemma 15 we have

$$\widehat{U} \circ f_1 \circ \cdots \circ f_m \cap f_i SH = \widehat{U} \circ f_1 \circ \cdots \circ f_i \cap f_i SH.$$

However, $\widehat{U} \circ f_1 \circ \cdots \circ f_i = \widehat{U}$ for every $i \leq n$. Therefore

$$\begin{aligned}
\widehat{U} \circ f_1 \circ \cdots \circ f_m \cap WSH &\subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m \cap (\bigcup_{i=1}^{n} f_i SH) \\
&= \bigcup_{i=1}^{n} (\widehat{U} \circ f_1 \circ \cdots \circ f_m \cap f_i SH) \\
&= \bigcup_{i=1}^{n} (\widehat{U} \circ f_1 \circ \cdots \circ f_i \cap f_i SH) \\
&= \bigcup_{i=1}^{n} (\widehat{U} \cap f_i SH) \subseteq \widehat{U}.
\end{aligned}$$

This proves Lemma 13 and hence Theorem 12.

6.5. *A Linear Time Computation*

The setting is as follows. The virtually free group G is fixed as well as the system P. In a preprocessing phase we have computed the system P_∞ and a suffix-closed subset $S \subseteq F$ such that $B \subseteq B' \subseteq SH$, for all $(B, B') \in P_\infty$ in constant time.

The input to our problem are two finite subsets $U, U' \subseteq G$. We assume that they are given as alternating sequences as described in Section 6.1. We work on a RAM, therefore we may use pointers to realize subtrees of the Cayley graph of F. Since S and H are viewed as constants we can realize a subtree W in linear time in the input size of U and U' such that W satisfies

$$\{1\} \cup U \cup U' \subseteq WSH.$$

Our task is now to compute $U \overset{\max}{\underset{P_\infty,W}{\Longrightarrow}} \widehat{U}$ in linear time. The final test whether $U' \subseteq \widehat{U}$ can be performed in linear time by reading U' once more.

In order to compute $U \overset{\max}{\underset{P_\infty,W}{\Longrightarrow}} \widehat{U}$ we build a list $L = (f_1, \ldots, f_n)$ which initially contains all elements of W.

As long as L is not empty we perform the following steps: Let f be the first element of L. Remove f from L. Compute a set B such that $fB = fSH \cap U$ in constant time. By table lookup in P_∞ find a set B' such that $(B, B') \in P_\infty$. If $B \neq B'$, then replace U by $U \cup fB'$ in constant time, and add all elements $g \in W$ to the list L, where $gSH \cap fB' \neq \emptyset$ and $g \neq f$. This amounts to calculate the intersection $W \cap fB'H^{-1}S^{-1}$ and can be performed in constant time. (If $B = B'$ then we do nothing.)

Once the list L is empty we claim that $U = \widehat{U}$. Before we prove that claim let us analyze the complexity. The inner parts of the loop can be performed in constant time. Thus, we have to give an upper bound on the number of times we can enter the loop. After each iteration of the loop, the list L is shorter or we have added less than c elements where $c = |S|^2|H|^2$ is a constant. Let us associate a weight ω to the pair (U, L) by

$$\omega = c|WSH \setminus U| + |L|.$$

Here $|L|$ denotes the length of the list L. The weight is always a non-negative integer and in the beginning it is at most $(c + 1)|WSH|$. This is linear in the input size of U and U'. We show that the weight decreases in each round.

Inside the loop there are two cases: either $B = B'$ or $B \neq B'$. If $B = B'$ then U is not changed but $|L|$ decreases by 1. If $B \neq B'$, then U becomes larger. We still have $U \subseteq WSH$ and hence the size of $|WSH \setminus U|$ decreases by at least 1. This subtracts from the weight at least c units, but we add to L less than c elements. Thus the weight decreases totally by at least 1. Thus, after at most $(c + 1)|WSH|$ rounds the list L must be empty.

It remains to show, that we have calculated $\widehat{U}$. For this we show the following invariant: After each round of the loop the list L contains all elements $g \in W$ such that $U \circ g \neq U$. This is certainly true in the beginning because at this time L contains all elements of W. Consider the situation where f is the first element of L and f has just been removed. Inside the loop we have replaced U by $U \circ f$ and since $U \circ f \circ f = U \circ f$ we do not need f in L anymore in order to keep the invariant for this round. Hence if we are in the situation $U = U \circ f$ then the invariant is not changed. Thus we may assume that U has been replaced by $U \cup fB'$ with $B \neq B'$.

Now, if

$$(U \cup fB') \circ g \neq U \cup fB',$$

for some $g \in W$ then $g \neq f$ and either $U \circ g \neq U$ or $gSH \cap fB' \neq \emptyset$. In the first case g is still in the list and in the second case g is added to the list L. Thus, in both cases g is in the list L after the inner part of the loop has been finished. Once the list L is empty the invariant says that U is irreducible with respect to the rewriting system $\underset{P_\infty,W}{\Longrightarrow}$. Hence $U = \widehat{U}$.

This shows, that the set $\widehat{U}$ can be calculated in linear time. Summarizing we have shown the following result:

Theorem 17. *Let G be a finitely generated virtually-free group and let P be a finite idempotent presentation over $\mathrm{IM}(G)$. Then the word problem of the inverse monoid $\mathrm{IM}(G)/P$ can be solved in linear time on a RAM.*

The linear time complexity above is in sharp contrast to the uniform time complexity, where the group G and the system P become part of the input.

Theorem 18. *The following problem is EXPTIME-complete:*
INPUT: A finitely generated virtually free group G, given say by a finite confluent string rewriting system as in Section 6.1, a finite idempotent presentation P over $\mathrm{IM}(G)$, elements $g, g' \in G$, and finite sets $U, U' \subseteq G$ with $1, g \in U$ and $1, g' \in U'$
QUESTION: Do we have $(U, g) = (U', g')$ in $\mathrm{IM}(G)/P$?

Proof. In the uniform setting the algorithm presented here can still be performed in exponential time. The problem is hard for exponential time due to [11]. □

6.6. *The word problem of* $\mathrm{IM}(\mathcal{G})/P$ *for the Margolis-Meakin expansion*

In Section 6.3–6.5 we have restricted our attention to $\mathcal{G} = G$. However, we can generalize the results at least to a situation where the group G acts freely on the set $\mathcal{G}$. This means $gx = x$ implies $g = 1$ for $g \in G$ and $x \in \mathcal{G}$. In this case, every orbit of $\mathcal{G}$ is a copy of G. Thus, the set $\mathcal{G}$ can be written as a disjoint union of copies of G.

We fix a set $\mathcal{B} \subseteq \mathcal{G}$ of minimal cardinality such that

$$\bigcup_{(E,E')\in P} E' \subseteq G\mathcal{B}.$$

Since $\mathcal{B}$ has minimal cardinality, $gb = g'b'$ for $g, g' \in G$, $b, b' \in \mathcal{B}$ implies $b = b'$ and $g = g'$. Note that we may assume that $\mathcal{B}$ is a finite set included in the union $\bigcup_{(E,E')\in P} E'$. In particular, the size $\mathcal{B}$ is smaller than the input size of P. The next step in the preprocessing phase computes a finite suffix-closed subset $S \subseteq F$ such that

$$\bigcup_{(E,E')\in P} HE' \subseteq SH\mathcal{B}.$$

Basically, all steps go through now, if we replace all occurrences of SH by $S\mathcal{H}$, where $\mathcal{H}$ denotes the set $H\mathcal{B}$. In particular Assertion (6.4) remains valid because the action of G on $\mathcal{G}$ is free. Details are left to the interested reader. Thus, we can solve the word problem of $\mathrm{IM}(\mathcal{G})/P$, if first, G acts freely on $\mathcal{G}$, and second, if there is an effective decomposition of $\mathcal{G}$ as a disjoint union of copies of G.

In particular, we can cope with the construction of Margolis and Meakin [13,14] as mentioned in the introduction. The elements of $M(G, \Sigma)$ are pairs of the form (U, g), where U is a finite and connected subgraph of the Cayley graph $\mathcal{C}(G, \Sigma)$, which contains 1 and g. Multiplication of two such pairs is again defined by the rule (2). The group G acts freely on the vertices and directed edges of the Cayley graph $\mathcal{C}(G, \Sigma)$ by left multiplication.

7. Decision problems for rational subsets of $\mathrm{IM}(G)/P$

In this section, we associate with the inverse monoid $\mathrm{IM}(G)/P$ a relational structure $\mathsf{R}(\mathrm{IM}(G)/P)$ and we prove that this structure has a decidable first-order theory. As a consequence, we deduce the decidability of several computational problems concerning rational subsets of $\mathrm{IM}(G)/P$. First, we recall some basic definitions from logic.

7.1. *Logic*

See [8] for more details on the subject of this section. A *signature* is a countable set $\mathcal{S}$ of relational symbols, where each relational symbol $R \in \mathcal{S}$ has an associated arity n_R. A *(relational) structure* over the signature $\mathcal{S}$ is a tuple $\mathcal{A} = (A, (R^{\mathcal{A}})_{R\in\mathcal{S}})$, where A is a set (the universe of $\mathcal{A}$) and $R^{\mathcal{A}}$ is a relation of arity n_R over the set A, which interprets the relational symbol R. We will assume that every signature contains the equality symbol $=$ and that $=^{\mathcal{A}}$ is the identity relation on the set A. As usual, a constant $c \in A$ can be encoded by the unary relation $\{c\}$. Usually, we denote the relation $R^{\mathcal{A}}$ also with R.

Next, let us introduce *monadic second-order logic (MSO-logic)*. Let $\mathbb{V}_1$ (resp. $\mathbb{V}_2$) be a countably infinite set of *first-order variables* (resp. *second-order variables*) which range over elements (resp. subsets) of the universe A. First-order variables (resp. second-order variables) are denoted x, y, z, x', etc. (resp. X, Y, Z, X', etc.). *MSO-formulas* over the signature $\mathcal{S}$ are constructed from the atomic formulas $R(x_1, \ldots, x_{n_R})$ and $x \in X$ (where $R \in \mathcal{S}$, $x_1, \ldots, x_{n_R}, x \in \mathbb{V}_1$, and $X \in \mathbb{V}_2$) using the boolean connectives $\neg, \wedge$, and $\vee$, and quantifications over variables from $\mathbb{V}_1$ and $\mathbb{V}_2$. The notion of a free occurrence of a variable is defined as usual. A formula without free occurrences of variables is called an *MSO-sentence*. For an MSO-sentence φ we write $\mathcal{A} \models \varphi$ if φ evaluates to true in $\mathcal{A}$.

A *first-order formula* over the signature $\mathcal{S}$ is an MSO-formula that does not contain any occurrences of second-order variables. The *first-order theory* of the structure $\mathcal{A}$ is the set of all first-order sentences φ such that $\mathcal{A} \models \varphi$.

7.2. *Relation structures over rational subsets*

Recall that for a monoid M, the class $\mathrm{RAT}(M)$ of all *rational subsets* of M is the smallest class of subsets of M, which contains all finite subsets and which is closed under union, multiplication, and Kleene star. The Kleene star associates to a subset $L \subseteq M$ the submonoid L^* generated by L. A rational language $L \in \mathrm{RAT}(M)$ can be represented either by a rational (or regular) expression with constants from M or by a (non-deterministic) finite automaton with transitions labeled with elements from M.

With the monoid M (with neutral element 1) we associate the relational structure

$$\mathsf{R}(M) = (M, (\mathrm{reach}_L)_{L\in\mathrm{RAT}(M)}, 1),$$

where

$$\mathrm{reach}_L = \{(x, y) \mid \exists z \in L : xz = y\}.$$

The following result generalizes a corresponding result from [11] for the monoid

$\mathrm{IM}(F, \Sigma)/P$, where F is the free group generated by Σ and P is a finite idempotent presentation.

Theorem 19. *Let G be a finitely generated virtually-free group and let P be a finite idempotent presentation over $\mathrm{IM}(G)$. Then the first-order theory of the structure $\mathsf{R}(\mathrm{IM}(G)/P)$ is decidable.*

The proof of Theorem 19 follows the proof for the corresponding result from [11]. We will reduce the first-order theory of $\mathsf{R}(\mathrm{IM}(G)/P)$ to the monadic second-order theory of the Cayley graph $\mathcal{C}(G, \Sigma)$. Before we do this, let us first recall some known results on monadic second-order logic over graphs.

In the following, we view a Cayley graph $\mathcal{C}(G, \Sigma)$ of a group G as a directed graph with edges labeled by symbols from Σ. There is an edge (g, h) with label a if and only if $ga = h$. Thus, as a relational structure the universe is the set G with the constant 1 and for each $a \in \Sigma$ there is binary relation

$$E_a = \left\{ (g, h) \in G \times G \;\middle|\; g^{-1}h = a \right\}.$$

Implicitly, we may think that for each edge (g, h) there is also also an edge (h, g) with label $h^{-1}g$. For virtually-free groups, Muller and Schupp have shown:

Theorem 20 ([19]). *Let G be virtually-free group G with a finite generating set Σ. Then the MSO-theory of the Cayley graph $\mathcal{C}(G, \Sigma)$ is decidable.*

Next let us introduce a few MSO-formulas, which are interpreted in the Cayley graph of the virtually-free group G: Let P be a finite idempotent presentation over $\mathrm{IM}(G)$. Following [14], we define for a subset $U \subseteq G$ its closure

$$\mathrm{cl}_P(U) = \bigcup \{V \subseteq G \mid U \underset{P}{\overset{*}{\Longrightarrow}} V\} \subseteq G.$$

It follows that $(U, g) = (V, h)$ in $\mathrm{IM}(G)/P$ if and only if $g = h$ in G and $\mathrm{cl}_P(U) = \mathrm{cl}_P(V)$. It is easy to see that there exists an MSO-formula $\mathrm{CL}_P(X, Y)$, expressing that $Y = \mathrm{cl}_P(X)$ (see also [14]): We just have to say that Y is the smallest (with respect to inclusion) subset of G which contains X and which is closed under the relation $\underset{P}{\Longrightarrow}$, i.e, $\forall Z : Y \underset{P}{\Longrightarrow} Z \implies Z = Y$. The rewrite relation $\underset{P}{\Longrightarrow}$ is easily MSO-definable in $\mathcal{C}(G, \Sigma)$.

We also have to express in MSO (over $\mathcal{C}(G, \Sigma)$) that a subset of G is finite. First we choose a free subgroup F of finite index and a finite set H (c.f. (9)) such that $U \subseteq G$ is infinite if and only if for some $h \in H$ the intersection $F \cap Uh^{-1} \subseteq F$ is infinite. The sets Uh^{-1} are MSO-definable from U in $\mathcal{C}(G, \Sigma)$. Moreover, the free subgroup F is MSO-definable, too (as is any finitely generated subgroup of G).

Using König's lemma, finiteness is MSO-definable in finitely branching trees. In particular, this is the case for the Cayley graph of the finitely generated free group F.

Finally we will need the following statement concerning MSO over arbitrary graphs, which was shown in [11]:

Proposition 21. *Let Γ be a finite alphabet and let $L \subseteq \Gamma^*$ be a rational language. There exists an MSO-formula $\mathrm{Reach}_L(x, y, X)$ over the signature consisting of binary relation* *symbols E_a, $a \in \Gamma$, such that for every directed edge-labeled graph $G = (V, (E_a)_{a\in\Gamma})$, all nodes $s, t \in V$, and every finite set of nodes $U \subseteq V$ we have: $G \models \mathrm{Reach}_L(s,t,U)$ if and only if there exist a path $(p_0, \ldots, p_m)$ ($p_i \in V$) and $a_1, \ldots, a_m \in \Gamma$ with $p_0 = s$, $p_m = t$, $(p_{i-1}, p_i) \in E_{a_i}$ for $i \in \{1, \ldots, m\}$, $a_1 \cdots a_m \in L$, and $U = \{p_0, \ldots, p_m\}$.*

Proof of Theorem 19. We will reduce the first-order theory of $\mathsf{R}(\mathrm{IM}(G)/P)$ to the MSO-theory of $\mathcal{C}(G,\Sigma)$. Since G is a finitely generated virtually free group, we can conclude the proof using Theorem 20.

Let us fix a first-order sentence φ over the (infinite) signature of $\mathsf{R}(\mathrm{IM}(G)/P)$. Let $L_1, \ldots, L_n \subseteq \mathrm{IM}(G)/P$ be all rational languages, which appear in φ, and assume that L_i is represented in φ by a finite automaton A_i with transition labels from $\mathrm{IM}(G)$. Let $\Theta \subseteq G$ be the union of Σ and of all finite subsets $U \subseteq G$ such that (U, g) labels a transition in one of the automata $A_1, \ldots, A_n$. Hence, for every $(U, g) \in \mathrm{IM}(G)$ which labels a transition of some A_i, the set U is connected in the Cayley graph $\mathcal{C}(G,\Theta)$, i.e., it belongs to $\mathrm{IM}(G,\Theta)$. Let $\Gamma = \Theta \cup \Theta^{-1}$ and recall that there is a canonical mapping

$$\gamma : \Gamma^* \to \mathrm{IM}(G,\Theta) \to \mathrm{IM}(G)/P$$

defined by $g \mapsto (\{1, g\}, g)$ for $g \in \Gamma \subseteq G$. Each $(U, g) \in \mathrm{IM}(G,\Theta)$ can be represented by a finite word over the alphabet Γ: If $U = \{g_1, \ldots, g_k\}$ then a possible representing word is $(g_1 g_1^{-1}) \cdots (g_k g_k^{-1}) g$. Now every A_i can be viewed as a finite automaton where the transitions are labeled with words over Γ. Thus, each A_i also accepts a subset of Γ^*, and it is justified to use the same symbol L_i to denote the accepted subset of $\mathrm{IM}(G)/P$ as well as the accepted subset of Γ^*.

We now translate the first-order sentence φ over $\mathsf{R}(\mathrm{IM}(G)/P)$ into an MSO-sentence $\widehat{\varphi}$ over the Cayley graph $\mathcal{C}(G,\Theta)$ such that $\mathsf{R}(\mathrm{IM}(G)/P) \models \varphi$ if and only if $\mathcal{C}(G,\Theta) \models \widehat{\varphi}$. The following translation is analogous to the one for the case that G is free from [11]. For completeness, we will repeat the arguments.

Let x be a variable in φ, which ranges over elements of $\mathrm{IM}(G)/P$. Hence, x will be interpreted by a pair (U, g), where $U \subseteq G$ is finite and $1, g \in U$. Therefore, we associate with x two variables in the MSO-sentence $\widehat{\varphi}$:

- an MSO-variable X' representing U and
- a first-order variable x', representing g.

The fact, that a pair (X', x') represents indeed an element of the monoid $\mathrm{IM}(G)$ (and hence $\mathrm{IM}(G)/P$) is expressed by the MSO-formula (over the signature of $\mathcal{C}(G,\Theta)$):

$$\mathrm{valid}(x', X') = (1 \in X' \ \wedge\ x' \in X' \ \wedge\ X' \text{ is finite}).$$

Recall that finiteness of a subset of G can be expressed in MSO. Equality in the monoid $\mathrm{IM}(G)/P$ is expressed by the MSO-formula

$$\mathrm{eq}(x', X', y', Y') = (x' = y' \ \wedge\ \exists Z : \mathrm{CL}_P(X', Z) \wedge \mathrm{CL}_P(Y', Z)).$$

We now define $\widehat{\varphi}$ inductively as follows:

(a) For $\varphi = (x = y)$ define $\widehat{\varphi} = \mathrm{eq}(x', X', y', Y')$.

(b) Let $L \in \{ L_1, \ldots, L_n \}$. For $\varphi = \mathrm{reach}_L(x, y)$ define

$$\widehat{\varphi} = \exists X'' \, \exists Y'' \, \exists Z : \left\{ \begin{array}{l} \mathrm{valid}(x', X'') \ \wedge \ \mathrm{valid}(y', Y'') \ \wedge \\ \mathrm{eq}(x', X', x', X'') \ \wedge \ \mathrm{eq}(y', Y', y', Y'') \ \wedge \\ Y'' = X'' \cup Z \ \wedge \ \mathrm{Reach}_L(x', y', Z) \end{array} \right\},$$

where Reach_L is the formula from Proposition 21.

(c) For $\varphi = \neg\psi$ define $\widehat{\varphi} = \neg\widehat{\psi}$.

(d) For $\varphi = \psi_1 \wedge \psi_2$ define $\widehat{\varphi} = \widehat{\psi_1} \wedge \widehat{\psi_2}$.

(e) For $\varphi = \exists x : \psi$ define $\widehat{\varphi} = \exists x' \, \exists X' : \mathrm{valid}(x', X') \ \wedge \ \widehat{\psi}$.

The formula

$$\exists X'' \, \exists Y'' \, \exists Z : \left\{ \begin{array}{l} \mathrm{valid}(x', X'') \ \wedge \ \mathrm{valid}(y', Y'') \ \wedge \\ \mathrm{eq}(x', X', x', X'') \ \wedge \ \mathrm{eq}(y', Y', y', Y'') \ \wedge \\ Y'' = X'' \cup Z \ \wedge \ \mathrm{Reach}_L(x', y', Z) \end{array} \right\} \tag{35}$$

in (b) expresses the following: There are pairs (X'', x') and (Y'', y'), which represent the same elements of $\mathrm{IM}(G)/P$ as (X', x') and (Y', y'), respectively. Moreover, there is a path in $\mathcal{C}(G, \Sigma)$, which starts in the node $x' \in G$, ends in $y' \in G$ and is labeled by a word from the rational language L. The set of nodes along this path is Z and therefore $(x'^{-1}Z, x'^{-1}y')$ represents an element of L. Finally, since $Y'' = X'' \cup Z$ we have $(X'', x')(x'^{-1}Z, x'^{-1}y') = (Y'', y')$ in $\mathrm{IM}(G)$. Thus, in $\mathrm{IM}(G)/P$ we have (as desired) $(X', x')(x'^{-1}Z, x'^{-1}y') = (X'', x')(x'^{-1}Z, x'^{-1}y') = (Y'', y') = (Y', y')$ with $(x'^{-1}Z, x'^{-1}y') \in L$. Vive versa, if $(X', x')(U, g) = (Y', y')$ for some $(U, g) \in L$ in $\mathrm{IM}(G)/P$, then (35) is easily seen to be satisfied. Now it is straightforward to verify that $\mathsf{R}(\mathrm{IM}(G)/P) \models \varphi$ if and only if $\mathcal{C}(G, \Theta) \models \widehat{\varphi}$. In the final step we just translate the MSO-formula $\widehat{\varphi}$ to another formula $\widetilde{\varphi}$ such that $\mathcal{C}(G, \Theta) \models \widehat{\varphi}$ if and only if $\mathcal{C}(G, \Sigma) \models \widetilde{\varphi}$. This is easy because each $\theta \in \Theta$ is effectively a word in Σ^*. This concludes the proof of Theorem 19 with the help of Theorem 20.

Since every monoid $\mathrm{IM}(G, \Sigma)/P$, for Σ a finite generating set of G, is a finitely generated submonoid of $\mathrm{IM}(G)/P$ and hence rational, it follows from Theorem 19 that also the first-order theory of every structure $\mathsf{R}(\mathrm{IM}(G, \Sigma)/P)$ is decidable. One should notice that the first-order theory of $\mathsf{R}(\mathrm{IM}(G, \Sigma)/P)$ depends on the generating set Σ. To see this, let G be the free group generated by a and b, let $P = \emptyset$, and consider the two generating sets $\Sigma = \{a, b\}$ and $\Sigma' = \{a, b, ab\}$ of G. Let $c = (\{1, a, ab\}, 1) \in \mathrm{IM}(G, \Sigma) \subseteq \mathrm{IM}(G, \Sigma')$; this element is first-order definable in $\mathsf{R}(\mathrm{IM}(G, \Sigma))$ (note that the neutral element is a constant in the structure $\mathsf{R}(\mathrm{IM}(G, \Sigma))$). Now let $L = \{(\{1, a\}, 1)\}$, which is a rational subset of $\mathrm{IM}(G, \Sigma)$. Assume that x is an element of $\mathrm{IM}(G, \Sigma)$ such that $\mathrm{reach}_L(x, c)$. We must have $x = c$. On the other hand, we have $\mathrm{reach}_L(y, c)$ for the element $y = (\{1, ab\}, 1) \in \mathrm{IM}(G, \Sigma') \setminus \mathrm{IM}(G, \Sigma)$. Thus, the sentence $\exists x : \mathrm{reach}_L(x, c) \ \wedge \ x \neq c$ belongs to the first-order theory of $\mathsf{R}(\mathrm{IM}(G, \Sigma'))$ but it does not belong to the first-order theory of $\mathsf{R}(\mathrm{IM}(G, \Sigma))$.

Let us finish this paper with some applications of Theorem 19. In the emptiness problem for boolean combinations of rational subsets of a monoid M one asks for a given boolean combination B of sets from $\mathrm{RAT}(M)$, whether $B = \emptyset$. Theorem 19 immediately implies:

Theorem 22. *Let G be a finitely generated virtually-free group and let P be a finite idempotent presentation over $\mathrm{IM}(G)$. Then the emptiness problem for boolean combinations of rational subsets of $\mathrm{IM}(G)/P$ is decidable.*

The membership problem problem for rational subsets of $\mathrm{IM}(G)/P$ (i.e., the question, whether a given element of $\mathrm{IM}(G)/P$ belongs to a given rational subset of $\mathrm{IM}(G)/P$) is clearly reducible to the emptiness problem for boolean combinations of rational subsets of $\mathrm{IM}(G)/P$. Hence, also the former problem is decidable. Since every finitely generated submonoid of a monoid M belongs to $\mathrm{RAT}(M)$, also the submonoid membership problem of $\mathrm{IM}(G)/P$ (i.e., the question, whether a given element of $\mathrm{IM}(G)/P$ belongs to a given finitely generated submonoid of $\mathrm{IM}(G)/P$) is decidable.

8. Open problems

The undecidability results from Section 5 make it hard to find non-virtually-free groups G such that for every finite idempotent presentation P over $\mathrm{IM}(G)$, the word problem of $\mathrm{IM}(G)/P$ is decidable. Moreover, our techniques from Section 7 can be definitely not extended beyond the virtually-free case: By a result from [10] the MSO-theory of the Cayley graph of a group G is decidable if and only if G is virtually-free. These results lead to an open problem, which we state as a conjecture: If G is not virtually-free, then there exists a finite idempotent presentation P over $\mathrm{IM}(G)$ such that the word problem for $\mathrm{IM}(G)/P$ is undecidable.

We have seen that the submonoid membership problem for a group G can be reduced to the word problem of some $\mathrm{IM}(G)/P$, but it is open whether we can reduce it to the word problem of some fixed finitely generated submonoid of $\mathrm{IM}(G)/P$.

Acknowledgment

The authors thank the anonymous referee for his detailed comments and bibliographical hints which helped to improve the presentation of the paper. In particular, we thank the referee that he forced us to prove Corollary 7 for a finitely presented monoid.

References

[1] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.
[2] J.-C. Birget, S. W. Margolis, and J. Meakin. The word problem for inverse monoids presented by one idempotent relator. *Theoretical Computer Science*, 123(2):273–289, 1994.
[3] J.-C. Birget and J. Rhodes. Almost finite expansions of arbitrary semigroups. *Journal of Pure and Applied Algebra*, 32(3):239–287, 1984.
[4] J.-C. Birget and J. Rhodes. Group theory via global semigroup theory. *Journal of Algebra*, 120:284–300, 1989.
[5] C. Choffrut and F. D'Alessandro. Commutativity in free inverse monoids. *Theoretical Computer Science*, 204(1–2):35–54, 1998.
[6] T. Deis, J. Meakin, and G. Sénizergues. Equations in free inverse monoids. *International Journal of Algebra and Computation*, 2005. Accepted for publication.
[7] V. Diekert, M. Lohrey, and A. Miller. Partially commutative inverse monoids. In R. Kralovic and P. Urzyczyn, editors, *Proceedings of the 31th International Symposium on Mathematical*

Foundations of Computer Science (MFCS 2006), Bratislave (Slovakia), number 4162 in Lecture Notes in Computer Science, pages 292–304. Springer, 2006. long version submitted.

[8] W. Hodges. *Model Theory*. Cambridge University Press, 1993.

[9] J. Kellendonk and M. V. Lawson. Partial actions of groups. *International Journal of Algebra and Computation*, 14(1):87–114, 2004.

[10] D. Kuske and M. Lohrey. Logical aspects of Cayley-graphs: the group case. *Annals of Pure and Applied Logic*, 131(1–3):263–286, 2005.

[11] M. Lohrey and N. Ondrusch. Inverse monoids: decidability and complexity of algebraic questions. To appear in *Information and Computation*, 2007.

[12] M. Lohrey and B. Steinberg. The submonoid and rational subset membership problems for graph groups. in preparation, 2007.

[13] S. Margolis and J. Meakin. E-unitary inverse monoids and the Cayley graph of a group presentation. *Journal of Pure and Applied Algebra*, 58(1):45–76, 1989.

[14] S. Margolis and J. Meakin. Inverse monoids, trees, and context-free languages. *Transactions of the American Mathematical Society*, 335(1):259–276, 1993.

[15] S. Margolis, J. Meakin, and M. Sapir. Algorithmic problems in groups, semigroups and inverse semigroups. In J. Fountain, editor, *Semigroups, Formal Languages and Groups*, pages 147–214. Kluwer, 1995.

[16] J. Meakin. Groups and semigroups: connections and contrasts. In C. Campbell, M. Quick, E. Robertson, and G. Smith, editors, *Proceedings of Groups St Andrews 2005*, number 340 in London Mathematical Society Lecture Note Series, pages 357–400. Cambridge University Press, 2007.

[17] J. Meakin and M. Sapir. The word problem in the variety of inverse semigroups with Abelian covers. *Journal of the London Mathematical Society, II. Series*, 53(1):79–98, 1996.

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

[19] D. E. Muller and P. E. Schupp. The theory of ends, pushdown automata, and second-order logic. *Theoretical Computer Science*, 37(1):51–75, 1985.

[20] W. Munn. Free inverse semigroups. *Proceedings of the London Mathematical Society*, 30:385–404, 1974.

[21] M. Petrich. *Inverse semigroups*. Wiley, 1984.

[22] M. O. Rabin. Decidability of second-order theories and automata on infinite trees. *Transactions of the American Mathematical Society*, 141:1–35, 1969.

[23] E. Rips. Subgroups of small cancellation groups. *Bulletin of the London Mathematical Society*, 14:45–47, 1982.

[24] B. V. Rozenblat. Diophantine theories of free inverse semigroups. *Siberian Mathematical Journal*, 26:860–865, 1985. English translation.

[25] G. Sénizergues. On the rational subsets of the free group. *Acta Informatica*, 33(3):281–296, 1996.

[26] P. V. Silva. Rational languages and inverse monoid presentations. *International Journal of Algebra and Computation*, 2:187–207, 1992.

[27] P. V. Silva. On free inverse monoid languages. *R.A.I.R.O. — Informatique Théorique et Applications*, 30:349–378, 1996.

[28] M. B. Szendrei. A note on Birget-Rhodes expansion of groups. *Journal of Pure and Applied Algebra*, 58(1):93–99, 1989.

[29] D. T. Wise. A residually finite version of Rips's construction. *Bulletin of the London Mathematical Society*, 35(1):23–29, 2003.