Existential and Positive Theories of Equations in Graph Products

Volker Diekert, Markus Lohrey
Universität Stuttgart, Institut für Informatik
Breitwiesenstr. 20–22, 70565 Stuttgart, Germany
{diekert,lohrey}@informatik.uni-stuttgart.de

April 28, 2003

Abstract

We prove that the existential theory of equations with normalized rational constraints in a fixed graph product of finite monoids, free monoids, and free groups is PSPACE-complete. Under certain restrictions this result also holds if the graph product is part of the input. As the second main result we prove that the positive theory of equations with recognizable constraints in graph products of finite and free groups is decidable.

1 Introduction

Since the seminal work of Makanin [25] on equations in free monoids, the decidability of various theories of equations in different monoids and groups has been studied, and several new decidability and complexity results have been shown. Let us mention here the results of [37, 40] for free monoids, [7, 18, 26, 27] for free groups, [10] for free partially commutative monoids (trace monoids), [11] for free partially commutative groups (graph groups), [9] for plain groups (free products of finite and free groups), and [39] for torsion-free hyperbolic groups.

In this paper we continue this stream of research. We will present two main results. The first one concerns existential theories of equations. We start with the definition of a class of monoids, which are constructed from finite monoids, free monoids, and free groups using the graph product construction, which is a well-known construction in mathematics, see e.g. [17, 20] This class of graph products strictly covers the classes mentioned above up to the class torsion-free hyperbolic groups, which is in some sense orthogonal to the classes considered here. We prove that for such a graph product the existential theory of equations can be decided in PSPACE. It becomes PSPACE-complete if we switch to the theory of equations with constraints. These constraints are taken from a class of sets, called normalized rational sets, which (in general) lies strictly between the class of recognizable and rational sets. Furthermore under certain restrictions our PSPACE upper-bound holds also in the case that (a suitable description of) the graph product is part of the input.

Our second main result concerns positive theories of equations. We prove that if we restrict our class of graph products to groups, then for each group from the resulting class the positive theory of equations with recognizable constraints for the variables is decidable. Under certain restrictions we obtain an elementary upper bound. This result extends the well-known result of Makanin for free groups [26, 27] to graph products of free and finite groups, which include in particular free partially commutative groups (graph groups), see [13], and plain groups, see [19]. The technical part relies on a generalization of the techniques introduced by Merzlyakov for free groups [31].

We assume some basic familiarity with monoid presentations, see e.g. [23] and computational complexity, see e.g. [36].

2 Monoids with involution

An *involution* on a set is a mapping $\overline{}$ such that $\overline{\overline{a}} = a$ for all elements a. For an involution on a monoid we demand in addition that both $\overline{ab} = \overline{b}\,\overline{a}$ and $\overline{1} = 1$, where 1 is the neutral element of the monoid. Taking the inverse in a group is an example of an involution. Another example is the lifting of an involution $\overline{} : \Delta \to \Delta$ to the free monoid Δ^* defined by $\overline{a_1 \cdots a_n} = \overline{a}_n \cdots \overline{a}_1$ for $a_i \in \Delta$.

Throughout the paper we consider finitely generated monoids, only. Thus, every monoid M is given together with a presentation $\pi : \Gamma^* \to M$, where Γ is a finite alphabet and π is a surjective monoid homomorphism. Furthermore, we denote by $\mathcal{I}(M)$ a submonoid of M such that an involution $\overline{} : \mathcal{I}(M) \to \mathcal{I}(M)$ is defined on it. We require that there is a subalphabet $\Delta \subseteq \Gamma$ together with an involution $\overline{} : \Delta \to \Delta$ (there will be no risk to confuse the involution $\overline{} : \Delta \to \Delta$ with the involution $\overline{} : \mathcal{I}(M) \to \mathcal{I}(M)$) such that $\pi^{-1}(\mathcal{I}(M)) = \Delta^*$ and $\pi(\overline{u}) = \overline{\pi(u)}$ for all $u \in \Delta^*$. In many cases we choose $\mathcal{I}(M)$ to be the submonoid of elements having left- and right-inverses, i.e., $\mathcal{I}(M)$ is the group of units of M, but this is not necessarily the case, for instance for $M = \Gamma^*$ we take $\mathcal{I}(M) = \Delta^*$.

We assume that the alphabet Γ is endowed with a linear order $\prec$, which is lifted to Γ^* by ordering Γ^* length-lexicographically: $u \prec v$ for $u, v \in \Gamma^*$ if either $|u| < |v|$ or $|u| = |v|$ and u is lexicographical less then v (with respect to the order $\prec$ on Γ). For $x \in M$ we denote by $\mathrm{llnf}(x)$ the smallest word in $\pi^{-1}(x)$ with respect to $\prec$. If we want to emphasize that llnf is considered as a mapping from M to Γ^*, we write $\mathrm{llnf}_M(x)$ instead of $\mathrm{llnf}(x)$. A subset $L \subseteq M$ is called

- *recognizable* if $\pi^{-1}(L) \subseteq \Gamma^*$ is regular,
- *normalized rational* if $\mathrm{llnf}(L) \subseteq \Gamma^*$ is regular, and
- *rational* if $L = \pi(L')$ for some regular language $L' \subseteq \Gamma^*$.

The corresponding classes are denoted by $\mathrm{REC}(M)$, $\mathrm{NRAT}(M)$, and $\mathrm{RAT}(M)$, respectively. The classes $\mathrm{REC}(M)$ and $\mathrm{RAT}(M)$ are classical, see e.g. [4]. Their definitions do not depend on π as can be seen easily. Since we deal with finitely generated monoids only, we have $\mathrm{REC}(M) \subseteq \mathrm{NRAT}(M) \subseteq \mathrm{RAT}(M)$. Moreover, $\mathrm{REC}(M)$ is a Boolean algebra, but for instance $\mathrm{RAT}(\mathbb{N} \times \{a,b\}^*)$ is not a Boolean algebra, since it is not closed under intersection, see e.g. [12, Example 6.1.16]. For $\mathrm{NRAT}(M)$ we can state the following lemma. The proof is easy and therefore omitted.

Proposition 1. *The class of normalized rational languages* $\mathrm{NRAT}(M)$ *is a Boolean algebra if and only if the set of length-lexicographic normal forms* $\mathrm{llnf}(M)$ *is regular (i.e.,* $M \in \mathrm{NRAT}(M)$*).*

In all cases we are going to consider, $\mathrm{NRAT}(M)$ will be a Boolean algebra.

Let us end this section with the discussion of some special cases which are of interest for us. For a free monoid M we have $\mathrm{REC}(M) = \mathrm{NRAT}(M) = \mathrm{RAT}(M)$ by Kleene's Theorem. If M is an infinite group then $\mathrm{REC}(M) \subsetneq \mathrm{NRAT}(M)$, since every finite subset of M is normalized rational but not recognizable, see e.g. [4]. For a free group M, $\mathrm{llnf}(M)$ is the set of freely reduced words, and we have $\mathrm{NRAT}(M) = \mathrm{RAT}(M)$ by a result due to Benois [2]. For a free partially commutative monoid (trace monoid) we have $\mathrm{REC}(M) = \mathrm{NRAT}(M)$ (this is Ochmanski's Theorem [35]) but $\mathrm{NRAT}(M) \subsetneq \mathrm{RAT}(M)$ as soon as M is not free. In fact the rational subset $(1,1)^*$ is not recognizable in $\mathbb{N} \times \mathbb{N}$. Finally for the group $\mathbb{Z} \times \mathbb{Z}$, we have $\mathrm{REC}(M) \subsetneq \mathrm{NRAT}(M) \subsetneq \mathrm{RAT}(M)$.

3 Graph products

Let (V, E) be a finite undirected graph with vertex set V and edge set $E \subseteq \binom{V}{2}$. Every node $n \in V$ is labeled with a monoid M_n which is either a free monoid, a free group, or a finite monoid. In fact, it is enough (and convenient) to assume that M_n is either isomorphic to $\mathbb{N}$ or to $\mathbb{Z}$, or M_n is finite. The *graph product* defined by (V, E) is the quotient monoid

$$\mathbb{P} = (*_{n \in V} M_n)/\{uv = vu \mid \exists m, n \in V : m \neq n, (m,n) \notin E, u \in M_n, v \in M_n\},$$

where $*_{n \in V} M_n$ denotes the free product of the monoids M_n, $n \in V$. Thus, commutation is only allowed between elements that belong to different and non-adjacent monoids. We have defined graph products only where each component is either a free monoid or a free group or a finite monoid. Graph products in a more general setting are investigated in [41, 17, 20]. If all M_n are equal to $\mathbb{N}$, then we obtain *free partially commutative monoids* (*trace monoids*) [6, 30]. If all M_n are equal to $\mathbb{Z}$, we obtain *free partially commutative groups*, which are also known as *graph groups* [13]. Free groups and free commutative groups arise as the extreme cases. If $E = \binom{V}{2}$ and all M_n are groups, then we obtain *plain groups* in the sense of Haring-Smith [19].

3.1 Free partially commutative monoids with involution

As already mentioned, free partially commutative monoids (trace monoids) arise as a special case of graph products. It is convenient to specify a trace monoid by a *dependence relation* on an alphabet Γ, which is a reflexive and symmetric relation $D \subseteq \Gamma \times \Gamma$. The *independence relation* corresponding to I is the complementary relation $I = (\Gamma \times \Gamma) \setminus D$. The pair (Γ, D) (resp. (Γ, I)) is called a *dependence alphabet* (resp. an *independence alphabet*). Given a dependence alphabet (Γ, D), we define the *free partially commutative monoid* (*trace monoid*) $\mathbb{M} = \mathbb{M}(\Gamma, D)$ as the quotient monoid $\Gamma^*/\{ab = ba \mid (a,b) \in I\}$. Extreme cases are free monoids (if $D = \Gamma \times \Gamma$) and and free commutative monoids (if $D = \mathrm{Id}_\Gamma = \{(a,a) \mid a \in \Gamma\}$). An element of $\mathbb{M}$, i.e., an equivalence class of words, is called a *trace*. Let $\tau : \Gamma^* \to \mathbb{M}$ be the canonical morphism, mapping a word $s \in \Gamma^*$ to the trace $\tau(s)$ that contains s. The neutral element of $\mathbb{M}$ is the empty trace $\tau(\epsilon)$ which will be denoted by 1. Let $t = \tau(s) \in \mathbb{M}$ be a trace. The length of t is $|t| = |s|$. Furthermore, we define $\mathrm{alph}(t) = \mathrm{alph}(s)$, where $\mathrm{alph}(s) \subseteq \Gamma$ is the set of symbols occuring in the word s. For two traces $t, u \in \mathbb{M}$ we write $(t,u) \in I$ if $\mathrm{alph}(t) \times \mathrm{alph}(u) \subseteq I$.

By definition, $L \in \mathrm{REC}(\mathbb{M})$ if and only if $\tau^{-1}(L) \subseteq \Gamma^*$ is regular. As already mentioned in Section 2, for a trace monoid $\mathbb{M}$ we have $\mathrm{REC}(\mathbb{M}) = \mathrm{NRAT}(\mathbb{M})$ by Ochmanski's Theorem [35] but $\mathrm{NRAT}(\mathbb{M}) \subsetneq \mathrm{RAT}(\mathbb{M})$ as soon as $\mathbb{M}$ is not free. In particular, $\mathrm{NRAT}(\mathbb{M})$ is a Boolean algebra. Moreover $\mathrm{NRAT}(\mathbb{M}) = \mathrm{REC}(\mathbb{M})$ is also closed under concatenation and connected Kleene stars, see [12] for definitions.

Given $\Delta \subseteq \Gamma$ with an involution $^- : \Delta \to \Delta$, we say that $^-$ is *compatible* with $D \subseteq \Gamma \times \Gamma$ if for all $a \in \Gamma$, $b \in \Delta$ we have $(a, \overline{b}) \in D$ if and only if $(a,b) \in D$. If this holds, then the lifting $^- : \Delta^* \to \Delta^*$ as defined in Section 2 satisfies $\tau(u) = \tau(v)$ if and only if $\tau(\bar{u}) = \tau(\bar{v})$ for all $u, v \in \Delta^*$. Thus, we may consider $^-$ also as a partially defined involution on $\mathbb{M}$ with domain $\Delta^* \in \mathrm{REC}(\mathbb{M})$, and we call $(\mathbb{M}, ^-)$ a *trace monoid with involution*.

A suitable visualization of a trace is given by its *dependence graph* which is a node labeled acyclic graph. Let $t = \tau(a_1 \cdots a_m) \in \mathbb{M}$, $a_i \in \Gamma$. Define the dependence graph $D_t = (V, \to, \lambda)$ of t as the node-labeled graph, consisting of the node set $V = \{1, \ldots, m\}$, the edge set $\to = \{(i,j) \mid i < j, (a_i, a_j) \in D\}$, and the labeling function λ defined by $\lambda(i) = a_i$. It is easy to see that up to isomorphism another word representing t yields the same dependence graph. The transitive reflexive closure $\xrightarrow{*}$ of the edge relation defines a partial order on V. Given a subset $U \subseteq V$ of the nodes such that $j \in U$ whenever $i \xrightarrow{*} j \xrightarrow{*} k$ and $i, k \in U$, it is easy to see that the restricted dependence graph $D_t\restriction_U$ is itself a dependence graph, i.e., $D_t\restriction_U$ is isomorpic to D_u for some trace u. In this case, we say that U is an *occurrence* of the trace u in t.

As a consequence of the representation of traces by dependence graphs, one obtains Levi's Lemma for traces, see e.g. [12, p 74] which is one of the fundamental facts in trace theory. The formal statement is as follows.

Lemma 2. *Let $u_1, \ldots, u_m, v_1, \ldots, v_n \in \mathbb{M}$. Then $u_1 u_2 \cdots u_m = v_1 v_2 \cdots v_n$ if and only if there exist $w_{i,j} \in \mathbb{M}$ $(1 \le i \le m,\ 1 \le j \le n)$ such that*

- *$u_i = w_{i,1} w_{i,2} \cdots w_{i,n}$ for every $1 \le i \le m$,*

- $v_j = w_{1,j} w_{2,j} \cdots w_{m,j}$ *for every* $1 \le j \le n$, *and*
- $(w_{i,j}, w_{k,\ell}) \in I$ *if* $1 \le i < k \le m$ *and* $1 \le \ell < j \le n$.

The situation in the lemma will be visualized by a diagram of the following kind. The i–th column corresponds to u_i, the j–th row corresponds to v_j and the intersection of the i–th column and the j–th row represents $w_{i,j}$. Furthermore $w_{i,j}$ and $w_{k,\ell}$ are independent if one of them is right-above the other one.

v_n	$w_{1,n}$	$w_{2,n}$	$w_{3,n}$	$\cdots$	$w_{m,n}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
v_3	$w_{1,3}$	$w_{2,3}$	$w_{3,3}$	$\cdots$	$w_{m,3}$
v_2	$w_{1,2}$	$w_{2,2}$	$w_{3,2}$	$\cdots$	$w_{m,2}$
v_1	$w_{1,1}$	$w_{2,1}$	$w_{3,1}$	$\cdots$	$w_{m,1}$
	u_1	u_2	u_3	$\cdots$	u_m

3.2 Trace rewriting systems

Another important tool in this paper are *trace rewriting systems*, which generalize semi-Thue systems [5, 21] from words to traces. Formally, a trace rewriting system over $\mathbb{M} = \mathbb{M}(\Gamma, D)$ is a finite subset $S \subseteq \mathbb{M} \times \mathbb{M}$. Analogously to semi-Thue systems, the one-step rewrite relation $\to_S \subseteq \mathbb{M} \times \mathbb{M}$ of a trace rewriting system S is defined by $s \to_S t$ if $s = u\,\ell\,v$ and $t = u\,r\,v$ for some $(\ell, r) \in S$ and $u, v \in \mathbb{M}$. Its transitive reflexive closure is $\xrightarrow{*}_S$. Let $\mathrm{RED}(S) = \{u\,\ell\,v \mid u, v \in \mathbb{M},\ \exists r : (\ell, r) \in S\}$ be the set of *reducible traces* and $\mathrm{IRR}(S) = \mathbb{M} \backslash \mathrm{RED}(S)$ be the set of *irreducible* traces. Due to the closure properties of $\mathrm{REC}(\mathbb{M})$, both $\mathrm{RED}(S)$ and $\mathrm{IRR}(S)$ are recognizable. The trace rewriting system S is called *length-reducing* if $(\ell, r) \in S$ implies $|\ell| > |r|$. Finally, S is called *confluent*, if for all $s, t, u \in \mathbb{M}$ with $s \xrightarrow{*}_S t$ and $s \xrightarrow{*}_S u$ there exists $v \in \mathbb{M}$ with $t \xrightarrow{*}_S v$ and $u \xrightarrow{*}_S v$. If S is length-reducing, then by Newman's Lemma [34] confluence is equivalent to *local confluence*, i.e., if $s \to_S t$ and $s \to_S u$, then there exists $v \in \mathbb{M}$ with $t \xrightarrow{*}_S v$ and $u \xrightarrow{*}_S v$. In general, it is undecidable whether a finite length-reducing trace rewriting system is confluent, see [33]. This is in sharp contrast to semi-Thue systems, and makes confluence proofs challenging. However, if S is length-reducing and confluent, then still for every $s \in \mathbb{M}$ there exists a unique $t \in \mathrm{IRR}(S)$ with $s \xrightarrow{*}_S t$.

3.3 The trace monoid underlying a graph product

For our further considerations, graph products are best described in terms of an underlying trace monoid with involution. Let $\mathbb{P}$ be a graph product, specified by a graph (V, E), where each node $n \in V$ is labeled with a monoid M_n, which is either finite, or $\mathbb{N}$, or $\mathbb{Z}$. Let $\mathcal{I}(M_n)$ be the subgroup of units of M_n, i.e., $\mathcal{I}(M_n) = \{a \in M_n \mid \exists b : ab = ba = 1 \text{ in } M_n\}$. If $M_n = \mathbb{N}$, then we let $\Gamma_n = \{a_n\}$ and $\Delta_n = \emptyset$. If $M_n = \mathbb{Z}$, then we let $\Gamma_n = \Delta_n = \{a_n, \overline{a}_n\}$. Finally, if M_n is finite, then we let $\Gamma_n = M_n \backslash \{1\}$ and $\Delta_n = \mathcal{I}(M_n) \backslash \{1\}$. Thus, for each

$n \in V$ we have a canonical presentation $\pi_n : \Gamma_n^* \to M_n$. Moreover, $\pi_n^{-1}(\mathcal{I}(M_n)) = \Delta_n^*$. For $M_n = \mathbb{N}$ or $M_n = \mathbb{Z}$ this is clear, for a finite M_n note that if $uv \in \mathcal{I}(M_n)$, then $u, v \in \mathcal{I}(M_n)$, too. We may assume that the alphabets Γ_n are pairwise disjoint. Let $\Gamma = \bigcup_{n\in V} \Gamma_n$ and $\Delta = \bigcup_{n\in V} \Delta_n$. Hence, the π_n, $n \in V$, can be extended to a presentation $\pi : \Gamma^* \to \mathbb{P}$ such that $\pi^{-1}(\mathcal{I}(\mathbb{P})) = \Delta^*$, where $\mathcal{I}(\mathbb{P})$ is the group of units of $\mathbb{P}$. Furthermore, there is a natural involution $\overline{}$ on Δ, which has fixed points as soon as some finite M_n contains an element of order two. We define a dependence relation $D \subseteq \Gamma \times \Gamma$ by $D = \bigcup_{(m,n)\in E\cup \mathrm{Id}_V} (\Gamma_m \times \Gamma_n)$. Let I be the corresponding independence relation. The basic reference monoid for the further consideration is the trace monoid $\mathbb{M} = \mathbb{M}(\Gamma, D)$. Since $\overline{} : \Delta \to \Delta$ is compatible with D, we can lift $\overline{} : \Delta^* \to \Delta^*$ to a partially defined involution on $\Delta^* \in \mathrm{REC}(\mathbb{M})$. We say that $(\mathbb{M}, \overline{})$ is the *trace monoid with involution underlying* $\mathbb{P}$. We now define a trace rewriting system S by

$$S = \{(a\overline{a}, 1) \mid a \in \Delta\} \cup \{(ab, c) \mid \exists n \in V : a, b, c \in \Gamma_n,\ ab = c \text{ in } M_n\}.$$

Then $\mathbb{P}$ can be defined as the quotient monoid $\mathbb{P} = \mathbb{M}/\{\ell = r \mid (\ell, r) \in S\}$. Clearly $\mathbb{P} = \Gamma^*/(\{ab = ba \mid (a, b) \in I\} \cup \{\ell = r \mid (\ell, r) \in S\})$. Furthermore, the canonical homomorphism $\pi : \Gamma^* \to \mathbb{P}$ factorizes as $\pi = \tau \circ \psi$, where $\tau : \Gamma^* \to \mathbb{M}$ and $\psi : \mathbb{M} \to \mathbb{P}$. Elements of both $\mathbb{M}$ and $\mathbb{P}$ will be represented as words from Γ^*. It will be always clear from the context, whether an element of Γ^*, $\mathbb{M}$, or $\mathbb{P}$, respectively, is denoted. The following proposition will be important for the further investigation.

Proposition 3. *The trace rewriting system S is confluent.*

Proof. We use Lemma 2.3. from [24].[1] According to this lemma it suffices to consider for all rules $(ab, d), (bc, e) \in S$ and all traces $w \in \mathbb{M}$ such that $(b, w) \in I$ the following situation: $dwc \;{}_S\!\leftarrow abwc = awbc \to_S awe$. We have to show that there exists $s \in \mathbb{M}$ such that $dwc \overset{*}{\to}_S s$ and $awe \overset{*}{\to}_S s$. Note that $a, b, c \in \Gamma_n$ for some $n \in V$. Since $(b, w) \in I$, also each of the traces a, c, d, and e is independent from w. Thus, it suffices to show that $dc \overset{*}{\to}_S s$ and $ae \overset{*}{\to}_S s$ for some s (then also $dwc = wdc \overset{*}{\to}_S ws$ and $awe = wae \overset{*}{\to}_S ws$). But this is easy. Let us consider for instance the case that $b = \overline{a}$, $d = 1$, and $e \in \Gamma_n$. Thus, $\overline{a}c = e$, i.e., $c = ae$ in M_n, and (ae, c) is a rule of S. Hence, we can choose $s = c$. $\square$

Since S is also length-reducing, Proposition 3 implies:

Corollary 4. *For each $x \in \mathbb{P}$ the set $\psi^{-1}(x) \subseteq \mathbb{M}$ contains a unique shortest trace, which will be denoted by $\mu(x) \in \mathbb{M} \cap \mathrm{IRR}(S)$.*

Since $\mathrm{llnf}_{\mathbb{P}} : \mathbb{P} \to \Gamma^*$ factorizes as $\mathrm{llnf}_{\mathbb{P}} = \mu \circ \mathrm{llnf}_{\mathbb{M}}$, Ochmanski's Theorem implies that $\mathrm{llnf}_{\mathbb{P}}(L) \subseteq \Gamma^*$ is regular if and only if $\mu(L) \in \mathrm{REC}(\mathbb{M})$. Thus, we obtain:

Corollary 5. *We have $L \in \mathrm{NRAT}(\mathbb{P})$ if and only if $\mu(L) \in \mathrm{REC}(\mathbb{M})$ if and only if $\tau^{-1}(\mu(L)) \in \mathrm{REC}(\Gamma^*)$.*

[1]One can argue also directly by an application of Lemma 2 similarly to the proof of Lemma 25.

In particular, we see that $\mathrm{NRAT}(\mathbb{P})$ does not depend on the linear order $\prec$ chosen for Γ. It depends on the canonical homomorphism $\pi : \Gamma^* \to \mathbb{P}$, only. Furthermore, since $\mu(\mathbb{P}) = \mathrm{IRR}(S) \in \mathrm{REC}(\mathbb{M})$ we have $\mathbb{P} \in \mathrm{NRAT}(\mathbb{P})$. Thus, Lemma 1 implies:

Corollary 6. *The class* $\mathrm{NRAT}(\mathbb{P})$ *is an effective Boolean algebra.*

The following diagram shows all relevant mappings, introduced so far. Surjective homomorphisms are indicated by $\twoheadrightarrow$-arrows, whereas $\hookrightarrow$-arrows indicate injective mappings. The diagram is commutative for all paths which do not finish by an injection.

$$\begin{tikzcd} \Gamma^* \arrow[r, two heads, shift left, "\tau"] \arrow[dr, two heads, shift left, "\pi"] & \mathbb{M} \arrow[l, hook, shift left, "\mathrm{llnf}_{\mathbb{M}}"] \arrow[d, two heads, shift left, "\psi"] \\ & \mathbb{P} \arrow[ul, hook, shift left, "\mathrm{llnf}_{\mathbb{P}}"] \arrow[u, hook, shift left, "\mu"] \end{tikzcd}$$

4 Theories of equations with constraints

Let M be a monoid as in Section 2 and let $\mathcal{C}$ be a family of subsets of M such that $\mathcal{I}(M) \in \mathcal{C}$. Let Ω be a set of variables and $\overline{\Omega} = \{\overline{X} \mid X \in \Omega\}$ a disjoint copy of Ω. An *equation* is a pair (U, V) with $U, V \in (\Gamma \cup \Omega \cup \overline{\Omega})^*$, it is written as $U = V$. A *constraint* is an expression of the form $X \in L$ with $X \in \Omega \cup \overline{\Omega}$ and $L \in \mathcal{C}$. Equations and constraints are called *atomic formulae*. From these we construct *first-order formulae* using conjunctions, disjunctions, negations, and universal and existential quantifications over variables from Ω. A *first-order sentence* is a first-order formula without free variables, where a quantification over $X \in \Omega$ binds both X and $\overline{X}$. We impose the syntactical restriction that whenever we use a variable $\overline{X} \in \overline{\Omega}$ in a first-order sentence, then the quantification over X is implicitly restricted to $\mathcal{I}(M)$. For instance $\forall X : X\overline{X} = 1$ is interpreted as $\forall X \in \mathcal{I}(M) : X\overline{X} = 1$. Given $\pi : \Gamma^* \to M$, $\mathcal{I}(M)$, the involution $\overline{} : \mathcal{I}(M) \to \mathcal{I}(M)$, and a first-order sentence ϕ, we can evaluate ϕ over M in the obvious way with the restriction that if a variable X evaluates to $x \in M$, then $\overline{X}$ must evaluate to $\overline{x}$. The *theory of equations with constraints in* $\mathcal{C}$, briefly $\mathrm{Th}(M, \mathcal{C})$, denotes the set of all first-order sentences that are true in M. A well-known example of a decidable theory of equations is Presburger Arithmetic [38]. Translated into our framework, the results of [16] give us the following:

Proposition 7. *The theories* $\mathrm{Th}(\mathbb{N}^k, \mathrm{RAT}(\mathbb{N}^k))$ *and* $\mathrm{Th}(\mathbb{Z}^k, \mathrm{RAT}(\mathbb{Z}^k))$ *are decidable in doubly exponential space.*

Remark 8. *Precise complexity bounds can be derived from the results in [3], which show that the theories in Proposition 7 are complete for doubly exponential alternating time with only a linear number of alternations.*

Note that $\mathrm{RAT}(\mathbb{N}^k)$ and $\mathrm{RAT}(\mathbb{Z}^k)$ are the classes of semilinear sets in $\mathbb{N}^k$ and $\mathbb{Z}^k$, respectively. The following result can be easily deduced from Proposition 7 since the free product $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ of two copies of $\mathbb{Z}/2\mathbb{Z}$ is isomorphic to the semi-direct product of $\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$.

Corollary 9. *For $M = \mathbb{Z}/2\mathbb{Z}*\mathbb{Z}/2\mathbb{Z}$, the theory $\mathrm{Th}(M, \mathrm{RAT}(M))$ is elementary decidable.*

Proof. Let $M = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ be given by the generators a, b and the defining relations $a^2 = b^2 = 1$. Every $x \in M$ can be represented uniquely as $x = (ab)^i a^j$ where $i \in \mathbb{Z}$ and $j \in \{0, 1\}$ (note that $(ab)^{-1} = ba$ in M). The subgroup K of M generated by ab is isomorphic to $\mathbb{Z}$. Furthermore let $Q \simeq \mathbb{Z}/2\mathbb{Z}$ be the subgroup of M generated by a. It is easy to see that M is the semidirect product of K by Q, thus $M \simeq \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. An isomorphism $\sigma : M \to \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ can be defined by $\sigma((ab)^i a^j) = (i, j)$, where $i \in \mathbb{Z}$ and $j \in \{0, 1\}$. In the following let $\sigma(x) = (n_x, a_x)$. Thus, $xy = z$ in M if and only if $n_z = n_x + (-1)^{a_x} n_y \ \wedge \ a_x + a_y \equiv a_z \mod 2$. Furthermore, it is easy to see that if $L \in \mathrm{RAT}(M)$, then $\sigma(L) = S_0 \times \{0\} \cup S_1 \times \{1\}$ where $S_0, S_1 \subseteq \mathbb{Z}$ are semilinear sets that can be constructed inductively from a rational expression for L, with at most an exponential size increase.

Now given a first-order sentence ϕ we replace every quantification $\exists X$ by $\exists n_X \in \mathbb{Z} \bigvee_{a_X \in \{0,1\}}$ (similarly for $\forall$-quantifications). Using standard methods, see e.g. [7], we may assume that all equalities $U = V$ are triangulated, i.e., $|U| = 2, |V| = 1$. An equation $AB = C$, where $A, B, C \in \Omega \cup \overline{\Omega} \cup \{a, b\}$, is replaced by $(n_C = n_A + (-1)^{a_B} n_B \wedge a_A + a_B \equiv a_C \mod 2)$, where n_A, a_A are either new variables (if $A \in \Omega \cup \overline{\Omega}$) or integer constants, similarly for B and C. A constraint $X \in L$ with $L \in \mathrm{RAT}(M)$ is replaced by $(n_X \in S_0 \ \wedge \ a_X = 0) \vee (n_X \in S_1 \ \wedge \ a_X = 1)$ where $\sigma(L) = S_0 \times \{0\} \cup S_1 \times \{1\}$. Occurrences of the variables $n_{\overline{X}}$ and $a_{\overline{X}}$ for $\overline{X} \in \overline{\Omega}$ can be replaced by $(-1)^{a_X+1} \cdot n_X$ and $1 - a_X$, respectively. Finally by substituting for the variables a_X the values 0 and 1 we obtain a Presburger formula. Now the corollary follows from Proposition 7. $\square$

The *positive theory of equations with constraints in $\mathcal{C}$* is the set of all sentences in $\mathrm{Th}(M, \mathcal{C})$ that do not use negations. The *existential theory of equations with constraints in $\mathcal{C}$* is the set of all sentences in $\mathrm{Th}(M, \mathcal{C})$ that are in prenex normal form without universal quantifiers.

In this paper we will be interested in existential and positive theories of graph products. Constraints will be taken from the class $\mathrm{NRAT}(\mathbb{P})$ or $\mathrm{REC}(\mathbb{P})$. Note that $\mathcal{I}(\mathbb{P}) \in \mathrm{REC}(\mathbb{P})$ since $\pi^{-1}(\mathcal{I}(\mathbb{P})) = \Delta^*$ is regular. Since we will also deal with complexity issues, we have to define the input length of a formula. A constraint $X \in L$ with $L \in \mathrm{NRAT}(\mathbb{P})$ is represented by some finite non-deterministic automaton that accepts $\tau^{-1}(\mu(L)) \in \mathrm{REC}(\Gamma^*)$. For a recognizable constraint $X \in L \in \mathrm{REC}(\mathbb{P})$ it will be more convenient, to represent it by by some finite non-deterministic automaton that accepts $\pi^{-1}(L) \in \mathrm{REC}(\Gamma^*)$. Using these representations, we assume some standard binary coding of formulae. The input length of a formula is the length of this coding. In order to obtain existing results for free monoids as special cases, we will put a description of the graph product $\mathbb{P}$ into the input, too. This description contains the adjacency matrix of (V, E), and for each node either the multiplication table of M_n if M_n is finite or a bit indicating whether $M_n = \mathbb{N}$ or $M_n = \mathbb{Z}$.

5 Existential theories

The main result of this section is that the existential theory of equations with constraints in $\mathrm{NRAT}(\mathbb{P})$ is decidable in PSPACE. First, we will recall some results from [11] concerning existential theories of equations in trace monoids with involution. Based on these results, we will prove our main result in Section 5.2.

5.1 Existential theories of equations in trace monoids

All our decidability results will be based on the main result from [11]. In order to state this result, we have to introduce the following graph theoretical concept: Let (V, E) be a finite graph. A *complete clan* in (V, E) is a maximal clique $A \subseteq V$ in (V, E) such that for all $a, b \in A$ and $c \in V \setminus A$, $(a, c) \in E$ if and only if $(b, c) \in E$. The set of complete clans in (V, E) is easily seen to be a partition of V. A complete clan A is called *thin*, if there are $a \in A$ and $b \in V \backslash A$ such that $(a, b) \notin E$. The number of complete thin clans in (V, E) is denoted by $c(V, E)$, it is obviously at most $|V|$. Moreover, $c(V, E) \neq 1$, and $c(V, E) = 0$ if and only if (V, E) is a complete graph. Now we can state the main result from [11].

Theorem 10. *For every $k \geq 0$, the following problem is in PSPACE:*

INPUT: A dependence alphabet (Γ, D) with $c(\Gamma, D) \leq k$, a partially defined involution $\overline{} : \Delta \to \Delta$, $\Delta \subseteq \Gamma$, which is compatible with D, and an existential sentence ϕ with constraints in $\mathrm{REC}(\mathbb{M}(\Gamma, D))$.

QUESTION: Is ϕ true in the trace monoid with involution $(\mathbb{M}(\Gamma, D), \overline{})$?

If $c(\Gamma, D)$ is not bounded by a constant, then this problem is in EXPSPACE.

A few remarks should be made on Theorem 10. First, in [11] this result is only stated for a completely defined involution $\overline{} : \Gamma \to \Gamma$. But if $\overline{}$ is only defined on $\Delta \subsetneq \Gamma$, then we can introduce a new dummy symbol $\overline{a}$ for every $a \in \Gamma \backslash \Delta$ and add for every variable X the recognizable constraint $X \in \Gamma^*$. Second, the uniform EXPSPACE upper bound for the case that $c(\Gamma, D)$ is not bounded by a constant is not explicitly stated in the preliminary version [11], but it can be easily derived from the proof in [11] and will appear in the full version of [11]. Finally, Theorem 10 cannot be extended to the case of rational constraints: For $M = \{a, b\}^* \times \{c, d\}^*$ it is undecidable whether $L_1 \cap L_2 = \emptyset$ for given $L_1, L_2 \in \mathrm{RAT}(M)$, see [1]. A further investigation leads to the following characterization of Muscholl, see [32, Prop. 2.9.2, Prop. 2.9.3].

Proposition 11. *Let $\mathbb{M}$ be a trace monoid. Then the existential theory of equations with constraints in $\mathrm{RAT}(\mathbb{M})$ is decidable, if and only if $\mathbb{M}$ is a free product of free commutative monoids, i.e., $\mathbb{M} = *_{i=1}^{n} \mathbb{N}^{k_i}$ for $n, k_i \in \mathbb{N}$.*

5.2 Existential theories of equations in graph products

In this section we prove that for a graph product $\mathbb{P}$ as considered in Section 3 the existential theory of equations with constraints in $\mathrm{NRAT}(\mathbb{P})$ is decidable. The main reduction step is based on the following theorem:

Theorem 12. *For every $k \geq 0$ there is a polynomial time algorithm such that:*

- *The input consists of a graph product $\mathbb{P}$, specified by a graph (V, E) with $c(V, E) \leq k$, and an existential sentence ϕ with constraints in* $\mathrm{NRAT}(\mathbb{P})$.
- *On a given input $(\mathbb{P}, \phi)$, the algorithm produces an existential sentence ϕ' with constraints in* $\mathrm{REC}(\mathbb{M})$ *such that ϕ holds in $\mathbb{P}$ if and only if ϕ' holds in $(\mathbb{M}, \overline{})$, the trace monoid with involution underlying $\mathbb{P}$.*

Let us fix for the rest of this section a graph product $\mathbb{P}$, specified by a graph (V, E), where every node $n \in V$ is labeled by a monoid M_n, which is either finite, or $\mathbb{N}$, or $\mathbb{Z}$. Let $(\mathbb{M}, \overline{})$, Γ, D, I, $\pi = \tau \circ \psi$, and S have the same meaning as in Section 3.3.

The next lemma is the main technical tool for proving Theorem 12. First we need some further definitions concerning traces. The set $\mathcal{F} \subseteq \mathrm{IRR}(S) \subseteq \mathbb{M}$ consists of all traces $a_1 \cdots a_n$, $a_i \in \Gamma$, such that $(a_i, a_j) \in I$ if $i \neq j$. Thus, traces in $\mathcal{F}$ correspond to independence cliques of (Γ, I). Note that if $u \in \mathcal{F}$, then the length of u is at most $|\Gamma|$. More precisely, $|u| \leq c(V, E)+1$, thus $|\mathcal{F}| \leq |\Gamma|^{c(V,E)+1}$. We identify $u \in \mathcal{F}$ with the set of symbols that occur in u. For $s \in \mathbb{M}$ the set of maximal symbols $\max(s) = \{a \in \Gamma \mid \exists t \in \mathbb{M} : s = ta\}$ of s and the set of minimal symbols $\min(s) = \{a \in \Gamma \mid \exists t \in \mathbb{M} : s = at\}$ of s belong to $\mathcal{F}$.

Lemma 13. *Let $x, y, z \in \mathrm{IRR}(S) \subseteq \mathbb{M}$. Then $xy \xrightarrow{*}_S z$ if and only if there exist $p, s, t, w \in \mathrm{IRR}(S)$ and $u, v \in \mathcal{F}$ such that*

$$u\,v \xrightarrow{*}_S w, \quad x = s\,u\,p, \quad y = \overline{p}\,v\,t, \quad z = s\,w\,t. \tag{1}$$

Note that since $u, v \in \mathcal{F}$, there exist only finitely many possibilities for w in (1). Hence, the existential quantification over all u, v, and w can be replaced by a finite disjunction of size $|\Gamma|^{2c(V,E)+2}$.

Proof of Lemma 13. Let $x, y, z \in \mathrm{IRR}(S)$. If (1) from Lemma 13 holds, then $xy \xrightarrow{*}_S z$ follows immediately. Now assume that $xy \xrightarrow{*}_S z$. We can choose $p \in \mathbb{M}$ of maximal length such that $x = x'p$ and $y = \overline{p}y'$. Let $u = \max(x') \in \mathcal{F}$, $v = \min(y') \in \mathcal{F}$, and $uv \xrightarrow{*}_S w \in \mathrm{IRR}(S)$. Hence, $x = sup$, $y = \overline{p}vt$, and $xy \xrightarrow{*}_S swt$. Note that $p, s, t, u, v \in \mathrm{IRR}(S)$. Due to the choice of p, only rules of the form $(ab, c) \in S$, where $a \in u$, $b \in v$, and $a, b, c \in \Gamma_n$ for some finite monoid M_n, can be applied to the trace uv. In particular, if $(d, w) \in I$ for $d \in \Gamma$, then also $(d, u) \in I$. We claim that $swt \in \mathrm{IRR}(S)$ which implies $z = swt$. Assume that there exist a left-hand side ab of a rule in S and traces q, r such that $swt = qabr$. By Lemma 2 we obtain up to symmetry one of the following two diagrams (recall that $s, w, t \in \mathrm{IRR}(S)$).

r	s_2	w_2	t_2
ab	a	1	b
q	s_1	w_1	t_1
	s	w	t

r	s_2	w_2	t_2
ab	a	b	1
q	s_1	w_1	t_1
	s	w	t

Let $n \in V$ such that $a, b \in \Gamma_n$. Let us first consider the left diagram. Since $(a, w_1) \in I$, $(b, w_2) \in I$, and $w = w_1 w_2$, we obtain $(a, w) \in I$ and thus $(a, u) \in I$. Furthermore from the diagram we obtain $(b, s_2) \in I$. Thus, $(a, s_2) \in I$ which implies $a \in \max(s)$. Together with $(a, u) \in I$ it follows that $a \in \max(su) = u$ which contradicts $(a, u) \in I$. Now let us consider the right diagram. Again we have $a \in \max(s)$. Furthermore, since $b \in \min(w) \cap \Gamma_n$, there are two possibilities: Either there exists $d \in u \cap \Gamma_n$ or $b \in v$ and $(b, u) \in I$. If $d \in u \cap \Gamma_n$, then su would contain the factor ad, which contradicts $x = sup \in \mathrm{IRR}(S)$. If $b \in v$ and $(b, u) \in I$, then $(a, u) \in I$, which implies $a \in \max(su) = u$, again a contradiction. $\square$

Proof of Theorem 12. Let us fix $k \geq 0$. Let $\mathbb{P}$ be a graph product, specified by a graph (V, E) with $c(V, E) \leq k$. Furthermore let ϕ be an existentially quantified Boolean combination of equations and constraints in $\mathrm{NRAT}(\mathbb{P})$. In a first step, we may push negations to the level of atomic subformulae. An inequality $U \neq V$ may be replaced by $\exists X, Y : X = U \ \wedge \ Y = V \ \wedge \ X \neq Y$, where X, Y are new variables. Moreover, the existential quantification over X and Y can be shifted to the topmost level of ϕ. Thus we may assume that all inequalities in ϕ are of the form $X \neq Y$ for variables X, Y. Using standard methods, see e.g. [7], we may assume that all equalities $U = V$ are triangulated, i.e., $|U| = 2, |V| = 1$. Next we will move from the graph product $\mathbb{P}$ to its underlying trace monoid with involution $(\mathbb{M}, \overline{})$. Note that $c(\Gamma, D) = c(V, E) \leq k$, where $\mathbb{M} = \mathbb{M}(\Gamma, D)$. We replace syntactically every subformula $U = V$ (resp. $X \in L$) by $\psi(U) = \psi(V)$ (resp. $X \in \mu(L)$) and add the negated recognizable constraint $X \notin \mathrm{RED}(S)$ for every variable X.[2] We obtain an existential sentence, which evaluates to *true* in $(\mathbb{M}, \overline{})$ if and only if ϕ evaluates to *true* in $\mathbb{P}$. Note also that the automaton used to specify $\mu(L)$ is the same as the one for L (recall that $L \in \mathrm{NRAT}(\mathbb{P})$ is represented by a finite non-deterministic automaton for $\tau^{-1}(\mu(L))$). It remains to eliminate all occurrences of ψ from (in)equalities. Since $\Gamma \subseteq \mathrm{IRR}(S)$ and S is confluent, we can replace an equation $\psi(AB) = \psi(C)$ $(A, B, C \in \Gamma \cup \Omega \cup \overline{\Omega})$ by $AB \xrightarrow{*}_S C$, which by Lemma 13 is equivalent to

$$\exists X, Y, Z : \bigvee_{\substack{u, v \in \mathcal{F}, \\ uv \xrightarrow{*}_S w \in \mathrm{IRR}(S)}} A = XuZ \ \wedge \ B = \overline{Z} vY \ \wedge \ C = XwY. \tag{2}$$

Since $|\mathcal{F}| \leq |\Gamma|^{k+1}$, this is a formula of polynomial size. Finally, due to the constraints $X, Y \notin \mathrm{RED}(S)$, an inequaility $\psi(X) \neq \psi(Y)$ is equivalent to $X \neq Y$. $\square$

Corollary 14. *The following problem is PSPACE-complete for every $k \geq 0$:*

INPUT: A graph product $\mathbb{P}$, specified by a graph (V, E) with $c(V, E) \leq k$ and an existential sentence ϕ with constraints in $\mathrm{NRAT}(\mathbb{P})$.

QUESTION: Does ϕ belong to $\mathrm{Th}(\mathbb{P}, \mathrm{NRAT}(\mathbb{P}))$ *?*

If $c(V, E)$ is not bounded by a constant, then this problem is in EXPSPACE.

[2] Of course this constraint is equivalent to $X \in \mathrm{IRR}(S)$, but we prefer the negated constraint $X \notin \mathrm{RED}(S)$, since an automaton for $\tau^{-1}(\mathrm{RED}(S))$ can be easily constructed in polynomial time. More precisely $\tau^{-1}(\mathrm{RED}(S))$ is the union of all sets $\Gamma^* a I(a)^* b \Gamma^*$, where ab is a left-hand side of S and $I(a) = \{c \in \Gamma \mid (a, c) \in I\} = I(b)$.

	$c(V,E)$ fixed	$c(V,E)$ variable
no constraints	PSPACE	EXPSPACE
REC($\mathbb{P}$)	PSPACE-complete	EXPSPACE
NRAT($\mathbb{P}$)	PSPACE-complete	EXPSPACE
RAT($\mathbb{P}$)	undecidable	undecidable

Table 1: Results for existential theories

Proof. PSPACE-hardness follows from the fact that for $\{a,b\}^*$ the existential theory of equations with constraints in REC($\{a,b\}^*$) is PSPACE-hard, see [22, Lem. 3.2.3] and [37, Thm. 1]. Membership in PSPACE (resp. EXPSPACE) follows from Theorem 10 and Theorem 12 (recall that $c(V,E) = c(\Gamma, D)$, where $(\mathbb{M}(\Gamma,D), \overline{})$ is the trace monoid with involution underlying $\mathbb{P}$). $\square$

Remark 15. *Corollary 14 encompasses corresponding statements from [7, 9, 10, 11, 18, 25, 26, 37].*

Table 1 summarizes our results for existential theories.

6 Positive theories of equations in graph products

The aim of this section is to prove our second main result, namely that the positive theory of equations with recognizable constraints is decidable, in case the graph product is a group. In order to emphasize the fact that we deal from now on with groups only, we denote this graph product by the symbol $\mathbb{G}$. Let $\mathbb{G}$ be specified by the graph (V,E), where every node $n \in V$ is labeled with a group G_n, which is either finite or $\mathbb{Z}$. Let $(\mathbb{M}, \overline{})$ be the underlying trace monoid with involution, where $\mathbb{M} = \mathbb{M}(\Gamma, D)$. Note that the involution $\overline{} : \mathbb{M} \to \mathbb{M}$ is completely defined, since all elements in Γ have inverses. Finally, let $I \subseteq \Gamma \times \Gamma$, $\pi = \tau \circ \psi$, and $S \subseteq \mathbb{M} \times \mathbb{M}$ have the same meaning as in Section 3.3. All these data will be fixed for the rest of this section.

We will consider positive sentences with equations and constraints from REC($\mathbb{G}$). Our aim is to decide whether such a sentence holds in $\mathbb{G}$. First, in Section 6.1 we will show that we can restrict the graph product $\mathbb{G}$ to some particular type. In a second step, we show in Section 6.2 that for such a restricted graph product, the positive theory with constraints in REC($\mathbb{G}$) can be reduced to the existential theory with constraints in NRAT($\mathbb{G}'$), where the graph product $\mathbb{G}'$ is derived from $\mathbb{G}$. This second step in inspired by techniques of Makanin and Merzlyakov [27, 31] developed for free groups. The proof of the main technical lemma is shifted into Section 6.3.

6.1 Simplifying the graph (V, E)

In a first step we may assume that no finite group G_n, $n \in V$, is a direct product of two finite non-trivial groups, since otherwise we could replace n by two non-connected nodes. In particular, if G_n is not $\mathbb{Z}/2\mathbb{Z}$, then there must exist $a \in \Gamma_n$ such that $a \neq \overline{a}$ in $\mathbb{G}$. Next, assume that the graph (V, E) consists of two non-empty disjoint components (V_1, E_1) and (V_2, E_2), which define graph products $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Then $\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2$. Furthermore by Mezei's Theorem, see e.g. [4], every $L \in \mathrm{REC}(\mathbb{G})$ is effectively a finite union of sets of the form $L_1 \times L_2$ with $L_i \in \mathrm{REC}(\mathbb{G}_i)$. Thus, we may apply the following Proposition 16, which is a decomposition lemma in the style of the Feferman Vaught Theorem [15].

Proposition 16. *Let M_1 and M_2 be monoids with classes $\mathcal{C}_1 \subseteq 2^{M_1}$ and $\mathcal{C}_2 \subseteq 2^{M_2}$. Let $\mathcal{C}$ be a class of subsets of $M_1 \times M_2$ such that each $L \in \mathcal{C}$ is effectively a finite union of sets of the form $L_1 \times L_2$ with $L_1 \in \mathcal{C}_1$ and $L_2 \in \mathcal{C}_2$. If both theories $\mathrm{Th}(M_1, \mathcal{C}_1)$ and $\mathrm{Th}(M_2, \mathcal{C}_2)$ are decidable, then $\mathrm{Th}(M_1 \times M_2, \mathcal{C})$ is decidable, too. Furthermore, the same implication also holds for positive theories.*

Proof. Since $M = M_1 \times M_2$ is generated by Γ, we may assume that Γ is the disjoint union of Γ_1 and Γ_2, where M_i is generated by Γ_i. Let ϕ be a formula with free variables whose atomic subformulae are all of the form $U = V$ with $U, V \in (\Gamma \cup \Omega \cup \overline{\Omega})^*$, or $X \in L$, where $X \in \Omega \cup \overline{\Omega}$ and $L \in \mathcal{C}$. Now for each $X \in \Omega \cup \overline{\Omega}$ that appears in ϕ let X_1 and X_2 be new variables. Furthermore, for $a \in \Gamma$ and $i \in \{1, 2\}$ let $a_i = a$ if $a \in \Gamma_i$ and $a_i = 1$ otherwise. Then we replace each quantification $\exists X$ (resp. $\forall X$) in ϕ by $\exists X_1, X_2$ (resp. $\forall X_1, X_2$). Furthermore each equation $U = V$ is replaced by the conjunction $U_1 = V_1 \wedge U_2 = V_2$, where U_i and V_i result from U and V, respectively, by replacing every occurrence of $X \in \Omega \cup \overline{\Omega}$ (resp. $a \in \Gamma$) by X_i (resp. a_i). Finally given a constraint $X \in L$ in ϕ, where $L = \bigcup_{i=1}^{n} L_{i,1} \times L_{i,2}$ with $L_{i,1} \in \mathcal{C}_1$ and $L_{i,2} \in \mathcal{C}_2$, we replace this constraint by $\bigvee_{i=1}^{n} (X_1 \in L_{i,1} \wedge X_2 \in L_{i,2})$. Let us call the resulting formula $\hat{\phi}$. If we let the variables with index $i \in \{1, 2\}$ only range over M_i, then in the case that ϕ is a sentence, the truth value of $\hat{\phi}$ and ϕ are the same. We claim that $\hat{\phi}$ is logically equivalent to a formula of the form $\bigvee_{j=1}^{m} (\theta_{j,1} \wedge \theta_{j,2})$, where for $i \in \{1, 2\}$ the formula $\theta_{j,i}$ only contains variables with index i. Note that this proves the proposition. The claim above can be shown by induction on the quantifier rank of ϕ. The case that ϕ is quantifier free is clear. Assume that $\phi \equiv \exists X\ \chi$. Hence, $\hat{\phi}$ is of the form $\hat{\phi} \equiv \exists X_1, X_2\ \hat{\chi}$. By induction we can assume that $\hat{\chi}$ is logically equivalent to a formula $\bigvee_{j=1}^{m} (\theta_{j,1} \wedge \theta_{j,2})$, where for $i \in \{1, 2\}$ the formula $\theta_{j,i}$ only contains variables with index i. Thus, $\exists X_1, X_2\ \hat{\chi}$ is equivalent to $\bigvee_{j=1}^{m} (\exists X_1\ \theta_{j,1}\ \wedge\ \exists X_2\ \theta_{j,2})$. In the case of a universal quantification we can conclude similarly, but we first have to transform the formula $\bigvee_{j=1}^{m} \theta_{j,1} \wedge \theta_{j,2}$ into a formula of the form $\bigwedge_{j=1}^{m'} \theta'_{j,1} \vee \theta'_{j,2}$ where $\theta'_{j,i}$ only contains variables with index i. This is of course possible with a possible exponential size increase. Finally note that the construction above does not introduce negations and thus can be also used for positive formulae. ☐

Hence, in the sequel we may assume that the graph (V, E) is connected. Furthermore, since by Proposition 7 the (positive) theory of equations with rational constraints in $\mathbb{Z}$ is decidable and the same holds for finite monoids for trivial reasons, we may assume that $|V| > 1$. By Corollary 9 we can also exclude the case that V contains exactly two adjacent nodes which are both labeled by $\mathbb{Z}/2\mathbb{Z}$. Thus, we may assume that either the graph (V, E) contains a path consisting of three different nodes or one of the groups labeling the nodes has a generator $x \in \Gamma$ with $\overline{x} \neq x$. Hence, there exist three different generators $a, b, c, \in \Gamma$ such that a and b belong to different and E-adjacent nodes from V, b and c also belong to different and E-adjacent nodes from V, and finally a and c either belong to different nodes from V or $a \neq \overline{a} = c$ in $\mathbb{G}$. In particular $(a, b), (b, c) \in D$, i.e., the dependency between a, b, and c being used is

$$a \text{ — } b \text{ — } c.$$

In the sequel, a, b, and c will always refer to these symbols.

6.2 Reducing to the existential theory

Our strategy for proving the decidability of the positive theory of $\mathbb{G}$ is based on [27, 31], but the presence of partial commutation and recognizable constraints makes the construction more involved: Given a positive sentence θ, which is interpreted over $\mathbb{G}$, we construct an *existential sentence* θ', which is interpreted over a free product $\mathbb{G}' = \mathbb{G} * F$ of $\mathbb{G}$ and a free group F, such that θ is true in $\mathbb{G}$ if and only if θ' is true in $\mathbb{G}'$. This allows us to apply Corollary 14 on the decidability of the existential theory of a graph product. Roughly speaking, θ' results from θ by replacing the universally quantified variables by the generators of F.

For the following consideration it is convenient to assume that a recognizable language L is represented by a homomorphism to a finite group instead of an automaton for $\pi^{-1}(L)$: Recall that $L \in \mathrm{REC}(\mathbb{G})$ if and only if there exists a surjective homomorphism $\rho : \mathbb{G} \to H$ onto a finite group H such that $L = \rho^{-1}(\rho(L))$, see e.g. [4]. Moreover, given a non-deterministic automaton for $\pi^{-1}(L)$ with n states, we can construct such a homomorphism $\rho : \mathbb{G} \to H$ with $|H| \leq 2^{n^2}$ [29]. Finally, given a Boolean combination ϕ of word equations and recognizable constraints $X_1 \in L_1, \ldots, X_n \in L_n$, we first construct homomorphisms $\rho_i : \mathbb{G} \to H_i$ such that $L_i = \rho_i^{-1}(\rho_i(L_i))$. Let $H = \prod_{i=1}^{n} H_i$ and define $\rho(x) = (\rho_1(x), \ldots, \rho_n(x))$ for $x \in \mathbb{G}$. Note that the size of H can be bounded exponentially in the size of the description of ϕ. Now we can replace the constraints $X_i \in L_i$ by constraints of the form $\rho(X_i) = h$ for $h \in H$. Moreover, the number of these constraints is also bounded exponentially in the size of the description of ϕ. Let us fix a surjective homomorphism $\rho : \mathbb{G} \to H$ for the rest of this section and assume that all recognizable constraints in our initial positive formula are given in the form $\rho(X) = h$ for $h \in H$.

For a finite set K of new constants, $K \cap \Gamma = \emptyset$, let $\overline{K} = \{\overline{k} \mid k \in K\}$ be a disjoint copy of K. Define an involution $\overline{} : K \cup \overline{K} \to K \cup \overline{K}$ by $\overline{\overline{k}} = k$. Let

$$F(K) = (K \cup \overline{K})^*/\{k\overline{k} = \overline{k}k = 1 \mid k \in K\}$$

be the free group generated by K. Instead of $F(\{k\})$ we write $F(k)$. In the following we also have to deal with formulae, where the constraints are given by different extensions of our basic homomorphism $\rho : \mathbb{G} \to H$. For this we introduce the following notation: Let G be an arbitrary finitely generated group, and let $\varrho : G \to H$ be a group homomorphism to some finite group H. Let $K = \{k_1, \ldots, k_n\}$ and $h_1, \ldots, h_n \in H$. Then $\varrho^{k_1,\ldots,k_n}_{h_1,\ldots,h_n} : G * F(K) \to H$ denotes the extension of ϱ, defined by $\varrho^{k_1,\ldots,k_n}_{h_1,\ldots,h_n}(k_i) = h_i$. Similarly, if ϕ is some Boolean combination of word equations and constraints of the form $\varrho(X) = h$, then $\phi^{k_1,\ldots,k_n}_{h_1,\ldots,h_n}$ denotes the formula that results from ϕ by replacing every constraint $\varrho(X) = h$ by $\varrho^{k_1,\ldots,k_n}_{h_1,\ldots,h_n}(X) = h$. Let us now fix a formula[3]

$$\theta(\tilde{Z}) \;\equiv\; \forall X_1 \exists Y_1 \cdots \forall X_n \exists Y_n\, \phi(X_1, \ldots, X_n, Y_1, \ldots, Y_n, \tilde{Z}),$$

where ϕ is a positive Boolean formula with constraints of the form $\rho(X) = h$. Choose for every universally quantified variable X_i in θ a new constant k_i and let $K = \{k_1, \ldots, k_n\}$. The following theorem yields the reduction from the positive to the existential theory.

Theorem 17. *Let $\theta(\tilde{Z}) \equiv \forall X_1 \exists Y_1 \cdots \forall X_n \exists Y_n\, \phi(X_1, \ldots, X_n, Y_1, \ldots, Y_n, \tilde{Z})$ be as above. For all $\tilde{z} \in \mathbb{G}$ we have $\theta(\tilde{z})$ in $\mathbb{G}$ if and only if*

$$\bigwedge_{h_1 \in H} \exists Y_1 \cdots \bigwedge_{h_n \in H} \exists Y_n \left\{ \begin{array}{l} \phi^{k_1,\ldots,k_n}_{h_1,\ldots,h_n}(k_1, \ldots, k_n, Y_1, \ldots, Y_n, \tilde{z}) \\ \wedge \displaystyle\bigwedge_{1 \le i \le n} Y_i \in \mathbb{G} * F(\{k_1, \ldots, k_i\}) \end{array} \right\} \text{ in } \mathbb{G} * F(K).$$

Proof. We prove the theorem by induction on n. The case $n = 0$ is clear. If $n > 0$, then inductively we can assume that for all $x_1, y_1, \tilde{z} \in \mathbb{G}$ we have

$$\forall X_2 \exists Y_2 \cdots \forall X_n \exists Y_n\, \phi(x_1, X_2, \ldots, X_n, y_1, Y_2, \ldots, Y_n, \tilde{z}) \quad \text{in } \mathbb{G}$$

if and only if

$$\bigwedge_{h_2 \in H} \exists Y_2 \cdots \bigwedge_{h_n \in H} \exists Y_n \left\{ \begin{array}{l} \phi^{k_2,\ldots,k_n}_{h_2,\ldots,h_n}(x_1, k_2, \ldots, k_n, y_1, Y_2, \ldots, Y_n, \tilde{z}) \\ \wedge \displaystyle\bigwedge_{2 \le i \le n} Y_i \in \mathbb{G} * F(\{k_2, \ldots, k_i\}) \end{array} \right\}$$

is true in $\mathbb{G} * F(\{k_2, \ldots, k_n\})$. Thus, for all $\tilde{z} \in \mathbb{G}$ we have

$$\forall X_1 \exists Y_1 \cdots \forall X_n \exists Y_n\, \phi(X_1, \ldots, X_n, Y_1, \ldots, Y_n, \tilde{z}) \quad \text{in } \mathbb{G}$$

if and only if

$$\forall X_1 \in \mathbb{G}\; \exists Y_1 \bigwedge_{h_2 \in H} \exists Y_2 \cdots \bigwedge_{h_n \in H} \exists Y_n \left\{ \begin{array}{l} \phi^{k_2,\ldots,k_n}_{h_2,\ldots,h_n}(X_1, k_2, \ldots, k_n, Y_1, \ldots, Y_n, \tilde{z}) \\ \wedge \displaystyle\bigwedge_{1 \le i \le n} Y_i \in \mathbb{G} * F(\{k_2, \ldots, k_i\}) \end{array} \right\}$$

[3] In the following symbols with a tilde like $\tilde{x}$ will denote sequences of arbitrary length over some set, which will be always clear form the context. If say $\tilde{x} = (x_1, \ldots, x_\nu)$, then $\tilde{x} \in A$ means $x_1 \in A, \ldots, x_\nu \in A$.

is true in $\mathbb{G} * F(\{k_2, \ldots, k_n\})$. Note that if we transform this formula into prenex normal form, in the resulting positive formula the constraints are given by different extensions of the homomorphism ρ. Since ρ is surjective, we can replace the universal quantifier $\forall X_1 \in \mathbb{G}$ by $\bigwedge_{h_1 \in H} \forall X \in \rho^{-1}(h_1)$. Hence, by the following Lemmata 19 and 20 this formula is true in $\mathbb{G} * F(\{k_2, \ldots, k_n\})$ if and only if

$$\bigwedge_{h_1 \in H} \exists Y_1 \bigwedge_{h_2 \in H} \exists Y_2 \cdots \bigwedge_{h_n \in H} \exists Y_n \left\{ \begin{array}{l} \phi^{k_1,k_2,\ldots,k_n}_{h_1,h_2,\ldots,h_n}(k_1, k_2, \ldots, k_n, Y_1, \ldots, Y_n, \tilde{z}) \\ \wedge \bigwedge\limits_{1 \le i \le n} Y_i \in \mathbb{G} * F(\{k_1, k_2, \ldots, k_i\}) \end{array} \right\}$$

is true in $\mathbb{G} * F(\{k_2, \ldots, k_n\}) * F(k_1) = \mathbb{G} * F(K)$. The first one, Lemma 19, is only valid for positive sentences, but has a quite simple proof, whereas Lemma 20 holds for arbitrary formulae, but its proof is quite involved. $\square$

Since $\mathbb{G} * F(\{k_1, \ldots, k_i\}) \in \mathrm{NRAT}(\mathbb{G} * F(K))$, Corollary 14 and Theorem 17 immediately imply:

Corollary 18. *The following problem is decidable.*

INPUT: A graph product $\mathbb{G}$ which is a group and a positive sentence ϕ with constraints in $\mathrm{REC}(\mathbb{G})$.

QUESTION: Does ϕ belong to $\mathrm{Th}(\mathbb{G}, \mathrm{REC}(\mathbb{G}))$*?*

Concerning the complexity, it can be shown that our proof of Corollary 18 gives us a non-elementary algorithm due to the construction in our proof of Proposition 16. If we restrict to connected graphs (V, E), then we obtain an elementary algorithm due to the upper complexity bounds in Proposition 7 and Corollary 9.

Note that Corollary 18 cannot be extended to the full class of graph products considered in Section 3: Already for a free monoid $\{a, b\}^*$ the positive $\forall\exists^3$-theory of equations is undecidable [14, 28]. Similarly, Corollary 18 cannot be extended to the case of normalized rational constraints, since $\{a_1, a_2\}^* \in \mathrm{NRAT}(F)$ for the free group F generated by a_1 and a_2.

For our further considerations let us introduce a few abbreviations. For a set K of new constants, $K \cap \Gamma = \emptyset$, let $\mathbb{G}' = \mathbb{G} * F(K)$. Let $k \notin \Gamma \cup K$ be a further constant. Let us fix subsets $K_i \subseteq K$ $(1 \le i \le m)$ and let $\mathbb{G}_i = \mathbb{G} * F(K_i) \subseteq \mathbb{G}'$. Finally fix $h \in H$ and a sequence $\tilde{z} = (z_1, \ldots, z_\nu)$ of elements $z_i \in \mathbb{G}$.

Lemma 19. *Let $\phi(X, Y_1, \ldots, Y_m, \tilde{Z})$ be a positive Boolean formula such that all constraints have the form $\rho'(Y) = g$, where $g \in H$ and $\rho' : \mathbb{G}' \to H$ is an extensions of $\rho : \mathbb{G} \to H$ (different constraints may be given by different g and ρ'). If*

$$\exists Y_1, \ldots, Y_m : \phi^k_h(k, Y_1, \ldots, Y_m, \tilde{z}) \;\wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{G}_i * F(k) \quad \textit{in } \mathbb{G}' * F(k),$$

then

$$\forall X \in \mathbb{G} \cap \rho^{-1}(h)\; \exists Y_1, \ldots, Y_m : \phi(X, Y_1, \ldots, Y_m, \tilde{z}) \;\wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{G}_i \quad \textit{in } \mathbb{G}'.$$

Proof. If

$$\exists Y_1,\ldots,Y_m : \phi_h^k(k,Y_1,\ldots,Y_m,\tilde{z}) \;\wedge \bigwedge_{1\le i\le m} Y_i \in \mathbb{G}_i * F(k) \quad \text{in } \mathbb{G}' * F(k),$$

then there are $t_i \in \mathbb{G}_i * F(k)$, $1 \le i \le m$, such that $\phi_h^k(k,t_1,\ldots,t_m,\tilde{z})$ is true in $\mathbb{G}' * F(k)$. Now choose an arbitrary $s \in \mathbb{G} \cap \rho^{-1}(h)$ and define a homomorphism $\sigma : \mathbb{G}' * F(k) \to \mathbb{G}'$ by $\sigma(k) = s$ and $\sigma(x) = x$ for $x \in \mathbb{G}'$. Since $\rho(s) = h$, $\sigma(\tilde{z}) = \tilde{z}$, and ϕ_h^k is positive, the statement $\phi(s,\sigma(t_1),\ldots,\sigma(t_m),\tilde{z})$ is true in $\mathbb{G}'$. Thus, we obtain

$$\forall X \in \mathbb{G} \cap \rho^{-1}(h)\; \exists Y_1,\ldots,Y_m : \phi(X,Y_1,\ldots,Y_m,\tilde{z}) \;\wedge \bigwedge_{1\le i\le m} Y_i \in \mathbb{G}_i \quad \text{in } \mathbb{G}'.$$

□

Note that the assertion of Lemma 19 does not hold in general, if ϕ involves negations. For example $\forall X : X \neq 1$ is false, but $k \neq 1$ is true. On the other hand, the converse implication of Lemma 19 is true for arbitrary formulae:

Lemma 20. *Let $\phi(X,Y_1,\ldots,Y_m,\tilde{Z})$ be a (not necessarily positive) Boolean formula such that all constraints have the form $\rho'(Y) = g$, where $g \in H$ and $\rho' : \mathbb{G}' \to H$ is an extensions of $\rho : \mathbb{G} \to H$ (different constraints may be given by different g and ρ'). If*

$$\forall X \in \mathbb{G} \cap \rho^{-1}(h)\; \exists Y_1,\ldots,Y_m : \phi(X,Y_1,\ldots,Y_m,\tilde{z}) \;\wedge \bigwedge_{1\le i\le m} Y_i \in \mathbb{G}_i \quad \textit{in } \mathbb{G}',$$

then

$$\exists Y_1,\ldots,Y_m : \phi_h^k(k,Y_1,\ldots,Y_m,\tilde{z}) \;\wedge \bigwedge_{1\le i\le m} Y_i \in \mathbb{G}_i * F(k) \quad \textit{in } \mathbb{G}' * F(k).$$

The statement of Lemma 20 will be shown by a reduction to the underlying trace monoid with involution. For this, we need the following Lemma 21. Its proof is the main technical difficulty and shifted to the next section. Let $(\mathbb{M}', \overline{})$ (resp. $(\mathbb{M}_i, \overline{})$) be the trace monoid with involution underlying $\mathbb{G}'$ (resp. $\mathbb{G}_i$). Thus, $\mathbb{M} \subseteq \mathbb{M}_i = \mathbb{M} * (K_i \cup \overline{K_i})^* \subseteq \mathbb{M}' = \mathbb{M} * (K \cup \overline{K})^*$. Let $\tilde{w} = (w_1,\ldots,w_\nu)$, where $w_i = \mu(z_i) \in \mathrm{IRR}(S) \subseteq \mathbb{M}$ is the irreducible trace representing $z_i \in \mathbb{G}$. Let $S' = S \cup \{(\alpha\overline{\alpha},1),(\overline{\alpha}\alpha,1) \mid \alpha \in K\}$, which is the trace rewriting system over $\mathbb{M}'$ presenting $\mathbb{G}'$, and let $S'_k = S' \cup \{(k\overline{k},1),(\overline{k}k,1)\}$, which is the system over $\mathbb{M}' * \{k,\overline{k}\}$ presenting $\mathbb{G}' * F(k)$. In the following, we identify a homomorphism $\rho' : \mathbb{G}' \to H$ with $\psi' \circ \rho' : \mathbb{M}' \to H$, where $\psi' : \mathbb{G}' \to \mathbb{M}'$ is canonical. Moreover, for $\rho' : \mathbb{M}' \to H$, we denote with ${\rho'}_h^k : \mathbb{M}' * \{k,\overline{k}\}^* \to H$ the extension of $\rho' : \mathbb{M}' \to H$, defined by ${\rho'}_h^k(k) = h$ and ${\rho'}_h^k(\overline{k}) = h^{-1}$.

Lemma 21. *Let $\chi(X,Y_1,\ldots,Y_m,\tilde{Z})$ be a (not necessarily positive) Boolean formula such that all constraints have the form $\rho'(Y) = g$, where $g \in H$ and $\rho' : \mathbb{M}' \to H$ is an extensions of $\rho : \mathbb{M} \to H$. If*

$$\forall X \in \mathrm{IRR}(S) \cap \rho^{-1}(h)\; \exists Y_1,\ldots,Y_m \in \mathrm{IRR}(S') : \chi(X,Y_1,\ldots,Y_m,\tilde{w}) \;\wedge \bigwedge_{1\le i\le m} Y_i \in \mathbb{M}_i,$$

in $(\mathbb{M}', \overline{})$, *then there exist* $s_1, s_2 \in \mathrm{IRR}(S) \subseteq \mathbb{M}$ *such that* $\rho(s_1)h\rho(s_2) = h$ *and*

$$\exists Y_1, \ldots, Y_m \in \mathrm{IRR}(S'_k) : \chi^k_h(s_1 k s_2, Y_1, \ldots, Y_m, \tilde{w}) \ \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{M}_i * \{k, \overline{k}\}^*$$

in $(\mathbb{M}' * \{k, \overline{k}\}^*, \overline{})$.

Proof of Lemma 20 using Lemma 21. Assume that

$$\forall X \in \mathbb{G} \cap \rho^{-1}(h) \ \exists Y_1, \ldots, Y_m : \phi(X, Y_1, \ldots, Y_m, \tilde{z}) \ \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{G}_i \quad \text{in } \mathbb{G}'.$$

Completely analogous to the proof of Theorem 12 we can first switch to the underlying trace monoid with involution $(\mathbb{M}', \overline{})$. Note that this procedure introduces existentially quantified variables ($\tilde{Y}$ below), only, and that $\forall X \in \mathbb{G} \cap \rho^{-1}(h)$ has to be replaced by $\forall X \in \mathrm{IRR}(S) \cap \rho^{-1}(h)$. We obtain a sentence of the form

$$\forall X \in \mathrm{IRR}(S) \cap \rho^{-1}(h) \ \exists Y_1, \ldots, Y_m, \tilde{Y} \in \mathrm{IRR}(S') : \chi(X, Y_1, \ldots, Y_m, \tilde{Y}, \tilde{w}) \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{M}_i,$$

which evaluates to true in $(\mathbb{M}', \overline{})$. Thus, by Lemma 21 there exist $s_1, s_2 \in \mathrm{IRR}(S) \subseteq \mathbb{M}$ such that $\rho(s_1)h\rho(s_2) = h$ and

$$\exists Y_1, \ldots, Y_m, \tilde{Y} \in \mathrm{IRR}(S'_k) : \chi^k_h(s_1 k s_2, Y_1, \ldots, Y_m, \tilde{Y}, \tilde{w}) \ \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{M}_i * \{k, \overline{k}\}^*$$

is true in $(\mathbb{M}' * \{k, \overline{k}\}^*, \overline{})$. Since in this sentence all variables are restricted to irreducible traces from $\mathrm{IRR}(S'_k)$ and also $s_1 k s_2, \tilde{w} \in \mathrm{IRR}(S'_k)$, it is also true in $\mathbb{G}' * F(k)$. Thus,

$$\exists Y_1, \ldots, Y_m, \tilde{Y} : \chi^k_h(s_1 k s_2, Y_1, \ldots, Y_m, \tilde{Y}, \tilde{z}) \ \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{G}_i * F(k) \tag{3}$$

in $\mathbb{G}' * F(k)$. Let us define a group homomorphism $\sigma : \mathbb{G}' * F(k) \to \mathbb{G}' * F(k)$ by $\sigma(k) = \overline{s}_1 k \overline{s}_2$ and $\sigma(x) = x$ for $x \in \mathbb{G}'$. First, note that σ is injective (the homomorphism defined by $\sigma(k) = s_1 k s_2$ defines an inverse). Thus, the truth value of all equations is preserved by σ. Moreover, $\rho(s_1)h\rho(s_2) = h$ and hence, $\rho'^k_h(\overline{s}_1 k \overline{s}_2) = \rho(s_1)^{-1} h \rho(s_2)^{-1} = h$ for every extension ρ' of ρ. Thus, all recognizable constraints are also preserved by σ. Finally, $\sigma(s_1 k s_2) = s_1 \overline{s}_1 k \overline{s}_2 s_2 = k$. Applying σ to (3) and using $\sigma(s_1 k s_2) = k$ yields

$$\exists Y_1, \ldots, Y_m, \tilde{Y} : \chi^k_h(k, Y_1, \ldots, Y_m, \tilde{Y}, \tilde{z}) \ \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{G}_i * F(k)$$

in $\mathbb{G}' * F(k)$. But then also

$$\exists Y_1, \ldots, Y_m : \phi^k_h(k, Y_1, \ldots, Y_m, \tilde{z}) \ \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{G}_i * F(k)$$

in $\mathbb{G}' * F(k)$, where ϕ is the initial Boolean formula. For this note that if the formula (2) on page 11 holds in $\mathbb{G}' * F(k)$, then also $AB = C$ in $\mathbb{G}' * F(k)$. $\square$

6.3 Proof of Lemma 21

Recall that $\mathbb{M} \subseteq \mathbb{M}_i \subseteq \mathbb{M}'$, $h \in H$, and $\tilde{w} = (w_1, \ldots, w_\nu)$ with $w_i \in \mathrm{IRR}(S) \subseteq \mathbb{M}$ are already fixed. Let $\chi(X, Y_1, \ldots, Y_m, \tilde{Z})$ be an arbitrary Boolean formula such that all constraints have the form $\rho'(Y) = g$, where $g \in H$ and $\rho' : \mathbb{M}' \to H$ is an extensions of $\rho : \mathbb{M} \to H$. We may assume that all equations in χ have the form $AB = C$ for $A, B, C \in \Omega \cup \overline{\Omega} \cup \Gamma \cup K \cup \overline{K}$. Let $W = \{w_1, \overline{w_1}, \ldots, w_\nu, \overline{w_\nu}\}$ and let d be the number of equations in χ. Choose λ such that $|H|$ divides $\lambda - 1$ and $\lambda \geq 2d + 1$.

We start with the definition of some specific traces. A *chain* is an irreducible trace $a_1 \cdots a_n \in \mathrm{IRR}(S) \subseteq \mathbb{M}$, where $a_1, \ldots, a_n \in \Gamma$ and $(a_i, a_{i+1}) \in D$ for $1 \leq i \leq n-1$. In particular, its dependence graph induces a linear order. Recall that at the end of Section 6.1 we have fixed three different symbols $a, b, c \in \Gamma$ with $(a, b), (b, c) \in D$.

Lemma 22. *There exists a trace $\ell \in \mathbb{M}$ such that $\rho(\ell) = h$, $\mathrm{alph}(\ell) = \Gamma$, $\min(\ell) = b$, and $\max(\ell) = a$.*

Proof. First, for every $x \in \Gamma$ we construct a trace $t_x \in \mathrm{IRR}(S)$ with $\min(t_x) = x$, $\max(t_x) = \overline{x}$, and $\rho(t_x) = 1$. If a, b, and c belong to pairwise different alphabets Γ_n, then $t_x = x\, x_1 \cdots x_p\, (b\, a)^{|H|} (c\, b)^{|H|}\, \overline{x}_p \cdots \overline{x}_1\, \overline{x}$, where $x\, x_1 \cdots x_p\, b$ is a chain, which exists since (V, E) is connected. On the other hand, if $a \neq \overline{a} = c$, then choose a chain $x\, x_1 \cdots x_p\, a$ and define $s_x = x\, x_1 \cdots x_p\, (a\, b\, a)^{|H|}\, \overline{x}_p \cdots \overline{x}_1\, \overline{x}$. If a belongs to a group isomorphic to $\mathbb{Z}$, then $s_x \in \mathrm{IRR}(S)$ and we can define $t_x = s_x$. On the other hand, if a belongs to a finite group, then, since $a \neq \overline{a}$, we have $a^2 = a' \in \Gamma$ in $\mathbb{G}$. Then in $\mathbb{G}$ the element s_x is equal to $x\, x_1 \cdots x_p\, a\, (b\, a')^{|H|-1}\, b\, a\, \overline{x}_p \cdots \overline{x}_1\, \overline{x} \in \mathrm{IRR}(S)$ and we can choose the latter trace for t_x.

Now we construct ℓ as follows:

- Select a trace $s = b_1 b_2 \cdots b_q \in \mathrm{IRR}(S)$, $b_i \in \Gamma$, such that $\rho(b_1 \cdots b_q) = h$.
- Let $u_1, \ldots, u_{q+1} \in \mathbb{M}$ be chains, visiting all symbols from Γ, such that the trace $b u_1 b_1 u_2 b_2 \cdots u_q b_q u_{q+1} a$ is also a chain (these u_i must exist).
- If $u_i = c_1 \cdots c_p$ with $c_j \in \Gamma$, then define $v_i = t_{c_1} \cdots t_{c_p}$.
- Finally let $\ell = t_b v_1 b_1 v_2 b_2 \cdots v_q b_q v_{q+1} t_{\overline{a}}$.

The construction implies that ℓ has indeed the desired properties. □

For the rest of the section let $\ell \in \mathbb{M}$ be some trace satisfying the properties from the previous lemma. In the following $R = (r_0, \ldots, r_\lambda)$ denotes a system of $\lambda + 1$ traces $r_i \in \{(ba)^{|H|}, (bc)^{|H|}\}^* \subseteq \mathbb{M}$, where $|r_i| = 2n|H|$ for some n large enough. The value of n will be made more precise later. Note that the traces r_i are chains with $\rho(r_i) = 1$ and that there are $2^{n(\lambda+1)}$ such systems R. We say that the trace $t \in \{a, b, c\}^* \subseteq \mathbb{M}$ *appears twice in R* if one of the following three conditions holds:

- There exist $i, j \in \{0, \ldots, \lambda\}$, $i \neq j$, such that r_i contains a factor, which is equal to t, and r_j contains a factor which is equal to t or $\overline{t}$.

- There exists $i \in \{0, \ldots, \lambda\}$ such that r_i contains both factors t and $\overline{t}$.
- There exists $i \in \{0, \ldots, \lambda\}$ such that r_i contains a factor t twice, i.e., $r_i = u_1 t v_1 = u_2 t v_2$ and $u_1 \neq u_2$.

We say that R *has enough randomness* if no trace t with $|t| \geq \frac{|r_i|-|\ell|}{2} = n|H| - \frac{|\ell|}{2}$ appears twice in R. Note that this implies in particular that the chains $r_0, \overline{r_0}, \ldots, r_\lambda, \overline{r_\lambda}$ are pairwise different. Moreover, if $r_i \ell r_j = urv$ with $r \in \{r_p, \overline{r_p}\}$, then either $u = 1$ and $r_i = r$ or $v = 1$ and $r_j = r$, i.e., r cannot be properly contained in $r_i \ell r_j$.

The following lemma can be derived by standard techniques that random strings are incompressible, the formal proof is therefore omitted. The idea is that if a long factor appears twice in R, then the description of R can be compressed to less than $n(\lambda+1)$ bits. Note that the chains r_i behave like words.

Lemma 23. *There exists n_0 (depending only on λ and $|H|$) such that for all $n \geq n_0$ there exists a system $R = (r_0, \ldots, r_\lambda)$, $r_i \in \{(ba)^{|H|}, (bc)^{|H|}\}^n$, having enough randomness.*

Remark 24. *Later, we will use R to construct a trace s, which can be replaced by the trace $s_1 k s_2$ in Lemma 21. An explicit construction of s without using the notion of randomness is given in [8].*

Let us fix a system $R = (r_0, \ldots, r_\lambda)$, $r_{i-1} \in \{(ba)^{|H|}, (bc)^{|H|}\}^n$, having enough randomness such that furthermore $4n|H| + |\ell| > |w|$ for all $w \in W$. For every $1 \leq i \leq \lambda$ define the length-reducing trace rewriting system

$$R_i = \{(r_{i-1}\, \ell\, r_i,\ r_{i-1}\, k\, r_i), (\overline{r_i}\, \overline{\ell}\, \overline{r_{i-1}},\ \overline{r_i}\, \overline{k}\, \overline{r_{i-1}})\}.$$

We consider R_i as a trace rewriting system over the trace monoid $\mathbb{M}' * \{k, \overline{k}\}^*$. Note that $w \in \mathrm{IRR}(R_i)$ for all $w \in W$ by the choice of n.

Lemma 25. *Every trace rewriting system R_i is confluent.*

Proof. Assume that $s \to_{R_i} t$ and $s \to_{R_i} u$. Assume that t (resp. u) results from s by an application of the rule $(r_{i-1}\ell r_i, r_{i-1} k r_i)$, the other two cases can be dealt analogously. Thus, there exist traces t_1, t_2, u_1, and u_2 such that

$$s = t_1(r_{i-1}\, \ell\, r_i)t_2 = u_1(r_{i-1}\, \ell\, r_i)u_2 \text{ and } t = t_1(r_{i-1}\, k\, r_i)t_2,\ u = u_1(r_{i-1}\, k\, r_i)u_2.$$

Now we apply Lemma 2 to the identity $t_1(r_{i-1}\, \ell\, r_i)t_2 = u_1(r_{i-1}\, \ell\, r_i)u_2$. Since non-empty prefixes (resp. suffixes) of r_{i-1} (resp. r_i) are dependent and ℓ is dependent from every non-empty trace, we obtain up to symmetry one of the following two diagrams:

u_2	1	s_2	t_2
$r_{i-1}\, \ell\, r_i$	1	$r_{i-1}\, \ell\, r_i$	1
u_1	t_1	s_1	1
	t_1	$r_{i-1}\, \ell\, r_i$	t_2

u_2	1	1	u_2
$r_{i-1}\, \ell\, r_i$	1	s	s_2
u_1	t_1	s_1	v
	t_1	$r_{i-1}\, \ell\, r_i$	t_2

In the first case we must have $s_1 = 1 = s_2$ and thus $t_1 = u_1$, $t_2 = u_2$, $t = u$. In the second case we may assume that $s_1 \neq 1 \neq s_2$, since otherwise we obtain a special case of the first diagram. Furthermore, if $s = 1$, then $t \to_{R_i} t_1\, r_{i-1}\, k\, r_i\, v\, r_{i-1}\, k\, r_i\, u_2 \;{}_{R_i}\!\!\leftarrow u$. Thus, assume that also $s \neq 1$. Since $s\, s_2 = r_{i-1}\, \ell\, r_i = s_1\, s$ and R has enough randomness, there exist traces p and q such that $s_1 = r_{i-1}\, \ell\, p$, $s_2 = q\, \ell\, r_i$, $r_i = p\, s$, $r_{i-1} = s\, q$ (and $|s| < n|H| - \frac{|\ell|}{2}$). Since $(v, s) \in I$, we obtain

$$\begin{aligned}
t = t_1(r_{i-1}\, k\, r_i)t_2 \;&=\; t_1\, r_{i-1}\, k\, p\, s\, v\, q\, \ell\, r_i\, u_2 \\
&=\; t_1\, r_{i-1}\, k\, p\, v\, s\, q\, \ell\, r_i\, u_2 \\
&\to_{R_i}\; t_1\, r_{i-1}\, k\, p\, v\, s\, q\, k\, r_i\, u_2 \\
&=\; t_1\, r_{i-1}\, k\, p\, s\, v\, q\, k\, r_i\, u_2 \\
&{}_{R_i}\!\!\leftarrow\; t_1\, r_{i-1}\, \ell\, p\, s\, v\, q\, k\, r_i\, u_2 \\
&=\; t_1\, r_{i-1}\, \ell\, p\, v\, s\, q\, k\, r_i\, u_2 = u_1(r_{i-1}\, k\, r_i)u_2 = u.
\end{aligned}$$

□

The previous lemma implies that for every $1 \leq i \leq \lambda$ and every trace s there exists a unique normal form $\kappa_i(s)$ such that $s \xrightarrow{*}_{R_i} \kappa_i(s) \in \mathrm{IRR}(R_i)$. Moreover, $\kappa_i(w) = w$ for all $w \in W$.

For the next lemma, let us consider a pair of traces $(u, v) \in \mathbb{M}' \times \mathbb{M}'$ and $t \in \mathbb{M}'$. We say that (u, v) splits t, if there exists an occurrence of t in the trace $u\, v$, which is neither contained in the prefix u nor in the suffix v of the trace $u\, v$.

Lemma 26. *Every $(u, v) \in \mathbb{M}' \times \mathbb{M}'$ splits at most two traces from $\{r_{i-1}\, \ell\, r_i,\ \overline{r_i}\, \overline{\ell}\, \overline{r_{i-1}} \mid 1 \leq i \leq \lambda\}$.*

Proof. Assume that (u, v) splits three traces from $\{r_{i-1}\, \ell\, r_i, \overline{r_i}\, \overline{\ell}\, \overline{r_{i-1}} \mid 1 \leq i \leq \lambda\}$, say $r_{i-1}\, \ell\, r_i$ for $i = i_1, i_2, i_3$ pairwise different (other cases can be dealt analogously). Denote by $\hat{t}$ the projection of the trace $t \in \mathbb{M}'$ to the alphabet $\{a, b, c\}$. Then we obtain factorizations $\widehat{(u\, v)} = \hat{u}\hat{v} = u_i\, r_{i-1}\, \hat{\ell}\, r_i\, v_i$ for $i = i_1, i_2, i_3$, where u_i, v_i are traces over $\{a, b, c\}$ such that $|u_i| < |\hat{u}| < |u_i\, r_{i-1}\, \hat{\ell}\, r_i|$. But then there must be $i, j \in \{i_1, i_2, i_3\}$, $i \neq j$, such that either r_{i-1} or r_i is properly contained in $r_{j-1}\, \hat{\ell}\, r_j$. Since R has enough randomness, this is not possible. □

It is easy to see that if (u, v) does neither split $r_{i-1}\, \ell\, r_i$ nor $\overline{r_i}\, \overline{\ell}\, \overline{r_{i-1}}$, then $\kappa_i(u)\kappa_i(v) = \kappa_i(u\, v)$. Since moreover $\kappa_i(x) = \kappa_i(y)$ implies $x = y$, we obtain the following lemma (recall that $\lambda \geq 2d + 1$, where d is the number of equations in χ).

Lemma 27. *Let $x_j, y_j, z_j \in \mathbb{M}'$ for $1 \leq j \leq d$. Then there exists $1 \leq i \leq \lambda$ such that for all $1 \leq j \leq d$, we have $x_j y_j = z_j$ if and only if $\kappa_i(x_j)\kappa_i(y_j) = \kappa_i(z_j)$.*

Finally the following lemma follows immediately from the fact that $\rho(\ell) = h$.

Lemma 28. *Let $\rho' : \mathbb{M}' \to H$ be an extension of $\rho : \mathbb{M} \to H$. Then $\rho'(t) = \rho'^{k}_{h}(\kappa_i(t))$ for every trace $t \in \mathbb{M}'$ and every $1 \leq i \leq \lambda$.*

Now we are able to prove Lemma 21. Assume that

$$\forall X \in \mathrm{IRR}(S) \cap \rho^{-1}(h)\ \exists Y_1, \ldots, Y_m \in \mathrm{IRR}(S') : \chi(X, Y_1, \ldots, Y_m, \tilde{w})\ \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{M}_i$$

is true in $(\mathbb{M}', \overline{\ })$, Let $s = r_0\, \ell\, r_1\, \ell \cdots r_{\lambda-1}\, \ell\, r_\lambda \in \mathrm{IRR}(S) \subseteq \mathbb{M}$. Since $|H|$ is a divisor of $\lambda - 1$ and $\rho(r_i) = 1$, we have $\rho(s) = \rho(\ell^\lambda) = h^\lambda = h$. Thus, there exist traces $t_1, \ldots, t_m \in \mathrm{IRR}(S') \cap \mathbb{M}_i$ with $\chi(s, t_1, \ldots, t_m, \tilde{w})$ in $(\mathbb{M}', \overline{\ })$. By Lemma 27 and Lemma 28 there exists $1 \le j \le \lambda$ such that $\chi_h^k(\kappa_j(s), \kappa_j(t_1), \ldots, \kappa_j(t_m), \tilde{w})$ in $(\mathbb{M}' * \{k, \overline{k}\}^*, \overline{\ })$ (recall that $\kappa_j(w) = w$ for all $w \in W$). Note that we can write $\kappa_j(s) = s_1\, k\, s_2$ for $s_1, s_2 \in \mathrm{IRR}(S) \subseteq \mathbb{M}$ such that $\rho(s_1) h \rho(s_2) = h$. Thus

$$\exists Y_1, \ldots, Y_m \in \mathrm{IRR}(S'_k) : \chi_h^k(s_1 k s_2, Y_1, \ldots, Y_m, \tilde{w})\ \wedge \bigwedge_{1 \le i \le m} Y_i \in \mathbb{M}_i * \{k, \overline{k}\}^*$$

is true in $(\mathbb{M}' * \{k, \overline{k}\}^*, \overline{\ })$.

Acknowledgments We would like to thank Yuri Matiyasevich for his proof of Proposition 16 and Yuri Gurevich for his hint to consider randomness in Section 6.3.

References

[1] I. J. Aalbersberg and H. J. Hoogeboom. Characterizations of the decidability of some problems for regular trace languages. *Mathematical Systems Theory*, 22:1–19, 1989.

[2] M. Benois. Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris*, Sér. A, 269:1188–1190, 1969.

[3] L. Berman. The complexity of logical theories. *Theoretical Computer Science*, 11:71–77, 1980.

[4] J. Berstel. *Transductions and context–free languages.* Teubner Studienbücher, Stuttgart, 1979.

[5] R. V. Book and F. Otto. *String–Rewriting Systems.* Springer, 1993.

[6] P. Cartier and D. Foata. *Problèmes combinatoires de commutation et réarrangements.* Number 85 in Lecture Notes in Mathematics. Springer, 1969.

[7] V. Diekert, C. Gutiérrez, and C. Hagenah. The existential theory of equations with rational constraints in free groups is PSPACE-complete. In A. Ferreira and H. Reichel, editors, *Proceedings of the 18th Annual Symposium on Theoretical Aspects of Computer Science (STACS 2001), Dresden (Germany)*, number 2010 in Lecture Notes in Computer Science, pages 170–182. Springer, 2001.

[8] V. Diekert and M. Lohrey. Existential and positive theories of equations in graph products. In H. Alt and A. Ferreira, editors, *Proceedings of the 19th Annual Symposium on Theoretical Aspects of Computer Science (STACS 2002), Juan les Pins (France)*, number 2285 in Lecture Notes in Computer Science, pages 501–512. Springer, 2002.

[9] V. Diekert and M. Lohrey. A note on the existential theory of equations in plain groups. *International Journal of Algebra and Computation*, 12(1 & 2):1–7, 2002.

[10] V. Diekert, Y. Matiyasevich, and A. Muscholl. Solving word equations modulo partial commutations. *Theoretical Computer Science*, 224(1–2):215–235, 1999.

[11] V. Diekert and A. Muscholl. Solvability of equations in free partially commutative groups is decidable. In F. Orejas, P. G. Spirakis, and J. van Leeuwen, editors, *Proceedings of the 28th International Colloquium on Automata, Languages and Programming (ICALP 2001), Crete (Greece)*, number 2076 in Lecture Notes in Computer Science, pages 543–554. Springer, 2001.

[12] V. Diekert and G. Rozenberg, editors. *The Book of Traces.* World Scientific, 1995.

[13] C. Droms. Graph groups, coherence and three-manifolds. *Journal of Algebra*, 106(2):484–489, 1985.

[14] V. G. Durnev. Undecidability of the positive $\forall\exists^3$-theory of a free semi-group. *Sibirsky Matematicheskie Jurnal*, 36(5):1067–1080, 1995. English translation.

[15] S. Feferman and R. L. Vaught. The first order properties of products of algebraic systems. *Fundamenta Mathematicae*, 47:57–103, 1959.

[16] J. Ferrante and C. Rackoff. A decision procedure for the first order theory of real addition with order. *SIAM Journal on Computing*, 4:69–76, 1975.

[17] E. R. Green. *Graph Products of Groups.* PhD thesis, The University of Leeds, 1990.

[18] C. Gutiérrez. Satisfiability of equations in free groups is in PSPACE. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC'2000)*, pages 21–27. ACM Press, 2000.

[19] R. H. Haring-Smith. Groups and simple languages. *Transactions of the American Mathematical Society*, 279:337–356, 1983.

[20] S. Hermiller and J. Meier. Algorithms and geometry for graph products of groups. *Journal of Algebra*, 171:230–257, 1995.

[21] M. Jantzen. Confluent string rewriting. In *EATCS Monographs on theoretical computer science*, volume 14. Springer, 1988.

[22] D. Kozen. Lower bounds for natural proof systems. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science (FOCS 77)*, pages 254–266. IEEE Computer Society Press, 1977.

[23] G. Lallement. *Semigroups and Combinatorial Applications*. Willey-Interscience, 1979.

[24] M. Lohrey. Confluence problems for trace rewriting systems. *Information and Computation*, 170:1–25, 2001.

[25] G. S. Makanin. The problem of solvability of equations in a free semigroup. *Math. Sbornik*, 103:147–236, 1977. In Russian; English translation in *Math. USSR Sbornik 32, 1977*.

[26] G. S. Makanin. Equations in a free group. *Izv. Akad. Nauk SSR*, Ser. Math. 46:1199–1273, 1983. In Russian; English translation in *Math. USSR Izvestija 21, 1983*.

[27] G. S. Makanin. Decidability of the universal and positive theories of a free group. *Izv. Akad. Nauk SSSR*, Ser. Mat. 48:735–749, 1984. In Russian; English translation in *Math. USSR Izvestija, 25*, 75–88, 1985.

[28] S. S. Marchenkov. Unsolvability of the positive ∀∃-theory of a free semi-group. *Sibirsky Matematicheskie Jurnal*, 23(1):196–198, 1982.

[29] G. Markowsky. Bounds on the index and period of a binary relation on a finite set. *Semigroup Forum*, 13:253–259, 1977.

[30] A. Mazurkiewicz. Concurrent program schemes and their interpretations. DAIMI Rep. PB 78, Aarhus University, Aarhus, 1977.

[31] Y. I. Merzlyakov. Positive formulas on free groups. *Algebra i Logika Sem.*, 5(4):25–42, 1966. In Russian.

[32] A. Muscholl. *Decision and Complexity Issues on Concurrent Systems*. Habilitation thesis, Universität Stuttgart, 1999.

[33] P. Narendran and F. Otto. Preperfectness is undecidable for Thue systems containing only length-reducing rules and a single commutation rule. *Information Processing Letters*, 29:125–130, 1988.

[34] M. H. A. Newman. On theories with a combinatorial definition of "equivalence". *Annals of Mathematics*, 43:223–243, 1943.

[35] E. Ochmański. Regular behaviour of concurrent systems. *Bulletin of the European Association for Theoretical Computer Science (EATCS)*, 27:56–67, 1985.

[36] C. H. Papadimitriou. *Computational Complexity*. Addison Wesley, 1994.

[37] W. Plandowski. Satisfiability of word equations with constants is in PSPACE. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS 99)*, pages 495–500. IEEE Computer Society Press, 1999.

[38] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Comptes Rendus du Premier Congrès des Mathématicienes des Pays Slaves*, pages 92–101, Warsaw, 1929.

[39] E. Rips and Z. Sela. Canonical representatives and equations in hyperbolic groups. *Inventiones Mathematicae*, 120:489–512, 1995.

[40] K. U. Schulz. Makanin's algorithm for word equations — Two improvements and a generalization. In K. U. Schulz, editor, *Word Equations and Related Topics*, number 572 in Lecture Notes in Computer Science, pages 85–150. Springer, 1991.

[41] A. Veloso da Costa. Graph products of monoids. *Semigroup Forum*, 63(2):247–277, 2001.