Decidable Theories of Cayley-graphs*

Dietrich Kuske[1] and Markus Lohrey[2]

[1] Institut für Algebra, Technische Universität Dresden
D-01062 Dresden, Germany
[2] Universität Stuttgart, Institut für Informatik,
Breitwiesenstr. 20-22, D-70565 Stuttgart, Germany
kuske@math.tu-dresden.de, lohrey@informatik.uni-stuttgart.de

Abstract. We prove that a connected graph of bounded degree with only finitely many orbits has a decidable MSO-theory if and only if it is context-free. This implies that a group is context-free if and only if its Cayley-graph has a decidable MSO-theory. On the other hand, the first-order theory of the Cayley-graph of a group is decidable if and only if the group has a decidable word problem. For Cayley-graphs of monoids we prove the following closure properties. The class of monoids whose Cayley-graphs have decidable MSO-theories is closed under free products. The class of monoids whose Cayley-graphs have decidable first-order theories is closed under general graph products. For the latter result on first-order theories we introduce a new unfolding construction, the factorized unfolding, that generalizes the tree-like structures considered by Walukiewicz. We show and use that it preserves the decidability of the first-order theory.
Most of the proofs are omitted in this paper, they can be found in the full version [17].

1 Introduction

The starting point of our consideration was a result by Muller and Schupp [21] showing that the Cayley-graph of any context-free group has a decidable monadic second-order theory (MSO-theory). The questions we asked ourselves were: is there a larger class of groups with this property? Can one show similar results for first-order theories (FO-theories) of Cayley-graphs? Are there analogous connections in monoid theory? Similarly to Muller and Schupp's work, this led to the investigation of graph classes with decidable theories that now forms a large part of the paper at hand. Due to potential applications for the verification of infinite state systems, recently such graph classes have received increasing interest, see [28] for an overview.

Courcelle showed that the class of graphs of tree-width at most b has a decidable MSO-theory (for any $b \in \mathbb{N}$) [5]. A partial converse was proved by Seese [24]

* This work was done while the first author worked at University of Leicester, parts of it were done while the second author was on leave at IRISA, Campus de Beaulieu, 35042 Rennes Cedex, France and supported by the INRIA cooperative research action FISC.

(in conjunction with another result by Courcelle [6]) showing that any class of graphs of bounded degree whose MSO-theory is decidable is of bounded tree-width. On the other hand, there are even trees with an undecidable FO-theory. We therefore restrict attention to connected graphs of bounded degree whose automorphism group has only finitely many orbits. If such a graph G has finite tree-width, then it is context-free (Theorem 3.1). Our proof of this fact is based on the construction of a tree decomposition with quite strong combinatorial properties, using techniques from the theory of groups acting on graphs [10]. By another result of Muller and Schupp [21], G has a decidable MSO-theory.

Using this general result on graphs, we can show that Muller and Schupp's result on Cayley-graphs of context-free groups is optimal: any finitely generated group whose Cayley-graph has a decidable MSO-theory is context-free (Corollary 4.1). A similar result will be also shown for first-order logic: the FO-theory of the Cayley-graph of a group is decidable if and only if the word problem of the group is decidable (Proposition 4.2). One implication is simple since one can express by a first-order sentence that a given word labels a cycle in the Cayley-graph. The other implication follows from Gaifman's locality theorem for first-order logic [14] which allows to restrict quantifications over elements of the Cayley-graph to certain spheres around the unit.

These results for groups do not carry over to monoids, e.g., there is a monoid with a decidable word problem whose Cayley-graph has an undecidable FO-theory (Proposition 6.1). On the other hand, we are able to prove some closure properties of the classes of monoids whose Cayley-graphs have decidable theories. Using a theorem of Walukiewicz [31] (the original statement goes back to work by Stupp [27], Shelah [26], Muchnik, and Semenov, see [31] for an account) on MSO-theories of unfoldings, we prove that the class of finitely generated monoids whose Cayley-graphs have decidable MSO-theories is closed under free products (Theorem 6.3(2)). Moreover, we show that the class of finitely generated monoids whose Cayley-graphs have decidable FO-theories is closed under graph products (Theorem 6.3(1)) which is a well-known construction in mathematics, see e.g. [15, 30]; it generalizes both, the free and the direct product of monoids. In order to show this closure property, we introduce the notion of a factorized unfolding in Section 5, which is also of independent interest (see the discussion in Section 5): Walukiewicz's unfolding of a structure $\mathcal{A}$ consists of the set of words over the set of elements of $\mathcal{A}$. This set of words is equipped with the natural tree structure. Hence the successors of any node of the tree can be identified with the elements of $\mathcal{A}$ and can therefore naturally be endowed with the structure of $\mathcal{A}$. Basically, a factorized unfolding is the quotient of this structure with respect to Mazurkiewicz's trace equivalence (in fact, it is a generalization of this quotient). We show that the FO-theory of a factorized unfolding can be reduced to the FO-theory of the underlying structure (Theorem 5.7). The proof of this result uses techniques of Ferrante and Rackoff [13] and a thorough analysis of factorized unfoldings using ideas from the theory of Mazurkiewicz traces [8]. From this result on factorized unfoldings, we obtain the closure under graph products similarly to the closure under free products.

Our results on FO-theories of Cayley-graphs should be also compared with the classical results about FO-theories of monoids: the FO-theory of a monoid $\mathcal{M}$ contains all true first-order statements about $\mathcal{M}$ that are built over the signature containing the monoid operation and all monoid elements as constants. Thus the FO-theory of the Cayley-graph of $\mathcal{M}$ can be seen as a fragment of the whole FO-theory of $\mathcal{M}$ in the sense that only equations of the form $xa = y$, with x and y variables and $a \in \mathcal{M}$ are allowed. In this context we should mention the classical results of Makanin, stating that the existential FO-theory of a free monoid [18] or free group [19] is decidable, see [7] for a more detailed overview.

2 Preliminaries

Let $\mathcal{A} = (A, (R_i)_{i \in K})$ be a relational structure with carrier set A and relations R_i of arbitrary arity. *First-order logic* (FO) and *monadic second-order logic* (MSO) over the structure $\mathcal{A}$ are defined as usual. The *FO-theory* (resp. *MSO-theory*) of $\mathcal{A}$ is denoted by $\mathrm{FOTh}(\mathcal{A})$ (resp. $\mathrm{MSOTh}(\mathcal{A})$).

A *Σ-labeled directed graph* (briefly graph) is a relational structure $G = (V, (E_a)_{a \in \Sigma})$, where Σ is a finite set of labels, and $E_a \subseteq V \times V$ is the set of all a-labeled edges. The undirected graph that results from G by forgetting all labels and the direction of edges is denoted by $\mathrm{undir}(G)$. We say that G is *connected* if $\mathrm{undir}(G)$ is connected. We say that G has *bounded degree*, if for some constant $c \in \mathbb{N}$, every node of G is incident with at most c edges in $\mathrm{undir}(G)$. The *diameter* of $U \subseteq V$ in G is the maximal distance in $\mathrm{undir}(G)$ between two nodes $u, v \in U$ (which might be ∞).

In Section 3 we will consider graphs of bounded tree-width. We will omit the formal definition of tree-width (see e.g. [9]) since we are mainly interested in the stronger notion of *strong tree-width.* A *strong tree decomposition* of an undirected graph $G = (V, E)$ is a partition $P = \{V_i \mid i \in K\}$ of V such that the quotient graph $G/_P = (P, E/_P)$, where $E/_P = \{(V_i, V_j) \in P \times P \mid V_i \times V_j \cap E \neq \emptyset\}$, is a forest, i.e., acyclic [23]. The *width of P* is the supremum of the cardinalities $|V_i|$, $i \in K$. If there exists a strong tree decomposition P of G of width at most b then G has *strong tree-width at most b.*

3 Graphs with a decidable MSO-theory

In [21], Muller & Schupp gave a graph-theoretical characterization of the transition graphs of pushdown automata, which are also called *context-free graphs.* Moreover, in [21] it is shown that the MSO-theory of any context-free graph is decidable. In this section, we outline a proof of the converse implication for graphs with a high degree of symmetry. More precisely, we consider graphs with only *finitely many orbits.* Here the orbits of a graph $G = (V, (E_a)_{a \in \Sigma})$ are the equivalence classes with respect to the equivalence $\sim$ defined as follows: $u \sim v$ for $u, v \in V$ if and only if there exists an automorphism f of G with $f(u) = v$.

Theorem 3.1. *Let $G = (V, (E_a)_{a\in\Sigma})$ be a connected graph of bounded degree with only finitely many orbits. Then* $\mathrm{MSOTh}(G)$ *is decidable if and only if* $\mathrm{undir}(G)$ *has finite tree-width if and only if G is context-free.*

Proof (sketch). Assume that $\mathrm{MSOTh}(G)$ is decidable. Notice that MSO only allows quantification over sets of nodes, whereas quantification over sets of edges is not possible. On the other hand, for graphs of bounded degree, Courcelle [6] has shown that the extension of MSO by quantification over sets of edges, which is known as MSO_2, can be defined within MSO. Thus the MSO_2-theory of G is decidable. A result of Seese [24] implies that $\mathrm{undir}(G)$ has finite tree-width.

Thus, assume that $H = \mathrm{undir}(G)$ has tree-width at most b for some $b \in \mathbb{N}$. Then also any finite subgraph of H has tree-width at most b. Since the degree of H is bounded by some constant d, the same holds for its finite subgraphs. Hence, by a result from [3], any finite subgraph of H has strong tree-width at most $c = (9b + 7)d(d + 1)$. From these strong tree decompositions of the finite subgraphs of H, one can construct a strong tree decomposition P of H of width at most c as follows. Since H is connected and of bounded degree, H must be countable. Thus we can take an ω-sequence $(G_i)_{i\in\mathbb{N}}$ of finite subgraphs of H whose limit is H. From the non-empty set of all strong-tree decompositions of width at most c of the graphs G_i, $i \in \mathbb{N}$, we construct a finitely branching tree as follows. Put an edge between a strong tree decomposition P_i (of width at most c) of G_i and a strong tree decomposition P_{i+1} (of width at most c) of G_{i+1} if P_i results from P_{i+1} by restriction to the nodes of G_i. By König's Lemma, this tree contains an infinite path. Taking the limit along this path results in a strong tree decomposition P of H of width at most c.

By splitting some of the partition classes of P, we can refine P into a strong tree decomposition Q of width at most c with the following property: for all edges (V_1, V_2) of the quotient graph $H/_Q$, removing all edges between V_1 and V_2 (note that there are at most c^2 such edges) splits H into exactly two connected components. In the terminology of [10, 29], the set of edges connecting V_1 and V_2 is called a *tight c^2-cut* of H. By [10, Paragraph 2.5] (see also [29, Prop. 4.1] for a simplified proof), every edge of H is contained in only finitely many tight c^2-cuts. From this fact and the assumption that G, and hence also H, has only finitely many orbits, one can deduce that the diameter of every partition class in Q is bounded by some fixed constant $\gamma \in \mathbb{N}$. Using this, one can show that the graph G can be $(2\gamma + 1)$-triangulated [20], this step is similar to the proof of [2, Thm. 8]. Then essentially the same argument that was given in the proof of [21, Thm. 2.9] for a vertex-transitive graph (i.e., a graph that has only one orbit) shows that G is context-free.

The remaining implication "G context-free $\Rightarrow$ $\mathrm{MSOTh}(G)$ decidable" was shown in [21]. □

Remark 3.2. In [25] it was shown that if G is context-free then also $G/_\sim$ is context-free. Thus, a natural generalization of the previous theorem could be the following: Let G be a connected graph of bounded degree such that the quotient graph $G/_\sim$ is context-free with finitely many orbits. Then G has a decidable

MSO-theory if and only if G is context-free. But this is false: take $\mathbb{Z}$ together with the successor relation and add to every number $m = \frac{1}{2}n(n+1)$ $(n \in \mathbb{Z})$ a copy m' together with the edge (m, m'), whereas for every other number m we add two copies m' and m'' together with the edges (m, m') and (m, m''). The resulting graph is not context-free, but it has a decidable MSO-theory [11] (see also [21]) and $G/_\sim$ is context-free with just two orbits.

4 Cayley-graphs of groups

Let $\mathcal{G}$ be a group generated by the finite set Γ. Its *Cayley graph* $\mathbb{C}(\mathcal{G}, \Gamma)$ has as vertices the elements of $\mathcal{G}$ and as a-labeled edges the pairs (x, xa) for $x \in \mathcal{G}$ and $a \in \Gamma$. The word problem of $\mathcal{G}$ wrt. Γ is the set of words over $\Gamma \cup \{a^{-1} \mid a \in \Gamma\}$ that represent the identity of $\mathcal{G}$. It is well known that the decidability of the word problem does not depend on the chosen generating set; henceforth we will speak of *the* word problem regardless of the generators. The group $\mathcal{G}$ is called *context-free* if its word problem is a context free language [1, 20]. By [21] this is equivalent to saying that $\mathbb{C}(\mathcal{G}, \Gamma)$ is a context-free graph. The automorphism group of any Cayley-graph acts transitively on the vertices (i.e., has just one orbit). Furthermore, Cayley-graphs are always connected. If the group is finitely generated, then moreover its Cayley-graph has bounded degree. Thus, from Theorem 3.1, we get the following (the implication "$\Rightarrow$" is due to Muller & Schupp)

Corollary 4.1. *Let $\mathcal{G}$ be a group finitely generated by Γ. Then $\mathcal{G}$ is context-free if and only if* $\mathrm{MSOTh}(\mathbb{C}(\mathcal{G}, \Gamma))$ *is decidable.*

For FO-theories we obtain

Proposition 4.2. *Let $\mathcal{G}$ be a group finitely generated by Γ. Then the following are equivalent:*

(1) The word problem of $\mathcal{G}$ is decidable.
(2) $\mathrm{FOTh}(\mathbb{C}(\mathcal{G}, \Gamma))$ *is decidable.*
(3) The existential FO-theory of the Cayley-graph $\mathbb{C}(\mathcal{G}, \Gamma)$ is decidable.

Proof (sketch). The implication (2) $\Rightarrow$ (3) is trivial. The implication (3) $\Rightarrow$ (1) is easily shown since a word over $\Gamma \cup \{a^{-1} \mid a \in \Gamma\}$ represents the identity of $\mathcal{G}$ if and only if it labels some cycle in the Cayley-graph, an existential property expressible in first-order logic. The remaining implication is shown using Gaifman's theorem [14]: since the automorphism group of $\mathbb{C}(\mathcal{G}, \Gamma)$ acts transitively on the vertices, it implies that it suffices to decide first-order properties of spheres in $\mathbb{C}(\mathcal{G}, \Gamma)$ around the identity of $\mathcal{G}$. But these spheres are finite and effectively computable since the word problem is decidable. □

In the complete version of this extended abstract [17], we prove that every FO-sentence is equivalent in $\mathbb{C}(\mathcal{G}, \Gamma)$ to the same sentence but with all quantifiers restricted to spheres around the unit of at most exponential diameter. This proof uses techniques developed by Ferrante and Rackoff [13]. In addition to the above result, it provides a tight relationship between the word problem of $\mathcal{G}$ and $\mathrm{FOTh}(\mathbb{C}(\mathcal{G}, \Gamma))$ in terms of complexity: the space complexity of $\mathrm{FOTh}(\mathbb{C}(\mathcal{G}, \Gamma))$ is bounded exponentially in the space complexity of the word problem of $\mathcal{G}$ [17].

5 Factorized unfoldings

In [31], Walukiewicz proved that the MSO-theory of the tree-like unfolding of a relational structure can be reduced to the MSO-theory of the underlying structure. The origin of this result goes back to [26, 27]. Tree-like unfoldings are defined as follows:

Definition 5.1. *Let $\mathcal{A} = (A, (R_i)_{1\le i\le n})$ be a relational structure where the relation R_i has arity p_i. On the set of finite words A^*, we define the following relations:*

$$\begin{aligned}\widehat{R_i} &= \{(ua_1, ua_2, \dots, ua_{p_i}) \mid u \in A^*, (a_1, a_2, \dots, a_{p_i}) \in R_i\}\\ \mathrm{suc} &= \{(u, ua) \mid u \in A^*, a \in A\}\\ \mathrm{cl} &= \{(ua, uaa) \mid u \in A^*, a \in A\}\end{aligned}$$

Then the relational structure $\widehat{\mathcal{A}} = (A^*, (\widehat{R_i})_{1\le i\le n}, \mathrm{suc}, \mathrm{cl})$ is called the tree-like unfolding *of $\mathcal{A}$.*

Theorem 5.2 (cf. [31]). *Let $\mathcal{A}$ be a relational structure. Then $\mathrm{MSOTh}(\widehat{\mathcal{A}})$ can be reduced to $\mathrm{MSOTh}(\mathcal{A})$.*

We will in particular use the immediate consequence that $\mathrm{MSOTh}(\widehat{\mathcal{A}})$ is decidable whenever the MSO-theory of $\mathcal{A}$ is decidable. The main result of this section is a FO-analogue of the above result (Theorem 5.7).

The relations of the tree-like unfoldings are instances of a more general construction that will be crucial for our notion of factorized unfoldings. Let $\varphi(x_1, x_2, \dots, x_n)$ be a first-order formula over the signature of $\mathcal{A}$ with n free variables. For a word $w = a_1a_2\cdots a_n \in A^*$ of length n we write $\mathcal{A} \models \varphi(w)$ if $\mathcal{A} \models \varphi(a_1, a_2, \dots, a_n)$. An n-ary relation R over A^* is *k-suffix definable* in $\mathcal{A}$ if there are $k_1, \dots, k_n \le k$ ($k_i = 0$ is allowed) and a first-order formula φ over the signature of $\mathcal{A}$ with $\sum_{i=1}^{n} k_i$ free variables such that

$$R = \{(uu_1,\ uu_2,\ \dots, uu_n) \mid u, u_i \in A^*, |u_i| = k_i, \mathcal{A} \models \varphi(u_1u_2\cdots u_n)\}.$$

Obviously, all relations of $\widehat{\mathcal{A}}$ are 2-suffix definable in $\mathcal{A}$. On the other hand, there exist 2-suffix definable relations such that adding them to $\widehat{\mathcal{A}}$ makes Theorem 5.2 fail. To see this, let

$$\mathrm{eq} = \{(ua, uba) \mid u \in A^*, a, b \in A\},$$

which is 2-suffix definable in $\mathcal{A}$. Define the prefix order $\preceq$ on A^* by $\preceq = \{(u, uv) \mid u, v \in A^*\}$, it is the reflexive transitive closure of the relation suc from $\widehat{\mathcal{A}}$, thus it is MSO-definable in $\widehat{\mathcal{A}}$. Let $A = \mathbb{N} \cup \{a, b\}$ be the set of natural numbers together with two additional elements. On A we define the predicates $S = \{(n, n+1) \mid n \in \mathbb{N}\}$, $U_a = \{a\}$, and $U_b = \{b\}$. Then the structure $\mathcal{A} = (A, S, U_a, U_b)$ has a decidable MSO-theory. We consider the structure $\mathcal{B} = (A^*, \widehat{S}, \widehat{U_a}, \widehat{U_b}, \mathrm{suc})$, which is a reduct of the tree-like unfolding of $\mathcal{A}$. Using FO-logic over $(\mathcal{B}, \mathrm{eq}, \preceq)$, we can express that a given 2-counter machine terminates. Thus we obtain

Proposition 5.3. $\mathrm{FOTh}(\mathcal{B}, \mathrm{eq}, \preceq)$ *is undecidable.*

In particular, the MSO-theory of $(\mathcal{B}, \mathrm{eq})$ is undecidable. Thus, the presence of the relation eq makes Walukiewicz's result fail.

Recall that the underlying set of the tree-like unfolding of a structure $\mathcal{A}$ is the set of words over the carrier set of $\mathcal{A}$. In factorized unfoldings that we introduce next, this underlying set consists of equivalence classes of words wrt. Mazurkiewicz's trace equivalence:

A (not necessarily finite) set A together with an irreflexive and symmetric relation $I \subseteq A \times A$ is called *independence alphabet*, the relation I is the *independence relation.* With any such independence alphabet, we associate the least congruence $\equiv_I$ on A^* identifying ab and ba for $(a, b) \in I$. The quotient $\mathbb{M}(A, I) = A^*/{\equiv_I}$ is the *free partially commutative* or *(Mazurkiewicz) trace monoid* generated by (A, I). The trace that is represented by the word $w \in A^*$ is denoted by $[w]_I$. Note that for $I = \emptyset$, the trace monoid $\mathbb{M}(A, I)$ is isomorphic to the free monoid A^*. In the other extreme, i.e., if $I = (A \times A) \setminus \{(a, a) \mid a \in A\}$, we have $\mathbb{M}(A, I) \cong \mathbb{N}^A$, i.e., the trace monoid is free commutative generated by A. For a trace $t \in \mathbb{M}(A, I)$, we let $\min(t) = \{a \in A \mid \exists s \in A^* : t = [as]_I\}$ the set of minimal symbols of t. The set $\max(t)$ of maximal symbols of t is defined analogously. For an n-ary relation R over A^*, we define its I-quotient

$$R/_I = \{([u_1]_I, \ldots, [u_n]_I) \mid (u_1, \ldots, u_n) \in R\}.$$

Definition 5.4. *Let $\mathcal{A}$ be a relational structure with carrier set A. Let furthermore*

- *$I \subseteq A \times A$ be an independence relation which is first-order definable in $\mathcal{A}$,*
- *$\eta : \mathbb{M}(A, I) \to S$ be a monoid morphism into some finite monoid S such that $\eta^{-1}(s) \cap A$ is first-order definable in $\mathcal{A}$ for all $s \in S$.*
- *R_i be a k_i-suffix definable relation in $\mathcal{A}$ for $1 \leq i \leq n$.*

Then the structure $\mathcal{B} = (\mathbb{M}(A, I), (\eta^{-1}(s))_{s \in S}, (R_i/_I)_{1 \leq i \leq n})$ is a factorized unfolding of $\mathcal{A}$.

Note that in contrast to the tree-like unfolding there are many different factorized unfoldings of $\mathcal{A}$. The notion of a factorized unfolding is a proper generalization of the tree-like unfolding even in case $I = \emptyset$: by Proposition 5.3, the relation eq cannot be defined in the tree-like unfolding, but since it is 2-suffix definable it may occur in a factorized unfolding. On the other hand, if $I = \emptyset$, then, since $\eta^{-1}(s) \cap A$ is first-order definable in $\mathcal{A}$, the set $\eta^{-1}(s) \subseteq \mathbb{M}(A, I) = A^*$ is MSO-definable in the tree-like unfolding of $\mathcal{A}$. Since Walukiewicz was interested in the MSO-theory of his unfolding, the relations $\eta^{-1}(s)$ are "effectively present" in $\widehat{\mathcal{A}}$.

The structure $(\mathcal{B}, \mathrm{eq}, \preceq)$ from Proposition 5.3 has an undecidable FO-theory. Thus, allowing the relation $\preceq/_I$ in factorized unfoldings would make the main result of this section (Theorem 5.7) fail. In Theorem 5.7, we will also assume that there are only finitely many different sets $I(a) = \{b \in A \mid (a, b) \in I\}$, which roughly speaking means that traces from $\mathbb{M}(A, I)$ have only "bounded parallelism". The reason is again that otherwise the result would fail:

Proposition 5.5. *There exists an infinite structure $\mathcal{A}$ and a factorized unfolding $\mathcal{B}$ of $\mathcal{A}$ such that* $\mathrm{FOTh}(\mathcal{A})$ *is decidable but* $\mathrm{FOTh}(\mathcal{B})$ *is undecidable.*

Proof (sketch). Let $(V, E) = K_{\aleph_0}$ be a countable complete graph, $A = V \dot\cup E$, and $R \subseteq (V \times E)$ be the incidence relation. Furthermore, $I = (A \times A) \setminus \mathrm{id}_A$. Then we think of a trace $t \in \mathbb{M}(A, I)$ as representing the subgraph $\max(t) \subseteq A$ of $K_{\aleph_0}$. This allows to reduce the FO-theory of all finite graphs to the FO-theory of the factorized unfolding $(\mathbb{M}(A, I), \mathrm{cl}/_I, R/_I)$ of $\mathcal{A}$. The former theory is undecidable by a result of Trakhtenbrot. □

In Proposition 5.3 and 5.5 we used infinite structures $\mathcal{A}$. Infinity is needed as the following shows:

Proposition 5.6. *Let $\mathcal{A}$ be a finite structure and $\mathcal{B}$ be a factorized unfolding of $\mathcal{A}$. Then $(\mathcal{B}, \preceq/_I)$ is an automatic structure [16]; hence its FO-theory is decidable.*

Proof (sketch). The underlying set of the structure $\mathcal{B}$ is the set of traces $\mathbb{M}(A, I)$. For these traces, several normal forms are known [8], here we use the Foata normal form. Since $\mathcal{A}$ is finite, all the relations in $(\mathcal{B}, \preceq/_I)$ (more precisely: their Foata normal form incarnations) are synchronized rational relations. □

Now we finally formulate the main result of this section:

Theorem 5.7. *Let $\mathcal{A}$ be a relational structure and consider a factorized unfolding $\mathcal{B} = (\mathbb{M}(A, I), (\eta^{-1}(s))_{s \in S}, (R_i/_I)_{1 \le i \le n})$ of $\mathcal{A}$ where $\{I(a) \mid a \in A\} \subseteq 2^A$ is finite. Then* $\mathrm{FOTh}(\mathcal{B})$ *can be reduced to* $\mathrm{FOTh}(\mathcal{A})$.

Proof (sketch). For a trace $t \in \mathbb{M}(A, I)$, let $|t|$ be the length of any word representing t. We will write $\exists x \le n : \psi$ as an abbreviation for $\exists x : |x| \le n \wedge \psi$, i.e., $\exists x \le n$ restricts quantification to traces of length at most n. In order to use techniques similar to those developed by Ferrante and Rackoff [13], one then defines a computable function $H : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with the following property:

Let $\varphi = Q_1 x_2\, Q_2 x_2\, \ldots Q_d x_d\, \psi$ be a formula in prenex normal form over the signature of $\mathcal{B}$, where $Q_i \in \{\forall, \exists\}$. Then $\mathcal{B} \models \varphi$ if and only if

$$\mathcal{B} \models Q_1 x_1 \le H(1, d)\, Q_2 x_2 \le H(2, d)\, \ldots Q_d x_d \le H(d, d) : \psi \qquad (1)$$

In order to be able to define H, the assumption that there are only finitely many sets $I(a)$ is crucial.

At this point we have restricted all quantifications to traces of bounded length. Now a variable x that ranges over traces of length n can be replaced by a sequence of first-order variables $y_1 \cdots y_n$ ranging over A. Since I is FO-definable in $\mathcal{A}$, we can express in FO-logic over $\mathcal{A}$ that two such sequences represent the same trace. Since also $\eta^{-1}(s)$ is first-order definable in $\mathcal{A}$ for every $s \in S$ and all other relations in $\mathcal{B}$ result from k-suffix definable relations, it follows that (1) can be translated into an equivalent first-order statement about $\mathcal{A}$. □

Remark 5.8. The function $H : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ refered to in the above proof satisfies $H(i, d) \le H(i + 1, d)$ and $H(d, d) \in 2^{O(d)}$ (values for $H(i, d)$ with $i > d$ are not used in the proof). This allows to show that this procedure transforms a formula φ over the signature of $\mathcal{B}$ into a formula of size $2^{2^{O(|\varphi|)}}$ over the signature of $\mathcal{A}$.

6 Cayley-graphs of monoids

The Cayley-graph $\mathbb{C}(\mathcal{M},\Gamma)$ of a monoid $\mathcal{M}$ wrt. some finite set of generators Γ can be defined analogously to that of a group. It will turn out to be convenient to consider the *rooted Cayley-graph* $(\mathbb{C}(\mathcal{M},\Gamma),1)$ that in addition contains a constant 1 for the unit element of the monoid $\mathcal{M}$.

It is easily checked that the implications (2) $\Rightarrow$ (3) $\Rightarrow$ (1) from Proposition 4.2 carry over to monoids, but the situation for the remaining implication is different. The following proposition follows from [22, Thm. 2.4].

Proposition 6.1. *There is a finitely presented monoid $\mathcal{M}$ with a decidable word problem such that $\mathbb{C}(\mathcal{M},\Gamma)$ has an undecidable existential FO-theory.*

On the decidability side let us mention that Cayley-graphs of automatic monoids [4] have decidable FO-theories since they are automatic structures [16].

In the sequel, we will prove closure properties of classes of monoids with decidable theories. Using simple MSO-interpretations it is easy to see that the class of finitely generated monoids, whose Cayley-graphs have decidable MSO-theories, is closed under finitely generated submonoids and Rees-quotients w.r.t. rational ideals. Moreover, if $\mathrm{MSOTh}(\mathbb{C}(\mathcal{M},\Gamma),1)$ is decidable and S is a finite monoid then also $\mathrm{MSOTh}(\mathbb{C}(\mathcal{M}\times S,\Gamma\cup S),1)$ is easily seen to be decidable.

Now, we consider graph products of monoids [15] which generalize both, the direct and the free product. In order to define it, let (Σ,J) be some finite independence alphabet and let $\mathcal{M}_\sigma$ be a monoid for $\sigma\in\Sigma$. Then the *graph product* $\prod_{(\Sigma,J)}\mathcal{M}_\sigma$ is the quotient of the free product of the monoids $\mathcal{M}_\sigma$ subject to the relations $ab=ba$ for $a\in\mathcal{M}_\sigma$, $b\in\mathcal{M}_\tau$ and $(\sigma,\tau)\in J$. If $J=\emptyset$, then there are no such relations, i.e., the graph product equals the free product $*_{\sigma\in\Sigma}\mathcal{M}_\sigma$. If, in the other extreme, $J=(\Sigma\times\Sigma)\setminus\{(\sigma,\sigma)\mid\sigma\in\Sigma\}$, then the graph product equals the direct product $\prod_{\sigma\in\Sigma}\mathcal{M}_\sigma$. For the subsequent discussions, fix some finite independence alphabet (Σ,J) and for every $\sigma\in\Sigma$ a monoid $\mathcal{M}_\sigma=(\mathcal{M}_\sigma,\circ_\sigma,1_\sigma)$, which is generated by the finite set Γ_σ. Furthermore, let $\mathcal{M}=(\mathcal{M},\circ,1)=\prod_{(\Sigma,J)}\mathcal{M}_\sigma$ be the graph product of these monoids wrt. (Σ,J). This monoid is generated by the finite set $\Gamma=\bigcup_{\sigma\in\Sigma}\Gamma_\sigma$.

We will prove decidability results for the theories of the rooted Cayley-graph $(\mathbb{C}(\mathcal{M},\Gamma),1)$ using Theorems 5.2 and 5.7. In these applications, the underlying structure $\mathcal{A}$ will always be the disjoint union of the rooted Cayley-graphs $(\mathbb{C}(\mathcal{M}_\sigma,\Gamma_\sigma),1_\sigma)$. Hence the carrier set A of the structure $\mathcal{A}$ is the disjoint union of the monoids $\mathcal{M}_\sigma$. It has binary edge-relations $E_a=\{(x,x\circ_\sigma a)\mid x\in\mathcal{M}_\sigma\}\subseteq\mathcal{M}_\sigma\times\mathcal{M}_\sigma$ for all $\sigma\in\Sigma$ and $a\in\Gamma_\sigma$, as well as unary relations $A_\sigma\subseteq A$ comprising all elements of the monoid $\mathcal{M}_\sigma$, and unary relations $U_\sigma=\{1_\sigma\}$. We now define a factorized unfolding $\mathcal{B}$ of this disjoint union $\mathcal{A}$: the independence relation

$$I=\bigcup_{(\sigma,\tau)\in J}\mathcal{M}_\sigma\times\mathcal{M}_\tau$$

is FO-definable in $\mathcal{A}$ using the unary predicates A_σ. Since Σ is finite, there are only finitely many sets $I(a)$ for $a\in A$. The relations $\widehat{E_a},\widehat{U_\sigma},\mathrm{suc}$, and $\mathrm{suc}_a=$

$\{(x, xa) \mid x \in A^*\}$, where $\sigma \in \Sigma$ and $a \in \Gamma \subseteq A$, are 1-suffix definable in $\mathcal{A}$ (note that every $a \in \Gamma$ is FO-definable in $\mathcal{A}$). We define the monoid morphism η in such a way that we are able to interpret the rooted Cayley-graph $(\mathbb{C}(\mathcal{M}, \Gamma), 1)$ in the factorized unfolding $\mathcal{B}$. In particular, elements of the graph product $\mathcal{M}$ will be represented by traces over (A, I). To this aim, the following paragraph defines the mapping η as follows:

For $a \in A$, let $\mu(a) \in \Sigma$ be the unique index with $a \in \mathcal{M}_{\mu(a)}$ and define $\mu(t) = \{\mu(a) \mid a \text{ occurs in } t\}$ for $t \in \mathbb{M}(A, I)$. Then set $\eta(t) = \bot$ if there is $\sigma \in \Sigma$ such that 1_σ is a factor of the trace t, or if there are $a, b \in \mathcal{M}_\sigma$ such that the trace ab is a factor of the trace t. If this is not the case, let $\eta(t) = (\mu(\min(t)), \mu(t), \mu(\max(t)))$. Thus, η is a mapping from $\mathbb{M}(A, I)$ into some finite set S. Then the kernel $\{(s, t) \in \mathbb{M}(A, I) \times \mathbb{M}(A, I) \mid \eta(s) = \eta(t)\}$ of η is a monoid congruence. In other words, the set S can be endowed with a monoid structure such that η is actually a monoid morphism into some finite monoid.

Now we have collected all the ingredients for our factorized unfolding of $\mathcal{A}$:

$$\mathcal{B} = (\mathbb{M}(A, I),\ (\eta^{-1}(s))_{s \in S},\ (\widehat{E_a}/_I)_{a \in \Gamma},\ (\widehat{U_\sigma}/_I)_{\sigma \in \Sigma},\ \mathrm{suc}/_I,\ (\mathrm{suc}_a/_I)_{a \in \Gamma})$$

is a factorized unfolding of $\mathcal{A}$. Note that it does not contain the relation $\mathrm{eq}/_I$. Therefore, in case $J = \emptyset$ (i.e., $I = \emptyset$) $\mathcal{B}$ is MSO-definable in the tree-like unfolding $\widehat{\mathcal{A}}$, which will allow to apply Theorem 5.2. A major step towards a proof of Theorems 6.3 is

Lemma 6.2. *There is a first-order interpretation of the rooted Cayley-graph $(\mathbb{C}(\mathcal{M}, \Gamma), 1)$ in the factorized unfolding $\mathcal{B}$ of $\mathcal{A}$.*

Proof (sketch). The elements of the graph product $\mathcal{M}$ can be identified with those traces t that satisfy $\eta(t) \neq \bot$ (in the terminology of [30], they are Γ-equivalence classes of words of the form $S(u)$). In order to define the edges of the rooted Cayley-graph $(\mathbb{C}(\mathcal{M}, \Gamma), 1)$ within $\mathcal{B}$, let us take $s, t \in \mathbb{M}(A, I)$ with $\eta(s) \neq \bot \neq \eta(t)$ and let $\sigma \in \Sigma$, $a \in \Gamma_\sigma$. Then one can show that $s \circ a = t$ (here we view s and t as elements of $\mathcal{M}$) if and only if the following holds in $\mathbb{M}(A, I)$:

- $sa = t$, or
- there is $b \in \mathcal{M}_\sigma$ such that $b \circ_\sigma a = 1_\sigma$ and $tb = s$, or
- there is $b \in \mathcal{M}_\sigma$ and $u \in \mathbb{M}(A, I)$ with $s = ub$, $b \circ_\sigma a \neq 1_\sigma$, and $t = u\,(b \circ_\sigma a)$.

All these properties can be easily expressed in first-order logic over $\mathcal{B}$. □

Now we can show the main result of this section:

Theorem 6.3. *Let $\mathcal{M} = \prod_{(\Sigma, J)} \mathcal{M}_\sigma$, where (Σ, J) is a finite independence alphabet and $\mathcal{M}_\sigma$ is a monoid finitely generated by Γ_σ ($\sigma \in \Sigma$). Let $\Gamma = \bigcup_{\sigma \in \Sigma} \Gamma_\sigma$.*

(1) If $\mathrm{FOTh}(\mathbb{C}(\mathcal{M}_\sigma, \Gamma_\sigma), 1_\sigma)$ is decidable for all $\sigma \in \Sigma$, then $\mathrm{FOTh}(\mathbb{C}(\mathcal{M}, \Gamma), 1)$ is decidable as well.
(2) If $J = \emptyset$ and $\mathrm{MSOTh}(\mathbb{C}(\mathcal{M}_\sigma, \Gamma_\sigma), 1_\sigma)$ is decidable for all $\sigma \in \Sigma$, then $\mathrm{MSOTh}(\mathbb{C}(\mathcal{M}, \Gamma), 1)$ is decidable as well.

Proof. First assume that $\mathrm{FOTh}(\mathbb{C}(\mathcal{M}_\sigma, \Gamma_\sigma), 1_\sigma)$ is decidable for all $\sigma \in \Sigma$. Lemma 6.2 implies that we can reduce $\mathrm{FOTh}(\mathbb{C}(\mathcal{M}, \Gamma), 1)$ to the FO-theory of the factorized unfolding $\mathcal{B}$, which is decidable by Theorem 5.7 since $\mathrm{FOTh}(\mathcal{A})$ is decidable by [12]. The second statement on MSO-theories follows similarly by refering to [31] and [26] instead of Theorem 5.7 and [12], respectively. □

Statement (2) from Theorem 6.3 does not generalize to graph products.

Proposition 6.4. *Let* (Σ, J), $\mathcal{M}_\sigma$, Γ_σ, $\mathcal{M}$, *and* Γ *as in Theorem 6.3 with* $\mathcal{M}_\sigma$ *non-trivial. Assume furthermore that* $\mathrm{MSOTh}(\mathbb{C}(\mathcal{M}, \Gamma), 1)$ *is decidable. Then*

(a) (Σ, J) *does not contain an induced cycle of length 4 (also called C4),*
(b) if $(\sigma, \tau) \in J$ *and* $\mathcal{M}_\sigma$ *is infinite, then* $\mathcal{M}_\tau$ *is finite,*
(c) if $(\sigma, \sigma_1), (\sigma, \sigma_2) \in J$, $\sigma_1 \neq \sigma_2$, *and* $\mathcal{M}_\sigma$ *is infinite, then* $(\sigma_1, \sigma_2) \in J$,
(d) $\mathrm{MSOTh}(\mathbb{C}(\mathcal{M}_\sigma, \Gamma_\sigma), 1_\sigma)$ *is decidable for every* $\sigma \in \Sigma$.

Proof (sketch). Condition (a), (b), and (c) hold, since otherwise $\mathcal{M}$ contains a direct product of two infinite monoids and thus $(\mathbb{C}(\mathcal{M}, \Gamma), 1)$ contains an infinite grid. In order to show (d), one defines $(\mathbb{C}(\mathcal{M}_\sigma, \Gamma_\sigma), 1_\sigma)$ in $(\mathbb{C}(\mathcal{M}, \Gamma), 1)$. □

It remains open whether the four conditions in Proposition 6.4 characterize graph products, whose corresponding Cayley-graphs have decidable MSO-theories.

References

1. A. V. Anisimov. Group languages. *Kibernetika*, 4:18–24, 1971. In Russian; English translation in: *Cybernetics 4*, 594–601, 1973.
2. A. Blumensath. Prefix-recognizable graphs and monadic second-order logic. Technical Report 2001-06, RWTH Aachen, Department of Computer Science, 2001.
3. H. L. Bodlaender. A note on domino treewidth. *Discrete Mathematics & Theoretical Computer Science*, 3(4):141–150, 1999.
4. C. M. Campbell, E. F. Robertson, N. Ruškuc, and R. M. Thomas. Automatic semigroups. *Theoretical Computer Science*, 250(1-2):365–391, 2001.
5. B. Courcelle. The monadic second-order logic of graphs, II: Infinite graphs of bounded width. *Mathematical Systems Theory*, 21:187–221, 1989.
6. B. Courcelle. The monadic second-order logic of graphs VI: On several representations of graphs by relational structures. *Discrete Applied Mathematics*, 54:117–149, 1994.
7. V. Diekert. Makanin's algorithm. In M. Lothaire, editor, *Algebraic Combinatorics on Words*, pages 342–390. Cambridge University Press, 2001.
8. V. Diekert and G. Rozenberg, editors. *The Book of Traces.* World Scientific, 1995.
9. R. Diestel. *Graph Theory, Second Edition.* Springer, 2000.
10. M. J. Dunwoody. Cutting up graphs. *Combinatorica*, 2(1):15–23, 1981.
11. C. C. Elgot and M. O. Rabin. Decidability and undecidability of extensions of second (first) order theory of (generalized) successor. *Journal of Symbolic Logic*, 31(2):169–181, 1966.
12. S. Feferman and R. L. Vaught. The first order properties of products of algebraic systems. *Fundamenta Mathematicae*, 47:57–103, 1959.

13. J. Ferrante and C. Rackoff. *The Computational Complexity of Logical Theories*, number 718 of *Lecture Notes in Mathematics*. Springer, 1979.
14. H. Gaifman. On local and nonlocal properties. In J. Stern, editor, *Logic Colloquium '81*, pages 105–135. North Holland, 1982.
15. E. R. Green. *Graph Products of Groups*. PhD thesis, The University of Leeds, 1990.
16. B. Khoussainov and A. Nerode. Automatic presentations of structures. In *LCC: International Workshop on Logic and Computational Complexity*, number 960 in Lecture Notes in Computer Science, pages 367–392, 1994.
17. D. Kuske and M. Lohrey. Decidable theories of graphs, factorized unfoldings and cayley-graphs. Technical Report 2002/37, University of Leicester, MCS, 2002.
18. 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*.
19. 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*.
20. 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.
21. 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.
22. P. Narendran and F. Otto. Some results on equational unification. In M. E. Stickel, editor, *Proceedings of the 10th International Conference on Automated Deduction (CADE 90), Kaiserslautern (Germany)*, number 449 in Lecture Notes in Computer Science, pages 276–291. Springer, 1990.
23. D. Seese. Tree-partite graphs and the complexity of algorithms. In L. Budach, editor, *Proceedings of Fundamentals of Computation Theory (FCT'85), Cottbus (GDR)*, number 199 in Lecture Notes in Computer Science, pages 412–421, 1985.
24. D. Seese. The structure of models of decidable monadic theories of graphs. *Annals of Pure and Applied Logic*, 53:169–195, 1991.
25. G. Sénizergues. Semi-groups acting on context-free graphs. In F. M. auf der Heide and B. Monien, editors, *Proceedings of the 28th International Colloquium on Automata, Languages and Programming (ICALP 96), Paderborn (Germany)*, number 1099 in Lecture Notes in Computer Science, pages 206–218. Springer, 1996.
26. S. Shelah. The monadic theory of order. *Annals of Mathematics, II. Series*, 102:379–419, 1975.
27. J. Stupp. The lattice-model is recursive in the original model. The Hebrew University, Jerusalem, 1975.
28. W. Thomas. A short introduction to infinite automata. In W. Kuich, G. Rozenberg, and A. Salomaa, editors, *Proceedings of the 5th International Conference on Developments in Language Theory (DLT 2001), Vienna (Austria)*, number 2295 in Lecture Notes in Computer Science, pages 130–144. Springer, 2001.
29. C. Thomassen and W. Woess. Vertex-transitive graphs and accessibility. *Journal of Combinatorial Theory, Series B*, 58:248–268, 1993.
30. A. Veloso da Costa. Graph products of monoids. *Semigroup Forum*, 63(2):247–277, 2001.
31. I. Walukiewicz. Monadic second-order logic on tree-like structures. *Theoretical Computer Science*, 275(1–2):311–346, 2002.