On the theory of one-step rewriting in trace monoids *

Dietrich Kuske[1] and Markus Lohrey[2]

[1] Department of Mathematics and Computer Science
University of Leicester, LEICESTER, LE1 7RH, UK
[2] Universität Stuttgart, Institut für Informatik,
Breitwiesenstr. 20-22, 70565 Stuttgart, Germany
D.Kuske@mcs.le.ac.uk, lohrey@informatik.uni-stuttgart.de

Abstract. We prove that the first-order theory of the one-step rewriting relation associated with a trace rewriting system is decidable and give a nonelementary lower bound for the complexity. The decidability extends known results on semi-Thue systems but our proofs use new methods; these new methods yield the decidability of local properties expressed in first-order logic augmented by modulo-counting quantifiers. Using the main decidability result, we describe a class of trace rewriting systems for which the confluence problem is decidable. The complete proofs can be found in the Technical Report [14].

1 Introduction

Rewriting systems received a lot of attention in mathematics and theoretical computer science and are still an active field of research. Historically, rewriting systems were introduced to solve word problems in certain structures [28]. By the work of Markov [18] and Post [24], this hope vanished as they showed that there exist fixed semi-Thue systems with an undecidable word problem. Despite this result, there are plenty of rewriting systems with a decidable word problem, the most famous class being that of confluent and terminating systems. By Newman's Lemma, confluence can be decided for terminating semi-Thue systems as well as for terminating term rewriting systems. In general, both confluence and termination are undecidable properties of a semi-Thue system. A large deal of research tries to identify sufficient conditions for confluence/termination of rewriting systems (cf. [26]), or to describe classes of rewriting systems where confluence/termination is decidable.

These two properties which are in the heart of research in this area are typical second-order properties of the rewrite graph: its nodes are the structures that are rewritten (e.g., words in case of a semi-Thue system or terms in case of a term rewriting system), and directed edges indicate that one such structure can be rewritten into the other in one step. In order to define confluence and termination, one needs to quantify over paths in this graph. Hence the monadic second-order theory of rewrite graphs is in general undecidable. The situation changes for semi-Thue systems when one considers the first-order theory: the edges of the rewrite graph of a semi-Thue system can be

* This work was partly 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.

described by two-tape automata that move their heads synchronously on both tapes.[1] Using the well known closure properties of regular sets, the decidability of the first-order theory of these graphs follows [5, 13]. This result also holds for rewrite graphs of ground term rewriting systems [5], but not for term rewriting systems in general [29]. Another result in this direction is the decidability of the monadic second-order theory of the rewrite graph of a prefix semi-Thue system [2] (a prefix semi-Thue system is a semi-Thue system where only prefixes can be rewritten). In particular confluence and termination are decidable for prefix semi-Thue systems.

This paper investigates the first-order theory of the rewrite graph of a trace rewriting system. Cartier and Foata [1] investigated the combinatorics of free partially commutative monoids that became later known as trace monoids. Mazurkiewicz [20] introduced them into computer science. They form a mathematically sound model for the concurrent behaviour of systems of high abstraction. Since trace monoids are a generalization of free monoids, it was tempting to extend the investigation of free monoids to free partially commutative monoids. This resulted, e.g., in the extensive consideration of recognizable and rational trace languages (cf. [9] for a collection of surveys on this field), trace equations [10, 19, 8], and trace rewriting systems [6, 7, 16, 17].

Our main result states that for any finite trace rewriting system, the first-order theory of the associated rewrite graph is decidable. Because of the non-local effects of trace rewriting,[2] the automata-theoretic techniques from Dauchet and Tison [5] and Jacquemard [13] are not applicable here and we had to search for other ideas. The first is an application of Gaifman's locality theorem: the validity of a first-order sentence in a structure $\mathcal{S}$ depends on first-order properties of spheres around elements of $\mathcal{S}$. Since this theorem is effective, we were left with the question how to describe the set of traces that are centers of an r-sphere satisfying a given first-order formula. Our second idea is that the r-sphere around a trace can be described in the dependence graph of this trace by a sentence of monadic second-order logic. Note that this logic does not speak about the infinite rewrite graph, but about a single finite dependence graph. We show that this is indeed effectively possible. Hence, by a result of Thomas [27], this implies the recognizability of the set of traces that are centers of an r-sphere satisfying a given first-order formula. Taking these two ideas together, we obtain that the first-order theory of the graph of any trace rewriting system is decidable.

We actually show a more general result since we do not only consider trace rewriting systems, but scattered rewriting systems. The idea is that of a parallel rewrite step where the intermediate factors of a trace have to satisfy some recognizable constraints and can be permuted as long as they are independent in the trace monoid.

As mentioned above, the first step in our decidability proof is an application of Gaifman's Theorem. To the knowledge of the authors, all known translations of a first-order sentence into a Boolean combination of local sentences are not elementary, thus our decision procedure is far from efficient. We also show that one cannot avoid this nonelementary complexity. To this aim, we construct a trace rewrite graph whose first-order theory is not elementary. Thus, our use of Gaifman's translation does not lead to

[1] As opposed to rational graphs where the movement is asynchronous.

[2] With a and c the only independent letters, one can, e.g., rewrite $a^n bc^m$ into $c^m ba^n$ in just two steps using the rules $abc \to ac$ and $ca \to cba$.

an unreasonable inefficiency. We actually show a slightly stronger result, namely that the set of valid local sentences for a fixed radius is not elementary. In other words, the complexity of the decision question is already present when restricting to local sentences. This nonelementary lower bound is shown for a nontrivial independence alphabet and the proof does not carry over to semi-Thue systems. We show a lower bound of doubly exponential nondeterministic time for this problem. Again this lower bound holds for local sentences for a fixed radius.

In the last section, we return to the confluence problem for trace rewriting systems. For terminating rewriting systems, confluence and local confluence are equivalent. The problem with trace rewriting systems is that there can be infinitely many critical pairs which makes it impossible to check all of them in turn [6, 7]. Even worse, by [22], it is undecidable whether a length-reducing trace rewriting system is confluent. We describe classes of terminating trace rewriting systems for which confluence is decidable. The classes of trace rewriting systems we consider in this last section ensure that local confluence is effectively expressible by a sentence of first-order logic (which is not the case in general). This then allows to apply our main result on the decidability of these first-order properties and therefore the decidability of confluence for these classes when restricted to terminating systems.

2 Rewriting in trace monoids

2.1 Trace monoids and recognizable trace languages

In the following we introduce some notions from trace theory, see [9] for more details. An *independence relation* on an alphabet Σ is an irreflexive and symmetric relation $I \subseteq \Sigma \times \Sigma$, the complementary relation $D = (\Sigma \times \Sigma)\backslash I$ is called a *dependence relation*. The pair (Σ, I) (resp. (Σ, D)) is called an *independence alphabet* (resp. a *dependence alphabet*). A *dependence graph* or *trace* is a triple (V, E, λ) where (V, E) is a directed acyclic and finite graph (possibly empty) and $\lambda : V \to \Sigma$ is a labeling function such that, for all $p, q \in V$ with $p \neq q$, we have

$$(\lambda(p), \lambda(q)) \in D \text{ if and only if } (p, q) \in E \text{ or } (q, p) \in E.$$

We will identify traces that are isomorphic as labeled graphs. The set of all (isomorphism classes of) traces is denoted by $\mathbb{M} = \mathbb{M}(\Sigma, I)$. For a trace $t = (V, E, \lambda)$, let $\mathrm{alph}(t) = \lambda(V)$. The independence relation I can be lifted to $\mathbb{M}$ by setting $(u, v) \in I$ if $\mathrm{alph}(u) \times \mathrm{alph}(v) \subseteq I$. On the set $\mathbb{M}$, one defines a binary operation $\circ$ by

$$(V_1, E_1, \lambda_1) \circ (V_2, E_2, \lambda_2) = (V_1 \dot{\cup} V_2, E_1 \cup E \cup E_2, \lambda_1 \cup \lambda_2)$$

where $E = \{(p_1, p_2) \in V_1 \times V_2 \mid (\lambda(p_1), \lambda(p_2)) \in D\}$. Then $(\mathbb{M}, \circ)$ becomes a monoid, its neutral element is the empty trace 1. If $I = \emptyset$ then $\mathbb{M}$ is isomorphic to the free monoid Σ^*. On the other extreme if $D = \mathrm{Id}_\Sigma$, then $\mathbb{M}$ is isomorphic to the free commutative monoid $\mathbb{N}^{|\Sigma|}$. We will identify the letter $a \in \Sigma$ with the singleton trace whose node is labeled by a. In this sense, a word $w = a_1 a_2 \ldots a_n \in \Sigma^*$ defines the trace $[w]_I = a_1 \circ a_2 \circ \cdots \circ a_n$. We write $u \equiv_I v$ for two words u and v if $[u]_I = [v]_I$.

This relation is the congruence on the free monoid Σ^* generated by all pairs $ab \equiv_I ba$ for $(a, b) \in I$. In the following for $u, v \in \mathbb{M}$ we will also write uv instead of $u \circ v$.

Let $t = (V, E, \lambda)$ be a trace. Then the transitive reflexive closure E^* of E is a partial order. Let $U \subseteq V$ such that, for $p_1, p_2 \in U$ and $q \in V$ with $(p_1, q), (q, p_2) \in E^*$ it holds $q \in U$ (i.e., U is convex w.r.t. E^*). Then $u = t\restriction_U \in \mathbb{M}$ is a trace and, furthermore, there exist $t_1, t_2 \in \mathbb{M}$ with $t = t_1 u t_2$. Vice versa if t can be factorized as $t = t_1 u t_2$ then there exists a convex $U \subseteq V$ such that $t\restriction_U = u$.

A set $L \subseteq \mathbb{M}$ is called *recognizable* if there exists a morphism $h : \mathbb{M} \to Q$ from $(\mathbb{M}, \circ)$ into a finite monoid Q and a subset $F \subseteq Q$ such that $L = h^{-1}(F)$. The set of all recognizable subsets of $\mathbb{M}$ is denoted by $\mathrm{REC}(\mathbb{M})$. It is well-known that $\mathrm{REC}(\mathbb{M})$ is effectively closed under Boolean operations and concatenation of languages.[3] Furthermore emptiness and finiteness are decidable for recognizable trace languages, and if $L \in \mathrm{REC}(\mathbb{M})$ is finite then its elements can be calculated effectively.

2.2 Scattered trace rewriting

Let us fix a countable infinite set Ω of (first-order) variables ranging over $\mathbb{M}$ for the rest of this paper. In order to make notations more succinct, we associate with every first-order variable $x \in \Omega$ a recognizable trace language $L(x)$. We assume that for every $L \in \mathrm{REC}(\mathbb{M})$ there is a countably infinite supply of variables $x \in \Omega$ with $L(x) = L$. The mapping $x \mapsto L(x)$ will be fixed for the rest of this paper. The intuition of this mapping is that the variable $x \in \Omega$ will be restricted to its associated set $L(x)$. On the set Ω we define an independence relation J by

$$J = \{(x, y) \mid \forall t \in L(x)\, \forall u \in L(y) : (t, u) \in I\} \setminus \mathrm{Id}_\Omega.$$

Let $x_1, \ldots, x_m$ be pairwise different variables from Ω. A *pattern* S over $\mathbb{M}$ and the variables $x_1, \ldots, x_m$ is a sequence $x_{\pi(1)}\, t_1\, x_{\pi(2)}\, t_2 \cdots x_{\pi(m)}$ where $t_1, \ldots, t_{m-1} \in \mathbb{M}$ and π is a permutation of $\{1, 2, \ldots, m\}$. We define $\mathrm{type}(S) = x_{\pi(1)} x_{\pi(2)} \cdots x_{\pi(m)}$. A pattern S over the variables $x_1, \ldots, x_m$ is also denoted by $S(x_1, \ldots, x_m)$. Note that in a pattern a variable occurs precisely once, but the variables may occur in an arbitrary order. If the variable x_i evaluates to $u_i \in \mathbb{M}$, $1 \leq i \leq m$, then the trace $S(u_1, \ldots, u_m) \in \mathbb{M}$ is defined in the obvious way. A *scattered rewrite rule* over $\mathbb{M}$ and the variables $x_1, \ldots, x_m$ is a pair $(S(x_1, \ldots, x_m), T(x_1, \ldots, x_m))$ of patterns over $\mathbb{M}$ such that $\mathrm{type}(S) \equiv_J \mathrm{type}(T)$. The set of all scattered rewrite rules over $\mathbb{M}$ is denoted by $\mathbb{S}$. A *scattered rewriting system* over $\mathbb{M}$ is a finite subset of $\mathbb{S}$. For a scattered rewrite rule $\rho = (S(x_1, \ldots, x_m), T(x_1, \ldots, x_m))$ and $s, t \in \mathbb{M}$ we write $s \to_\rho t$ if there exist traces $u_i \in L(x_i)$ such that $s = S(u_1, \ldots, u_m)$ and $t = T(u_1, \ldots, u_m)$. For a scattered rewriting system $\mathcal{R}$ we write $s \to_\mathcal{R} t$ if $s \to_\rho t$ for some $\rho \in \mathcal{R}$.

An important special case of scattered rewriting systems are *trace rewriting* systems [6, 7], i.e., scattered rewriting systems whose rules are all of the form $(x\ell y, xry)$ for $x, y \in \Omega$, $\ell, r \in \mathbb{M}$ such that $L(x) = L(y) = \mathbb{M}$. If $I = \emptyset$, i.e., $\mathbb{M} \simeq \Sigma^*$, then a trace rewriting system over $\mathbb{M}$ is also called a *semi-Thue system* over Σ^*. On the other hand if $I = (\Sigma \times \Sigma) \setminus \mathrm{Id}_\Sigma$, i.e., $\mathbb{M} \simeq \mathbb{N}^{|\Sigma|}$, then a trace rewriting system over $\mathbb{M}$ is also

[3] In these effectiveness statements, a recognizable language is given as a triple (Q, F, h).

called a *vector replacement system* over $\mathbb{N}^{|\Sigma|}$. A rule $(x\ell y, xry)$ of a trace rewriting system will be briefly denoted by (ℓ, r).

In this paper we will be concerned with the first-order theory of the structure

$$\mathcal{M} = (\mathbb{M}, (L)_{L\in\mathrm{REC}(\mathbb{M})}, (\to_\rho)_{\rho\in\mathbb{S}})$$

and its reducts $\mathcal{M}_\mathcal{R} = (\mathbb{M}, (L)_{L\in\mathrm{REC}(\mathbb{M})}, (\to_\rho)_{\rho\in\mathcal{R}})$, where $\mathcal{R}$ is a scattered rewriting system. Each recognizable language $L \in \mathrm{REC}(\mathbb{M})$ is put into $\mathcal{M}$ as a unary predicate. Furthermore, $\mathcal{M}$ contains all binary relations $\to_\rho \subseteq \mathbb{M} \times \mathbb{M}$ for $\rho \in \mathbb{S}$, while $\mathcal{M}_\mathcal{R}$ contains only those relations $\to_\rho$ for $\rho \in \mathcal{R}$.

Formally, trace rewriting systems are more general than semi-Thue and vector replacement systems since they work modulo a partial commutation. Even more, there are trace rewriting systems $\mathcal{R}$ such that the graph $(\mathbb{M}, \to_\mathcal{R})$ is not isomorphic to the graph $(\Sigma^*, \to_\mathcal{S})$ for any semi-Thue system $\mathcal{S}$. To see this let us introduce some notions concerning confluence. We say that the trace rewriting system $\mathcal{R}$ is *confluent* (resp. *locally confluent*) if for all $t, t_1, t_2 \in \mathbb{M}$ with $t \xrightarrow{*}_\mathcal{R} t_1$ and $t \xrightarrow{*}_\mathcal{R} t_2$ (resp. $t \to_\mathcal{R} t_1$ and $t \to_\mathcal{R} t_2$) there exists $u \in \mathbb{M}$ with $t_1 \xrightarrow{*}_\mathcal{R} u$ and $t_2 \xrightarrow{*}_\mathcal{R} u$. These two notions are standard. The following notion seems to be new: We say that $\mathcal{R}$ is *α-confluent*, where $\alpha \in \mathbb{N}$, if for all $t, t_1, t_2 \in \mathbb{M}$ with $t \to_\mathcal{R} t_1$ and $t \to_\mathcal{R} t_2$ there exists $u \in \mathbb{M}$ with $t_1 \to_\mathcal{R}^{\leq\alpha} u$ and $t_2 \to_\mathcal{R}^{\leq\alpha} u$ (where $t_i \to^{\leq\alpha} u$ denotes that u can be obtained from t_i in at most α steps). Using critical pairs one can show that any locally confluent semi-Thue system is α-confluent for some $\alpha \in \mathbb{N}$. On contrast, the trace rewriting system $\{(ab, 1), (ba, 1), (c, 1)\}$ over the trace monoid $\mathbb{M}(\{a, b, c\}, \{(a, c), (c, a)\})$ is locally confluent [17] but not α-confluent (consider $c^n b \leftarrow bac^n b \equiv_I bc^n ab \to bc^n$ for $n > \alpha$).

2.3 The main result

The main result of this paper states that the first-order theory of any structure $\mathcal{M}$ is decidable. Since our decision procedure is uniform in the underlying alphabet, we obtain

Theorem 2.1. *There exists an algorithm that, on input of an independence alphabet (Σ, I) and a first-order sentence φ over the signature of the structure $\mathcal{M}$, decides whether $\mathcal{M} \models \varphi$.*

Note that $\mathcal{M} \models \varphi$ if and only if $\mathcal{M}_\mathcal{R} \models \varphi$ where $\mathcal{R} \subseteq \mathbb{S}$ is finite and contains the set of rewrite rules mentioned in φ. Thus, in order to prove Theorem 2.1, it suffices to prove the decidability of the first-order theory of $\mathcal{M}_\mathcal{R}$ for any scattered rewriting system $\mathcal{R}$.

An immediate corollary of Theorem 2.1 is that the rewrite graph of a trace rewriting system has a decidable first-order theory. This generalizes the corresponding result for semi-Thue systems in [5, 13], furthermore this generalization is a strict one by the observation at the end of the previous section. The basic fact used in [5, 13] is that for a semi-Thue system $\mathcal{R}$ the relation $\to_\mathcal{R}$ is a synchronized rational transduction [11]. While these methods can be generalized to work for the case that $\mathbb{M}$ is a direct product of free monoids, there seems to be no way to generalize them to arbitrary trace monoids. Hence in our proof of Theorem 2.1 we will follow a completely different and new strategy.

Let us close this section with some remarks on the limitations of our results. First, if one omits the restriction $\mathrm{type}(S) \equiv_J \mathrm{type}(T)$ for scattered rewrite rules (S, T), the theory of $\mathcal{M}$ becomes undecidable [14, Thm. 3.6]. A prefix rewriting system over $\mathbb{M}$ is a scattered rewriting system $\mathcal{R}$ where all rules have the form $(x\ell y, xry)$ with $L(x) = \{1\}$ and $L(y) = \mathbb{M}$ (we abbreviate this rule by (ℓ, r)). Based on results from [4], Caucal has shown in [2] that for a prefix rewriting system $\mathcal{R}$ over a free monoid Σ^* the monadic second-order theory of the graph $(\Sigma^*, \to_{\mathcal{R}})$ is decidable (this does not hold for semi-Thue systems). In contrast to this, let $\mathcal{R}$ be the prefix rewriting system $\{(1, a), (1, b)\}$ over the free commutative monoid $\mathbb{M}(\{a, b\}, \{(a, b), (b, a)\})$. The graph $(\mathbb{M}, \to_{\mathcal{R}})$ is a two-dimensional grid which has an undecidable monadic second-order theory. Hence, in general, the monadic second-order theory of the relation $\to_{\mathcal{R}}$ for a prefix rewriting system $\mathcal{R}$ is undecidable.

3 Decidability of scattered rewriting

In this section we will prove Theorem 2.1. It is important to note that all statements are effective although we do not state this fact explicitly in order to smoothen the formulations. Let $\mathcal{R}$ be a fixed scattered rewriting system over the trace monoid $\mathbb{M}$.

3.1 Reduction to local properties

The main tool in this section is Gaifman's locality theorem for first-order logic [12]. For two traces $s, t \in \mathbb{M}$, let $d_{\mathcal{R}}(s, t)$ denote the length of a shortest undirected path from s to t in the graph $(\mathbb{M}, \to_{\mathcal{R}})$. For $r \geq 0$ and $t \in \mathbb{M}$, the *r-sphere* around t is $S(r, t) = \{s \in \mathbb{M} \mid d_{\mathcal{R}}(s, t) \leq r\}$. The r-sphere around t is definable in $\mathcal{M}_{\mathcal{R}}$, i.e., there exists a first-order formula with two free variables expressing $d_{\mathcal{R}}(x, y) \leq r$. Now let φ be a first-order formula in the signature of $\mathcal{M}_{\mathcal{R}}$. Then the first-order formula $\varphi^{S(r,x)}$ results from φ by relativizing all quantifiers to $S(r, x)$. It can be defined inductively, in particular $(\exists y\, \phi)^{S(r,x)} \equiv \exists y\{d_{\mathcal{R}}(x, y) \leq r \wedge \phi^{S(r,x)}\}$. Now Gaifman's theorem applied to the structure $\mathcal{M}_{\mathcal{R}}$ states the following:

Theorem 3.1. *For a given first-order sentence ϕ over the signature of $\mathcal{M}_{\mathcal{R}}$ one can effectively compute a natural number r ≥ 1 and a Boolean combination $\widehat{\phi}$ of sentences of the form*

$$\exists x_1 \cdots \exists x_m \left\{ \bigwedge_{1 \leq i < j \leq m} d_{\mathcal{R}}(x_i, x_j) > 2r \ \wedge \bigwedge_{1 \leq i \leq m} \psi^{S(r,x_i)}(x_i) \right\}$$

where ψ is a first-order sentence over the signature of $\mathcal{M}_{\mathcal{R}}$ such that $\mathcal{M}_{\mathcal{R}} \models \phi$ if and only if $\mathcal{M}_{\mathcal{R}} \models \widehat{\phi}$.

In order to use Gaifman's locality theorem for decidability purposes, we will need a "useful" description of the set of all traces $t \in \mathbb{M}$ with $\mathcal{M}_{\mathcal{R}} \models \varphi^{S(r,x)}(t)$. We will show that this set is recognizable and that it is indeed a "useful" description.

3.2 Reduction to 1-spheres

The aim of this section is to show that by enlarging the set $\mathcal{R}$ it suffices to restrict to the case $r = 1$ in Theorem 3.1. The basic idea is the following: let s, t, v be traces and (S, T), (U, V) be scattered rewrite rules such that $s \to_{(S,T)} t \to_{(U,V)} v$. Then the trace t can be factorized in two ways, one according to the pattern T and one according to the pattern U. Using Levi's Lemma for traces (see e.g. [9]), one can then refine the scattered rewrite rules (S, T) and (U, V) to (S', T') and (U', V') such that $s \to_{(S',T')} t \to_{(U',V')} v$, and the two factorizations of t according to T' and to U' are actually the same. Then also (S', V') is a scattered rewrite rule and $s \to_{(S',V')} v$. Any pair of rewrite rules (S, T) and (U, V) from $\mathcal{R}$ gives rise to a finite set of refinements. Using this process of refinement inductively, one obtains

Lemma 3.2. *For $r \geq 0$, there exists a scattered rewriting system $\mathcal{R}_r$ over $\mathbb{M}$ such that $\mathcal{R} \subseteq \mathcal{R}_r$ and for all $s, t \in \mathbb{M}$ it holds $d_{\mathcal{R}}(s, t) \leq r$ if and only if $s \to_{\mathcal{R}_r} t$.*

It should be noted that if $\mathcal{R}$ is a trace rewriting system then the system $\mathcal{R}_r$ is in general not a trace rewriting systems. This was one of the reasons for generalizing trace rewriting systems to scattered rewriting systems.

3.3 Internalizing the 1-sphere

As a major tool in the further consideration we will use monadic second-order logic (MSO logic) over dependence graphs. Formulae in this logic are interpreted over dependence graphs (V, E, λ). There exist first-order variables $x, y, z, \ldots$ ranging over elements of V and second-order variables $X, Y, Z, \ldots$ ranging over subsets of V. Atomic formulae are of the form $Q_a(x)$, $x \preceq y$, and $x \in X$ where x and y are first-order variables, X is a second-order variable, and Q_a is a unary relation symbol for every $a \in \Sigma$. The interpretation of $Q_a(x)$ is $\lambda(x) = a$ whereas $x \preceq y$ is interpreted as $(x, y) \in E^*$. From atomic formulae, MSO-formulae are constructed using Boolean connectives and quantification over first-order and second-order variables.

Note that this logic is *not* an extension of first-order logic as considered so far in this paper. The reason is simply that it speaks on finite dependence graphs (V, E, λ) while the first-order logic we are interested in speaks on the infinite structure $\mathcal{M}$. Since the elements of this latter structure are traces, we will use the following terminology: formulae of the first-order logic considered so far are called *external first-order formulae* and formulae of the MSO-logic on dependence graphs are called *internal MSO-formulae*. Similarly, we will speak of *external first-order variables* that range over traces and *internal second-order variables* (resp. *internal first-order variables*) that range over subsets (resp. elements) of a dependence graph (V, E, λ).

Theorem 3.3. *Let $\varphi(x)$ be an external first-order formula. There exists an internal MSO-sentence $\mathrm{int}(\varphi)$ such that we have for all dependence graphs $s = (V, E, \lambda)$*

$$s \models \mathrm{int}(\varphi) \text{ if and only if } \mathcal{M}_{\mathcal{R}_r} \models \varphi^{S(1,x)}(s).$$

Proof (sketch). The underlying idea is as follows: suppose $s, t \in \mathbb{M}$ are traces such that $s \rightarrow_{(S,T)} t$ for some scattered rewrite rule (S, T). Then the dependence graphs $s = (V_s, E_s, \lambda_s)$ and $t = (V_t, E_t, \lambda_t)$ coincide on large parts. In order to make this more precise, let $S = x_1\, s_1\, x_2 \ldots s_{m-1}\, x_m$ and $T = x_{\pi(1)}\, t_1\, x_{\pi(2)} \ldots t_{m-1}\, x_{\pi(m)}$ where π is a permutation of $\{1, 2, \ldots m\}$. There are traces $u_1, u_2, \ldots, u_m$ such that $s = u_1 \circ s_1 \circ u_2 \circ \ldots s_{m-1} \circ u_m$ and $t = u_{\pi(1)} \circ t_1 \circ u_{\pi(2)} \circ \ldots t_{m-1} \circ u_{\pi(m)}$. Hence the trace t can be represented by a tuple $u_1, u_2, \ldots u_m$ of factors of s (i.e., convex subsets of V) and the scattered rewrite rule (S, T). It is therefore possible to replace the external quantification over neighbors of s in $\mathcal{M}_{\mathcal{R}_r}$ by a finite disjunction over all rules from $\mathcal{R}_r$ and an internal quantification over m-tuples of factors of s. For $i = 1, 2$, let t_i be a neighbor of s represented by the rule (S_i, T_i) and the tuple $(u_1^i, u_2^i, \ldots u_m^i)$. One than has to express internally that $t_1 = t_2$ as well as $t_1 \rightarrow_\rho t_2$. This is achieved using a thorough analysis of the interplay of the scattered rewrite rules, the independence relation I, and the recognizable constraints $L(x)$ on the external first order variables $x \in \Omega$. Only here the restriction that $\mathrm{type}(S) \equiv_J \mathrm{type}(T)$ for $(S, T) \in \mathbb{S}$ becomes important. The proof can be found in [14]. $\square$

Now we can prove Theorem 2.1, our main result:

Proof sketch of Theorem 2.1. By Gaifman's Theorem and Lemma 3.2, it suffices to check whether a sentence of the form

$$\exists x_1 \cdots \exists x_m \left\{ \bigwedge_{1 \le i < j \le m} d_{\mathcal{R}_r}(x_i, x_j) > 2 \;\wedge\; \bigwedge_{1 \le i \le m} \varphi^{S(1,x_i)}(x_i) \right\} \tag{1}$$

holds in $\mathcal{M}_{\mathcal{R}_r}$. By Theorem 3.3, $M_{\mathcal{R}_r} \models \varphi^{S(1,x)}(t)$ if and only if $t \models \mathrm{int}(\varphi)$. Hence the set $L = \{t \in \mathbb{M} \mid \mathcal{M}_{\mathcal{R}_r} \models \varphi^{S(1,x)}(t)\}$ is recognizable by [27]. Thus we can check whether L is infinite. If this is the case than L contains traces of arbitrary size; there are in particular infinitely many traces $t_i \in L$, $i \in \mathbb{N}$, such that $d_{\mathcal{R}_r}(t_i, t_j) > 2$ for $i < j$. Hence (1) is true. On the other hand if L is finite, then we can enumerate all elements of L and calculate their 1-spheres with respect to $\mathcal{R}_r$. In this way we can check whether there are at least m traces $t_1, \ldots, t_m \in L$ such that $d_{\mathcal{R}_r}(t_i, t_j) > 2$ for $i < j$. Hence the decidability follows. $\square$

First-order logic can be extended by modulo counting quantifiers [25]; the resulting logic is called FO+MOD. The only difference between FO+MOD and FO is that we now have a second type of quantifiers: if φ is a formula of FO+MOD, then $\exists^{(p,q)} x \varphi$ is a formula as well for $p, q \in \mathbb{N}$ and $p < q$. Then $\mathcal{M} \models \exists^{(p,q)} x \varphi$ if the number of traces $t \in \mathbb{M}$ with $\mathcal{M} \models \varphi(t)$ is finite and congruent p modulo q.

Since there is no locality theorem known for this logic,[4] our decidability proof for the first-order theory of $\mathcal{M}$ does not work for this more expressive logic; but the second step of our proof, i.e., the recognizability of the set of traces satisfying some local formula in FO extends to the logic FO+MOD. Thus, we obtain the decidability of local properties expressed in the logic FO+MOD. It seems that this result is new even for

[4] Libkin [15] and Nurmonen [23] proved locality theorems for counting logics including modulo counting, but not in the form of Theorem 3.1. We could not make them work in our situation.

semi-Thue systems and, as far as we see, cannot be shown using the automata theoretic methods from [5, 13].

Theorem 3.4. *There is an algorithm that, on input of an independence alphabet* (Σ, I)*, a natural number* $r \geq 0$*, and a sentence* φ *of* FO+MOD *in the language of the model* $\mathcal{M}$*, decides whether there exists* $t \in \mathbb{M}$ *with* $\mathcal{M} \models \varphi^{S(r,x)}(t)$.

4 Complexity issues

We prove a nonelementary lower bound for the first-order theory of $\mathcal{M}$ by reducing the first-order theory of finite labeled linear orders. In order to formulate this, we take the MSO-logic over dependence graphs from Section 3.3 but forbid the use of second-order variables. The resulting formulae are called first-order formulae over dependence graphs. For the further consideration we will use this logic only for dependence graphs t where t is in fact a word $t \in \Sigma^*$. In this case the relation symbol $\preceq$ is interpreted by the usual order on the set $\{1, \ldots, |t|\}$, and we speak of first-order formulae over words. Throughout this section, let $\Gamma = \{\alpha, \beta\}$ be an alphabet with two elements. The *first-order theory of* Γ^* is the set of all first-order sentences over words φ such that $w \models \varphi$ for all $w \in \Gamma^*$. It is known that the first-order theory of Γ^* is not elementary decidable. This lower bound was announced in [21] where it is attributed to Stockmeyer. Stockmeyer's proof can only be found in his thesis and the same holds for the sharpening by Führer while Robertson's independent proof appeared as an extended abstract, only. The only proof that has been published seems to be [3, Example 8.1].

Let $\Sigma_1 = \Gamma \times \{0, 1, 2, 3\}$. On this set, we define a dependence relation D_1 as follows: $((a, i), (b, j)) \in D_1$ if and only if $i = j$ or $i, j \leq 2$ or ($a = b$ and $\{i, j\} \subseteq \{1, 2, 3\}$). The complementary relation is denoted by I_1. Next, we will consider the (preliminary) trace rewriting system $\mathcal{R}_1$ over $\mathbb{M}(\Sigma_1, I_1)$ defined by

$$\mathcal{R}_1 = \{(a, 0) \to (a, 3)(a, 1)(a, 3),\ (a, 1) \to (a, 2) \mid a \in \Gamma\}.$$

We first reduce the first-order theory of Γ^* to the first-order theory of the structure $(\mathbb{M}(\Sigma_1, I_1), \to_{\mathcal{R}_1}, (F_t)_{t \in F})$ where $F \subseteq \mathbb{M}(\Sigma_1, I_1)$ is finite and $F_t = \mathbb{M} \circ t \circ \mathbb{M}$ is the set of all traces that contain the factor t:

Lemma 4.1. *The first-order theory of* Γ^* *can be reduced in polynomial time to the first-order theory of* $(\mathbb{M}(\Sigma_1, I_1), \to_{\mathcal{R}_1}, (F_t)_{t \in F})$ *for some finite set* $F \subseteq \mathbb{M}(\Sigma_1, I_1)$.

Proof (sketch). A trace in $\mathbb{M}$ contains only letters from $\Gamma \times \{0\}$ if and only if it does not contain any factor of the form (a, i) for $1 \leq i \leq 3$. Hence (with $\Sigma_1 \times \{1, 2, 3\} \subseteq F$) the set of words over $\Gamma \times \{0\}$ (which will be identified with the words over Γ) can be defined in $(\mathbb{M}(\Sigma_1, I_1), \to_{\mathcal{R}_1}, (F_t)_{t \in F})$. The successors of such a word w are in one-to-one correspondence with the positions in w, hence the internal quantification over positions in w gets replaced by external quantifications over neighbors of w. The label of a position can be recovered using the predicates $F_{(a,1)}$ for $a \in \Gamma$. The order between positions requires the use of predicates F_t with $t = (a, 2)(a, 3)(b, 3)$ and $t = (a, 3)(b, 3)(b, 1)$. $\square$

In order to get rid of the predicates F_t in the lemma above, one extends the alphabet Σ_1 and the trace rewriting system $\mathcal{R}_1$ in such a way that loops of characteristic lengths are attached to traces from F_t. This allows to reduce the first-order theory of Γ^* to the set of valid local sentences of the resulting structure $(\mathbb{M}(\Sigma_2, I_2), \rightarrow_{\mathcal{R}_2})$. Hence one obtains

Theorem 4.2. *There exists an independence alphabet (Σ_2, I_2) and a trace rewriting system $\mathcal{R}_2$ over $\mathbb{M}(\Sigma_2, I_2)$ such that the first-order theory of $(\mathbb{M}(\Sigma_2, I_2), \rightarrow_{\mathcal{R}_2})$ is not elementary decidable.*

For semi-Thue systems, we can only show a weaker lower bound:

Theorem 4.3. *There exists an alphabet Σ_3 and a semi-Thue system $\mathcal{R}_3$ over Σ_3^* such that any decision procedure for the first-order theory of $(\Sigma_3^*, \rightarrow_{\mathcal{R}_3})$ requires at least doubly exponential nondeterministic time.*

5 Applications to the confluence problem

In this section we present applications of Theorem 2.1 to the confluence problem for trace rewriting systems. For terminating semi-Thue systems, i.e., systems without infinite derivations, confluence is decidable by Newman's Lemma and the use of critical pairs. For trace rewriting systems, the situation becomes more complicated since even finite length-reducing trace rewriting systems can have infinitely many critical pairs [6, 7]. Generalizing a result from [22], it is shown in [17] that confluence of length-reducing trace rewriting systems is decidable if and only if $I = \emptyset$ or $I = (\Sigma \times \Sigma)\backslash \mathrm{Id}_\Sigma$, i.e., undecidable in most cases. In this section we describe specific classes of trace rewriting systems with a decidable confluence problem, see [7, 17] for related results.

First we have to introduce some notation. For $t \in \mathbb{M}$ define $\mathrm{D}(t) = \{a \in \Sigma \mid (a, t) \notin I\}$. For a subalphabet $\Gamma \subseteq \Sigma$ and a trace rewriting system $\mathcal{R}$ we define the trace rewriting system $\pi_\Gamma(\mathcal{R})$ by $\pi_\Gamma(\mathcal{R}) = \{(\pi_\Gamma(\ell), \pi_\Gamma(r)) \mid (\ell, r) \in \mathcal{R}\}$, where $\pi_\Gamma(t)$ denotes the projection of the trace t to the alphabet Γ. A *clique covering* of a dependence alphabet (Σ, D) is a sequence $(\Gamma_1, \dots, \Gamma_n)$ with $\Gamma_i \subseteq \Sigma$ such that $\Sigma = \bigcup_{i=1}^n \Gamma_i$ and $D = \bigcup_{i=1}^n \Gamma_i \times \Gamma_i$. Finally a trace rewriting system $\mathcal{R}$ is *terminating on a trace* t if there does not start an infinite $\rightarrow_\mathcal{R}$ path in t.

Theorem 5.1. *Confluence is decidable for the class of terminating trace rewriting systems $\mathcal{R}$ over $\mathbb{M}(\Sigma, I)$ satisfying the following conditions:*

(1) For all $(\ell, r) \in \mathcal{R}$ and all $a \in \Sigma$ with $(a, \ell) \in I$ it holds $ar = ra$.
(2) For all $p_0, p_1, q_0, q_1, \in \mathbb{M}\backslash\{1\}$, $r_0, r_1 \in \mathbb{M}$ with $(p_0q_0, r_0), (p_1q_1, r_1) \in \mathcal{R}$ and $(p_0, p_1), (q_0, q_1) \in I$ there exist $s_0, s_1, t_0, t_1 \in \mathbb{M}$ such that $r_i = s_it_i$, $\mathrm{D}(s_i) \subseteq \mathrm{D}(p_i)$, and $\mathrm{D}(t_i) \subseteq \mathrm{D}(q_i)$ for $i = 0, 1$.
(3) For all $p_0, p_1, q_0, q_1, r_0, r_1 \in \mathbb{M}$, $s \in \mathbb{M}\backslash\{1\}$ with $(p_0sq_0, r_0), (p_1sq_1, r_1) \in \mathcal{R}$ and $(p_0, p_1), (q_0, q_1) \in I$, the trace rewriting system $\pi_\Gamma(\mathcal{R})$ is terminating on the traces $\pi_\Gamma(p_1r_0q_1)$ and $\pi_\Gamma(p_0r_1q_0)$, where $\Gamma = \mathrm{D}(p_0sq_1) \cap \mathrm{D}(p_1sq_0)$.

Proof (sketch). One shows that in this case $\alpha \in \mathbb{N}$ can be computed effectively such that confluence and α-confluence (see Section 2.3) are equivalent. Since α-confluence is first-order expressible, it is decidable by Theorem 2.1. ◻

From this very technical decidability criterion, one can infer [16, Thm. 2] and the following new special case:

Corollary 5.2. *Confluence is decidable for the class of trace rewriting systems $\mathcal{R}$ over $\mathbb{M}(\Sigma, I)$ such that*

(1) for all $(\ell, r) \in \mathcal{R}$, the graph $(\mathrm{alph}(\ell), D)$ is connected, and
(2) there exists a clique covering $(\Gamma_1, \ldots, \Gamma_n)$ of $(\Sigma, (\Sigma \times \Sigma)\backslash I)$ such that for all $i \in \{1, \ldots, n\}$ the semi-Thue system $\pi_i(\mathcal{R})$ is terminating.

6 Open questions

In Section 4, we gave a lower bound for the complexity of the first-order theory of the one-step rewriting by a semi-Thue system. There is a huge gap between this doubly exponential lower and the nonelementary upper bound that follows immediately from the proofs in [5, 13].

Although our decidability result is very similar to corresponding results in [5, 13], our technique is new. It could provide a means to identify term rewriting systems whose rewrite graph has a decidable first-order theory. Several classes of term rewriting systems with this property have been identified, like for instance ground term rewriting systems [5], but in general the problem is undecidable [29].

Semi-Thue systems can be seen as term rewriting systems modulo associativity (it is a very simple case since there are no further symbols). Similarly, trace rewriting is term rewriting modulo associativity and partial commutativity. Is it possible to use the technique developed in this paper to handle other "term rewriting modulo ..." theories?

References

1. P. Cartier and D. Foata. *Problèmes combinatoires de commutation et réarrangements*. Lecture Notes in Mathematics vol. 85. Springer, Berlin - Heidelberg - New York, 1969.
2. D. Caucal. On the regular structure of prefix rewriting. *Theoretical Computer Science*, 106:61–86, 1992.
3. K. Compton and C. Henson. A uniform method for proving lower bounds on the computational complexity of logical theories. *Annals of Pure and Applied Logic*, 48:1–79, 1990.
4. B. Courcelle. The monadic second-order logic of graphs, II: Infinite graphs of bounded width. *Mathematical Systems Theory*, 21:187–221, 1989.
5. M. Dauchet and S. Tison. The theory of ground rewrite systems is decidable. In *Proceedings of the 5th Annual IEEE Symposium on Logic in Computer Science (LICS '90)*, pages 242–256. IEEE Computer Society Press, 1990.
6. V. Diekert. On the Knuth-Bendix completion for concurrent processes. In Th. Ottmann, editor, *Proceedings of the14th International Colloquium on Automata, Languages and Programming (ICALP 87), Karlsruhe (Germany)*, number 267 in Lecture Notes in Computer Science, pages 42–53. Springer, 1987.
7. V. Diekert. *Combinatorics on Traces*. Number 454 in Lecture Notes in Computer Science. Springer, 1990.
8. V. Diekert, Y. Matiyasevich, and A. Muscholl. Solving word equations modulo partial commutations. *Theoretical Computer Science*, 224(1–2):215–235, 1999.

9. V. Diekert and G. Rozenberg, editors. *The Book of Traces*. World Scientific, Singapore, 1995.
10. C. Duboc. On some equations in free partially commutative monoids. *Theoretical Computer Science*, 46:159–174, 1986.
11. C. Frougny and J. Sakarovitch. Synchronized rational relations of finite and infinite words. *Theoretical Computer Science*, 108(1):45–82, 1993.
12. H. Gaifman. On local and nonlocal properties. In J. Stern, editor, *Logic Colloquium '81*, pages 105-135, 1982, North Holland.
13. F. Jacquemard. *Automates d'arbres et Réécriture de termes*. PhD thesis, Université de Paris-Sud, 1996.
14. D. Kuske and M. Lohrey. On the theory of one-step rewriting in trace monoids. Technical Report 2002-01, Department of Mathematics and Computer Science, University of Leicester. Available at `www.mcs.le.ac.uk/~dkuske/pub-rest.html#UNP9`.
15. L. Libkin. Logics capturing local properties. *ACM Transactions on Computational Logic*. To appear.
16. M. Lohrey. On the confluence of trace rewriting systems. In V. Arvind and R. Ramanujam, editors, *Proceedings of the 18th Conference on Foundations of Software Technology and Theoretical Computer Science, (FSTTCS'98), Chennai (India)*, number 1530 in Lecture Notes in Computer Science, pages 319–330. Springer, 1998.
17. M. Lohrey. Confluence problems for trace rewriting systems. *Information and Computation*. 170:1–25, 2001.
18. A. Markov. On the impossibility of certain algorithms in the theory of associative systems. *Doklady Akademii Nauk SSSR*, 55, 58:587–590, 353–356, 1947.
19. Y. Matiyasevich. Some decision problems for traces. In S. Adian and A. Nerode, editors, *Proceedings of the 4th International Symposium on Logical Foundations of Computer Science (LFCS'97), Yaroslavl (Russia)*, number 1234 in Lecture Notes in Computer Science, pages 248–257. Springer, 1997.
20. A. Mazurkiewicz. Concurrent program schemes and their interpretation. Technical report, DAIMI Report PB-78, Aarhus University, 1977.
21. A. Meyer. Weak monadic second order theory of one successor is not elementary recursive. In *Proc. Logic Colloquium*, Lecture Notes in Mathematics vol. 453, pages 132–154. Springer, 1975.
22. 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.
23. J. Nurmonen. Counting modulo quantifiers on finite structures. *Information and Computation*, 160:62–87, 2000. LICS 1996, Part I (New Brunswick, NJ).
24. E. Post. Recursive unsolvability of a problem of Thue. *Journal of Symbolic Logic*, 12(1):1–11, 1947.
25. H. Straubing, D. Thérien, and W. Thomas. Regular languages defined with generalized quantifiers. *Information and Computation*, 118:289–301, 1995.
26. Terese. Term Rewriting Systems. To appear with Cambridge University Press, 2001.
27. W. Thomas. On logical definability of trace languages. In V. Diekert, editor, *Proceedings of a workshop of the ESPRIT Basic Research Action No 3166: Algebraic and Syntactic Methods in Computer Science (ASMICS), Kochel am See (Germany)*, Report TUM-I9002, Technical University of Munich, pages 172–182, 1990.
28. A. Thue. Probleme über die Veränderungen von Zeichenreihen nach gegebenen Regeln. *Skr. Vid. Kristiania, I Math. Natuv. Klasse*, No. 10, 34 S., 1914.
29. R. Treinen. The first-order theory of linear one-step rewriting is undecidable. *Theoretical Computer Science*, 208(1-2):149–177, 1998.