The FO^2 alternation hierarchy is decidable

Manfred Kufleitner*
University of Stuttgart, Germany
kufleitner@fmi.uni-stuttgart.de

Pascal Weil†
CNRS, LaBRI, UMR5800, F-33400 Talence, France
Univ. Bordeaux, LaBRI, UMR5800, F-33400 Talence, France
pascal.weil@labri.fr

Abstract

We consider the two-variable fragment $\mathrm{FO}^2[<]$ of first-order logic over finite words. Numerous characterizations of this class are known. Thérien and Wilke have shown that it is decidable whether a given regular language is definable in $\mathrm{FO}^2[<]$. From a practical point of view, as shown by Weis, $\mathrm{FO}^2[<]$ is interesting since its satisfiability problem is in NP. Restricting the number of quantifier alternations yields an infinite hierarchy inside the class of $\mathrm{FO}^2[<]$-definable languages. We show that each level of this hierarchy is decidable. For this purpose, we relate each level of the hierarchy with a decidable variety of finite monoids.

Our result implies that there are many different ways of climbing up the $\mathrm{FO}^2[<]$-quantifier alternation hierarchy: deterministic and co-deterministic products, Mal'cev products with definite and reverse definite semigroups, iterated block products with $\mathcal{J}$-trivial monoids, and some inductively defined omega-term identities. A combinatorial tool in the process of ascension is that of condensed rankers, a refinement of the rankers of Weis and Immerman and the turtle programs of Schwentick, Thérien, and Vollmer.

*The first author was supported by the German Research Foundation (DFG) under grant DI 435/5-1.

†The second author was supported by the grant ANR 2010 BLAN 0202 01 FREC.

1 Introduction

The investigation of logical fragments has a long history. McNaughton and Papert [16] showed that a language over finite words is definable in first-order logic FO[$<$] if and only if it is star-free. Combined with Schützenberger's characterization of star-free languages in terms of finite aperiodic monoids [22], this leads to an algorithm to decide whether a given regular language is first-order definable. Many other characterizations of this class have been given over the past 50 years, see [3] for an overview. Moreover, mainly due to its relation to linear temporal logic [7], it became relevant to a large number of application fields, such as verification.

Very often one is interested in fragments of first-order logic. From a practical point of view, the reason is that smaller fragments often yield more efficient algorithms for computational problems such as satisfiability. For example, satisfiability for FO[$<$] is non-elementary [25], whereas the satisfiability problem for first-order logic with only two variables is in NP, cf. [38]. And on the theoretical side, fragments form the basis of a descriptive complexity theory inside the regular languages: the simpler a logical formula defining a language, the easier the language. Moreover, in contrast to classical complexity theory, in some cases one can actually decide whether a given language has a particular property. From both the practical and the theoretical point of view, several natural hierarchies have been considered in the literature: the quantifier alternation hierarchy inside FO[$<$] which coincides with the Straubing-Thérien hierarchy [26, 31], the quantifier alternation hierarchy inside FO[$<, +1$] with a successor predicate $+1$ which coincides with the dot-depth hierarchy [2, 35], the until hierarchy of temporal logic [33], and the until-since hierarchy [34]. Decidability is known for the levels of the until and the the until-since hierarchies, and only for the very first levels of the alternation hierarchies, see e.g. [4, 20].

Fragments are usually defined by restricting resources in a formula. Such resources can be the predicates which are allowed, the quantifier depth, the number of quantifier alternations, or the number of variables. When the quantifier depth is restricted, only finitely many languages are definable over a fixed alphabet: decidability of the membership problem is not an issue in this case. When restricting the number of variables which can be used (and reused), then first-order logic $\mathrm{FO}^3[<]$ with three variables already has the full expressive power of FO[$<$], see [6, 7]. On the other hand, first-order logic $\mathrm{FO}^2[<]$ with only two variables defines a proper subclass. The languages definable in $\mathrm{FO}^2[<]$ have a huge number of different characterizations, see e.g. [4, 29, 30]. For example, $\mathrm{FO}^2[<]$ has the same expressive power as $\Delta_2[<]$;

the latter is a fragment of FO[<] with two blocks of quantifiers [32].

Turtle programs are one of these numerous descriptions of $\mathrm{FO}^2[<]$-definable languages [23]. They are sequences of instructions of the form "go to the next a-position" and "go to the previous a-position". Using the term *ranker* for this concept and having a stronger focus on the order of positions defined by such sequences, Weis and Immerman [39] were able to give a combinatorial characterization of the alternation hierarchy $\mathrm{FO}^2_m[<]$ inside $\mathrm{FO}^2[<]$. Straubing [27] gave an algebraic characterization of $\mathrm{FO}^2_m[<]$. But neither result yields the decidability of $\mathrm{FO}^2_m[<]$-definability for $m > 2$. In some sense, this is the opposite of a previous result of the authors [14, Thm. 6.1], who give necessary and sufficient conditions which helped to decide the $\mathrm{FO}^2_m[<]$-hierarchy with an error of at most one. In this paper we give a new algebraic characterization of $\mathrm{FO}^2_m[<]$, and this characterization immediately yields decidability.

The algebraic approach to the membership problem of logical fragments has several advantages. In favorable cases, it opens the road to decidability procedures. Moreover, it allows a more *semantic* comparison of fragments; for example, the equality $\mathrm{FO}^2[<] = \Delta_2[<]$ was obtained by showing that both $\mathrm{FO}^2[<]$ and $\Delta_2[<]$ correspond to the same variety of finite monoids, namely **DA** [21, 32].

Building on previous detailed knowledge of the lattice of *band* varieties (varieties of idempotent monoids), Trotter and Weil defined a sub-lattice of the lattice of subvarieties of **DA** [36], which we call the $\mathbf{R}_m$-Łm-hierarchy. These varieties have many interesting properties and in particular, each $\mathbf{R}_m$ (resp. Łm) is efficiently decidable (by a combination of results of Trotter and Weil [36], Kufleitner and Weil [10], and Straubing and Weil [28], see Section 3 for more details). Moreover, one can climb up the $\mathbf{R}_m$-Łm-hierarchy algebraically, using Mal'cev products, see [10] and Section 2 below; language-theoretically, in terms of alternated closures under deterministic and co-deterministic products [18, 14]; and combinatorially using *condensed* rankers, see [13, 15] and Section 2.

We relate the $\mathrm{FO}^2[<]$ quantifier alternation hierarchy with the $\mathbf{R}_m$-Łm-hierarchy. More precisely, the main result of this paper is that a language is definable in $\mathrm{FO}^2_m[<]$ if and only if it is recognized by a monoid in $\mathbf{R}_{m+1} \cap$ Ł$m + 1$, thus establishing the decidability of each $\mathrm{FO}^2_m[<]$. This result was first conjectured in [13], where one inclusion was established. Our proof combines a technique introduced by Klíma [8] and a substitution idea [11] with algebraic and combinatorial tools inspired by [14]. The proof is by induction and the base case is Simon's Theorem on piecewise testable languages [24].

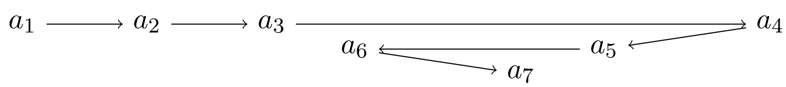

Figure 1: The positions defined by r in u, when $r = \mathsf{X}_{a_1}\mathsf{X}_{a_2}\mathsf{X}_{a_3}\mathsf{X}_{a_4}\mathsf{Y}_{a_5}\mathsf{Y}_{a_6}\mathsf{X}_{a_7}$ is condensed on u

2 Preliminaries

Let A be a finite alphabet and let A^* be the set of all finite words over A. The *length* $|u|$ of a word $u = a_1 \cdots a_n$, $a_i \in A$, is n and its *alphabet* is $\mathsf{alph}(u) = \{a_1, \ldots, a_n\} \subseteq A$. A position i of $u = a_1 \cdots a_n$ is an *a-position* if $a_i = a$. A factorization $u = u_- a u_+$ is the *a-left factorization* of u if $a \notin \mathsf{alph}(u_-)$, and it is the *$a$-right factorization* if $a \notin \mathsf{alph}(u_+)$, i.e., we factor at the first or at the last a-position.

2.1 Rankers

A *ranker* is a nonempty word over the alphabet $\{\mathsf{X}_a, \mathsf{Y}_a \mid a \in A\}$. It is interpreted as a sequence of instructions of the form "go to the next a-position" and "go to the previous a-position". More formally, for $u = a_1 \cdots a_n \in A^*$ and $x \in \{0, \ldots, n+1\}$ we let

$$\mathsf{X}_a(u,x) = \min\{y \mid y > x \text{ and } a_y = a\}, \qquad \mathsf{X}_a(u) = \mathsf{X}_a(u,0),$$
$$\mathsf{Y}_a(u,x) = \max\{y \mid y < x \text{ and } a_y = a\}, \qquad \mathsf{Y}_a(u) = \mathsf{Y}_a(u,n+1).$$

Here, both the minimum and the maximum of the empty set are undefined. The modality X_a is for "neXt-a" and Y_a is for "Yesterday-a". For $r = \mathsf{Z}\,s$, $\mathsf{Z} \in \{\mathsf{X}_a, \mathsf{Y}_a \mid a \in A\}$, we set

$$r(u,x) = s(u, \mathsf{Z}(u,x)), \qquad r(u) = s(u, \mathsf{Z}(u)).$$

In particular, rankers are executed (as a set of instructions) from left to right. Every ranker r either defines a unique position in a word u, or it is undefined on u. For example, $\mathsf{X}_a\,\mathsf{Y}_b\,\mathsf{X}_c(bca) = 2$ and $\mathsf{X}_a\,\mathsf{Y}_b\,\mathsf{X}_c(bac) = 3$ whereas $\mathsf{X}_a\,\mathsf{Y}_b\,\mathsf{X}_c(cabc)$ and $\mathsf{X}_a\,\mathsf{Y}_b\,\mathsf{X}_c(bcba)$ are undefined. A ranker r is *condensed* on u if it is defined and, during the execution of r, no previously visited position is overrun [14]. One can think of condensed rankers as *zooming in* on the position they define, see Figure 1. More formally $r = \mathsf{Z}_1 \cdots \mathsf{Z}_k$, $\mathsf{Z}_i \in \{\mathsf{X}_a, \mathsf{Y}_a \mid a \in A\}$, is *condensed* on u if there exists a chain of open intervals

$$(0; |u|+1) = (x_0; y_0) \supset (x_1; y_1) \supset \cdots \supset (x_{n-1}; y_{n-1}) \ni r(u)$$

such that for all $1 \leq \ell \leq n-1$ the following properties are satisfied:

- If $\mathsf{Z}_\ell \, \mathsf{Z}_{\ell+1} = \mathsf{X}_a \, \mathsf{X}_b$, then $(x_\ell; y_\ell) = (\mathsf{X}_a(u, x_{\ell-1}); y_{\ell-1})$.
- If $\mathsf{Z}_\ell \, \mathsf{Z}_{\ell+1} = \mathsf{Y}_a \, \mathsf{Y}_b$, then $(x_\ell; y_\ell) = (x_{\ell-1}; \mathsf{Y}_a(u, y_{\ell-1}))$.
- If $\mathsf{Z}_\ell \, \mathsf{Z}_{\ell+1} = \mathsf{X}_a \, \mathsf{Y}_b$, then $(x_\ell; y_\ell) = (x_{\ell-1}; \mathsf{X}_a(u, x_{\ell-1}))$.
- If $\mathsf{Z}_\ell \, \mathsf{Z}_{\ell+1} = \mathsf{Y}_a \, \mathsf{X}_b$, then $(x_\ell; y_\ell) = (\mathsf{Y}_a(u, y_{\ell-1}); y_{\ell-1})$.

For example, $\mathsf{X}_a \, \mathsf{Y}_b \, \mathsf{X}_c$ is condensed on bca but not on bac.

The *depth* of a ranker is its length as a word. A *block* of a ranker is a maximal factor of the form $\mathsf{X}_{a_1} \cdots \mathsf{X}_{a_k}$ or of the form $\mathsf{Y}_{b_1} \cdots \mathsf{Y}_{b_\ell}$. A ranker with m blocks changes direction $m-1$ times. By $R_{m,n}$ we denote the class of all rankers with depth at most n and with up to m blocks. We write $R^{\mathsf{X}}_{m,n}$ for the set of all rankers in $R_{m,n}$ which start with an X_a-modality and we write $R^{\mathsf{Y}}_{m,n}$ for all rankers in $R_{m,n}$ which start with a Y_a-modality.

We define $u \rhd_{m,n} v$ if the same rankers in $R^{\mathsf{X}}_{m,n} \cup R^{\mathsf{Y}}_{m-1,n-1}$ are condensed on u and v. Similarly, $u \lhd_{m,n} v$ if the same rankers in $R^{\mathsf{Y}}_{m,n} \cup R^{\mathsf{X}}_{m-1,n-1}$ are condensed on u and v. The relations $\rhd_{m,n}$ and $\lhd_{m,n}$ are finite index congruences [14, Lem. 3.13].

The *order type* $\operatorname{ord}(i,j)$ is one of $\{<,=,>\}$, depending on whether $i<j$, $i=j$, or $i>j$, respectively. We define $u \equiv_{m,n} v$ if

- the same rankers in $R_{m,n}$ are defined on u and v,
- for all $r \in R^{\mathsf{X}}_{m,n}$ and $s \in R^{\mathsf{Y}}_{m,n-1}$: $\operatorname{ord}(r(u), s(u)) = \operatorname{ord}(r(v), s(v))$,
- for all $r \in R^{\mathsf{Y}}_{m,n}$ and $s \in R^{\mathsf{X}}_{m,n-1}$: $\operatorname{ord}(r(u), s(u)) = \operatorname{ord}(r(v), s(v))$,
- for all $r \in R^{\mathsf{X}}_{m,n}$ and $s \in R^{\mathsf{X}}_{m-1,n-1}$: $\operatorname{ord}(r(u), s(u)) = \operatorname{ord}(r(v), s(v))$,
- for all $r \in R^{\mathsf{Y}}_{m,n}$ and $s \in R^{\mathsf{Y}}_{m-1,n-1}$: $\operatorname{ord}(r(u), s(u)) = \operatorname{ord}(r(v), s(v))$.

Remark 1. For $m=1$, each of the families $(\equiv_{1,n})_n$, $(\rhd_{1,n})_n$, and $(\lhd_{1,n})_n$ defines the class of piecewise testable languages, see e.g. [8, 24]. Recall that a language $L \subseteq A^*$ is *piecewise testable* if it is a Boolean combination of languages of the form $A^* a_1 A^* \cdots a_k A^*$ ($k \geq 0$, $a_1, \ldots, a_k \in A$).

2.2 First-order Logic

We denote by FO[<] the first-order logic over words interpreted as labeled linear orders. The atomic formulas are $\top$ (for *true*), $\perp$ (for *false*), the unary predicates $\mathbf{a}(x)$ (one for each $a \in A$), and the binary predicate $x<y$ for variables x and y. Variables range over the linearly ordered positions of a word and $\mathbf{a}(x)$ means that x is an a-position. Apart from the Boolean connectives, we allow composition of formulas using existential quantification $\exists x \colon \varphi$ and universal quantification $\forall x \colon \varphi$ for $\varphi \in \mathrm{FO}[<]$. The semantics is as usual. A *sentence* in FO[<] is a formula without free variables. For a sentence φ the *language defined by* φ, denoted by $L(\varphi)$, is the set of all words $u \in A^*$ which model φ.

The fragment $\mathrm{FO}^2[<]$ of first-order logic consists of all formulas which use at most two different names for the variables. This is a natural restriction, since FO with three variables already has the full expressive power of FO. A formula $\varphi \in \mathrm{FO}^2[<]$ is in $\mathrm{FO}^2_m[<]$ if, on every path of its parse tree, φ has at most m blocks of alternating quantifiers.

Note that $\mathrm{FO}^2_1[<]$-definable languages are exactly the piecewise testable languages, cf. [27]. For $m \geq 2$, we rely on the following important result, due to Weis and Immerman [39, Thm. 4.5].

Theorem 2. *A language L is definable in $\mathrm{FO}^2_m[<]$ if and only if there exists $n \in \mathbb{N}$ such that L is a union of $\equiv_{m,n}$-classes.*

Remark 3. The definition of $\equiv_{m,n}$ above is formally different from the conditions in Weis and Immerman's [39, Thm. 4.5]. A careful but elementary examination reveals that they are actually equivalent.

2.3 Algebra

A monoid M *recognizes* a language $L \subseteq A^*$ if there exists a morphism $\varphi : A^* \to M$ such that $L = \varphi^{-1}\varphi(L)$. If $\varphi : A^* \to M$ is a morphism, then we set $u \equiv_\varphi v$ if $\varphi(u) = \varphi(v)$. The join $\equiv_1 \vee \equiv_2$ of two congruences $\equiv_1$ and $\equiv_2$ is the least congruence containing $\equiv_1$ and $\equiv_2$. An element u is *idempotent* if $u^2 = u$. The set of all idempotents of a monoid M is denoted by $E(M)$. For every finite monoid M there exists $\omega \in \mathbb{N}$ such that u^ω is idempotent for all $u \in M$. *Green's relations* $\mathcal{J}$, $\mathcal{R}$, and $\mathcal{L}$ are an important concept to describe the structural properties of a monoid M: we set $u \leq_{\mathcal{J}} v$ (resp. $u \leq_{\mathcal{R}} v$, $u \leq_{\mathcal{L}} v$) if $u = pvq$ (resp. $u = vq$, $u = pv$) for some $p, q \in M$. We also define $u \mathrel{\mathcal{J}} v$ (resp. $u \mathrel{\mathcal{R}} v$, $u \mathrel{\mathcal{L}} v$) if $u \leq_{\mathcal{J}} v$ and $v \leq_{\mathcal{J}} u$ (resp. $u \leq_{\mathcal{R}} v$ and $v \leq_{\mathcal{R}} u$, $u \leq_{\mathcal{L}} v$ and $v \leq_{\mathcal{L}} u$). A monoid M is *$\mathcal{J}$-trivial* (resp. *$\mathcal{R}$-trivial*, *$\mathcal{L}$-trivial*) if $\mathcal{J}$ (resp. $\mathcal{R}$, $\mathcal{L}$) is the identity relation on M. We define the relations $\sim_{\mathbf{K}}$, $\sim_{\mathbf{D}}$, and $\sim_{\mathbf{LI}}$ on M as follows:

- $u \sim_{\mathbf{K}} v$ if and only if, for all $e \in E(M)$, we have either $eu, ev <_{\mathcal{J}} e$, or $eu = ev$.
- $u \sim_{\mathbf{D}} v$ if and only if, for all $f \in E(M)$, we have either $uf, vf <_{\mathcal{J}} f$, or $uf = vf$.
- $u \sim_{\mathbf{LI}} v$ if and only if, for all $e, f \in E(M)$ such that $e \mathrel{\mathcal{J}} f$, we have either $euf, evf <_{\mathcal{J}} e$, or $euf = evf$.

The relations $\sim_{\mathbf{K}}$, $\sim_{\mathbf{D}}$ and $\sim_{\mathbf{LI}}$ are congruences [9]. If $\mathbf{V}$ is a class of finite monoids, we say that a monoid M is in $\mathbf{K} \mathbin{ⓜ} \mathbf{V}$ (resp. $\mathbf{D} \mathbin{ⓜ} \mathbf{V}$, $\mathbf{LI} \mathbin{ⓜ} \mathbf{V}$) if

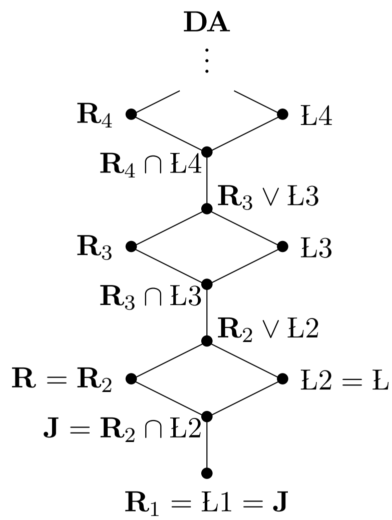

Figure 2: The $\mathbf{R}_m$-Łm-hierarchy

$M/{\sim_{\mathbf{K}}} \in \mathbf{V}$ (resp. $M/{\sim_{\mathbf{D}}} \in \mathbf{V}$, $M/{\sim_{\mathbf{LI}}} \in \mathbf{V}$). The classes $\mathbf{K} \mathbin{\textcircled{m}} \mathbf{V}$, $\mathbf{D} \mathbin{\textcircled{m}} \mathbf{V}$ and $\mathbf{LI} \mathbin{\textcircled{m}} \mathbf{V}$ are called *Mal'cev products* and they are usually defined in terms of relational morphisms. In the present context however, the definition above will be sufficient [9], see [5]. We will need the following classes of finite monoids:

- $\mathbf{J}_1$ consists of all finite commutative monoids satisfying $x^2 = x$.
- $\mathbf{J}$ (resp. $\mathbf{R}$, Ł) consists of all finite $\mathcal{J}$-trivial (resp. $\mathcal{R}$-trivial, $\mathcal{L}$-trivial) monoids.
- $\mathbf{A}$ consists of all finite monoids satisfying $x^{\omega+1} = x^{\omega}$. Monoids in $\mathbf{A}$ are called *aperiodic*.
- $\mathbf{DA}$ consists of all finite monoids satisfying $(xy)^{\omega}x(xy)^{\omega} = (xy)^{\omega}$.
- $\mathbf{R}_1 = \text{Ł}1 = \mathbf{J}$, $\mathbf{R}_{m+1} = \mathbf{K} \mathbin{\textcircled{m}} \text{Ł}m$, $\text{Ł}m+1 = \mathbf{D} \mathbin{\textcircled{m}} \mathbf{R}_m$.

It is well known that

$$\mathbf{DA} = \mathbf{LI} \mathbin{\textcircled{m}} \mathbf{J}_1,\ \mathbf{R}_2 = \mathbf{R},\ \text{Ł}2 = \text{Ł},\ \mathbf{R} \cap \text{Ł} = \mathbf{J}, \text{and}$$
$$\mathbf{R}_m \cup \text{Ł}m \ \subseteq\ \mathbf{R}_{m+1} \cap \text{Ł}m+1 \ \subset\ \mathbf{DA} \ \subset\ \mathbf{A}$$

see e.g. [19]. The $\mathbf{R}_m$-Łm-hierarchy is depicted in Figure 2.

2.4 The variety approach to the decidability of $\mathrm{FO}^2_m[<]$

Classes of finite monoids that are closed under taking submonoids, homomorphic images and finite direct products are called *pseudovarieties*. The classes of finite monoids $\mathbf{J}_1$, $\mathbf{J}$, $\mathbf{A}$, $\mathbf{DA}$, $\mathbf{R}_m$ and $\text{Ł}m$ introduced above are all pseudovarieties.

If $\mathbf{V}$ is a pseudovariety of monoids, the class $\mathcal{V}$ of languages recognized by a monoid in $\mathbf{V}$ is called a *variety of languages*. Eilenberg's variety theorem (see *e.g.* [17, Annex B]) shows that varieties of languages are characterized by natural closure properties, and that the correspondence $\mathbf{V} \mapsto \mathcal{V}$ is onto. Elementary automata theory shows in addition that a language L is recognized by a monoid in a pseudovariety $\mathbf{V}$ if and only the syntactic monoid of L is in $\mathbf{V}$. It follows that if $\mathbf{V}$ has a decidable membership problem, then so does the corresponding variety of languages $\mathcal{V}$.

Simon's Theorem on piecewise testable languages [8, 24] is an important instance of this Eilenberg correspondence: a language L is recognizable by a monoid in $\mathbf{J}$ if and only if L is piecewise testable (and hence, as we already observed, if and only if L is definable in $\mathrm{FO}^2_1[<]$). Simon's result implies the decidability of piecewise testability.

It immediately follows from the definition that membership in $\mathbf{R}_m$ and $\text{Ł}m$ is decidable for all m since membership in $\mathbf{J}$ is decidable (see Corollary 10 for a more precise statement). Many additional properties of the pseudovarieties $\mathbf{R}_m$ and $\text{Ł}m$, and of the corresponding varieties of languages were established by the authors [10, 14, 36]. We will use in particular the following results, respectively [14, Cor. 3.15] and [10, Thms. 2.1 and 3.5].

Proposition 4. *An A-generated monoid M is in $\mathbf{R}_m$ (resp. $\text{Ł}m$) if and only if there exists an integer n such that M is a quotient of $A^*/\rhd_{m,n}$ (resp. $A^*/\lhd_{m,n}$).*

Let $x_1, x_2, \ldots$ be a sequence of variables. For each word u, we denote by $\bar{u}$ the mirror image of u, that is, the word obtained by reading u from right to left. Let $G_2 = x_2x_1$, $I_2 = x_2x_1x_2$ and, for $m \geq 2$, $G_{m+1} = x_{m+1}\overline{G_m}$ and $I_{m+1} = G_{m+1}x_{m+1}\overline{I_m}$. Finally, let φ be the substitution given by

$$\begin{aligned}
&\varphi(x_1) = (x_1^\omega x_2^\omega x_1^\omega)^\omega, \quad \varphi(x_2) = x_2^\omega, \\
&\text{and, for } m \geq 2, \quad \varphi(x_{m+1}) = (x_{m+1}^\omega \varphi(G_m\overline{G_m})^\omega x_{m+1}^\omega)^\omega.
\end{aligned}$$

Proposition 5. $\mathbf{R}_m$ *(resp. $\text{Ł}m$) is the class of finite monoids satisfying $(xy)^\omega x(xy)^\omega = (xy)^\omega$ and $\varphi(G_m) = \varphi(I_m)$ (resp. $\varphi(\overline{G_m}) = \varphi(\overline{I_m})$).*

Straubing [27] and Kufleitner and Lauser [12, Cor. 3.4] established, by different means, that for each $m \geq 1$, the class of $\mathrm{FO}^2_m[<]$-definable languages forms a variety of languages, and we denote by $\mathbf{FO}^2_m$ the corresponding pseudovariety. In particular, $\mathbf{FO}^2_1 = \mathbf{J}$. Our strategy to establish the decidability of $\mathrm{FO}^2_m[<]$-definability, is to establish the decidability of membership in $\mathbf{FO}^2_m$.

It is to be noted that neither Straubing's result, nor Kufleitner's and Lauser's result implies the decidability of $\mathbf{FO}^2_m$. Straubing's result is the following [27, Thm. 4].

Theorem 6. *For $m \geq 1$, $\mathbf{FO}^2_{m+1} = \mathbf{FO}^2_m ** \mathbf{J}$, where $**$ denotes the two-sided wreath product.*

We refer the reader to [27] for the definition of the two-sided wreath product, which is also called the block product in the literature. As discussed by Straubing, this exact algebraic characterization of $\mathbf{FO}^2_m$ implies the decidability of $\mathbf{FO}^2_2$ but not of the other levels of the hierarchy. Straubing however conjectured that the following holds [27, Conj. 10].

Conjecture 7 (Straubing)**.** *Let $u_1 = (x_1x_2)^\omega$, $v_1 = (x_2x_1)^\omega$ and, for $m \geq 1$,*

$$u_{m+1} = (x_1 \cdots x_{2n}x_{2n+1})^\omega u_n (x_{2n+2}x_1 \cdots x_{2n})^\omega$$
$$v_{m+1} = (x_1 \cdots x_{2n}x_{2n+1})^\omega v_n (x_{2n+2}x_1 \cdots x_{2n})^\omega.$$

Then a monoid is in $\mathbf{FO}^2_m$ if and only if it satisfies $x^{\omega+1} = x^\omega$ and $u_m = v_m$.

If established, this conjecture would prove the decidability of each $\mathbf{FO}^2_m$. The authors on the other hand proved the following [14, Thm. 5.1].

Theorem 8. *If a language L is recognized by a monoid in the join $\mathbf{R}_m \vee \text{Ł}m$, then L is definable in $\mathrm{FO}^2_m[<]$; and if L is definable in $\mathrm{FO}^2_m[<]$, then L is recognized by a monoid in $\mathbf{R}_{m+1} \cap \text{Ł}m + 1$.*

3 The FO^2 alternation hierarchy is decidable

We tighten the connection between the alternation hierarchy within $\mathrm{FO}^2[<]$ and the $\mathbf{R}_m$-Łm-hierarchy and we prove the following result.

Theorem 9. *A language $L \subseteq A^*$ is definable in $\mathrm{FO}^2_m[<]$ if and only if it is recognizable by a monoid in $\mathbf{R}_{m+1} \cap \text{Ł}m + 1$.*

Theorem 9 immediately yields a decidability result.

Corollary 10. *For each $m \geq 1$, it is decidable whether a given regular language L is $\mathrm{FO}^2_m[<]$-definable. This decision can be achieved in* LOGSPACE *on input the multiplication table of the syntactic monoid of L, and in* PSPACE *on input its minimal automaton.*

Moreover, given a $\mathrm{FO}^2[<]$-definable language L, one can compute the least integer m such that L is $\mathrm{FO}^2_m[<]$.

Proof. We already observed that the $\mathbf{R}_m$ and Łm are decidable, and that each is described by two omega-term identities (Proposition 5). The decidability statement follows immediately. The complexity statement is a consequence of Straubing and Weil's [28, Thm. 2.19]. The computability statement follows immediately. □

We now turn to the proof of Theorem 9. One implication was established in Theorem 8. To prove the reverse implication, we prove Proposition 11 below, which establishes that every language recognized by a monoid $M \in \mathbf{R}_{m+1} \cap$ Ł$m + 1$ is a union of $\equiv_{m,n}$-classes for some integer n depending on M. Theorem 9 follows, in view of Theorem 2.

Proposition 11. *For every $m \geq 1$ and every morphism $\varphi\colon A^* \to M$ with $M \in \mathbf{R}_{m+1} \cap$ Ł$m + 1$ there exists an integer n such that $\equiv_{m,n}$ is contained in $\equiv_\varphi$.*

Before we embark in the proof of Proposition 11, we record several algebraic and combinatorial lemmas.

3.1 A collection of technical lemmas

Lemma 12. *Let M be a finite monoid. If $s \mathrel{\mathcal{R}} sx$ and $x \sim_{\mathbf{K}} y$, then $sx = sy$. If $s \mathrel{\mathcal{L}} xs$ and $x \sim_{\mathbf{D}} y$, then $xs = ys$.*

Proof. Let $z \in M$ such that $sxz = u$. We have $(xz)^\omega x \mathrel{\mathcal{J}} (xz)^\omega$. Now, $x \sim_{\mathbf{K}} y$ implies $(xz)^\omega x = (xz)^\omega y$. Thus $sx = s(xz)^\omega x = s(xz)^\omega y = sy$. The second statement is left-right symmetric. □

The following lemma illustrates an important structural property of monoids in **DA**.

Lemma 13. *Let $\varphi\colon A^* \to M$, with $M \in \mathbf{DA}$ and let $x, y, z \in A^*$ such that $\varphi(x) \mathrel{\mathcal{R}} \varphi(xy)$ and $\mathsf{alph}(z) \subseteq \mathsf{alph}(y)$. Then $\varphi(x) \mathrel{\mathcal{R}} \varphi(xz)$.*

Proof. The map $\mathsf{alph}\colon A^* \to \mathcal{P}(A)$ can be seen as a morphism, where the product on $\mathcal{P}(A)$ is the union operation. Since $M \in \mathbf{DA}$, we have $M/{\sim_{\mathbf{LI}}} \in \mathbf{J}_1$; let $\pi\colon M \to M/{\sim_{\mathbf{LI}}}$ be the projection morphism. It is easily verified that there exists a morphism $\psi\colon \mathcal{P}(A) \to M/{\sim_{\mathbf{LI}}}$ such that $\psi \circ \mathsf{alph} = \pi \circ \varphi$, see Figure 3.

By assumption, $\varphi(x) = \varphi(xyt)$ for some $t \in A^*$, and hence $\varphi(x) = \varphi(x)\varphi(yt)^\omega$. Since $\mathsf{alph}((yt)^\omega) = \mathsf{alph}((yt)^\omega z (yt)^\omega)$, we have $\varphi(yt)^\omega \sim_{\mathbf{LI}} \varphi(yt)^\omega \varphi(z) \varphi(yt)^\omega$. Applying the definition of $\sim_{\mathbf{LI}}$ with $e = f = \varphi(yt)^\omega$, it follows that $\varphi(yt)^\omega = \varphi(yt)^\omega \varphi(z) \varphi(yt)^\omega$ and we now have

$$\varphi(x) = \varphi(x)\varphi(yt)^\omega = \varphi(x)\varphi(yt)^\omega\varphi(z)\varphi(yt)^\omega = \varphi(x)\varphi(z)\varphi(yt)^\omega.$$

$$\begin{tikzcd}
A^* \arrow[r, "\varphi"] \arrow[d, "\mathsf{alph}"'] & M \arrow[d, "\pi"] \\
\mathcal{P}(A) \arrow[r, "\psi"'] & M/{\sim_{\mathbf{LI}}}
\end{tikzcd}$$

Figure 3: $M \in \mathbf{DA} = \mathbf{LI} \textcircled{m} \mathbf{J}_1$

Therefore $\varphi(x) \mathrel{\mathcal{R}} \varphi(xz)$, which concludes the proof. $\square$

A proof of the following lemma can be found in [14, Prop. 3.6 and Lem. 3.7].

Lemma 14. *Let $m \geq 2$, $u, v \in A^*$, $a \in A$.*

1. *If $u \triangleright_{m,n} v$ and $u = u_- a u_+$ and $v = v_- a v_+$ are a-left factorizations, then $u_- \triangleright_{m,n-1} v_-$ and $u_+ \triangleright_{m,n-1} v_+$.*
2. *If $u \triangleright_{m,n} v$ and $u = u_- a u_+$ and $v = v_- a v_+$ are a-right factorizations, then $u_- \triangleright_{m,n-1} v_-$ and $u_+ \triangleleft_{m-1,n-1} v_+$.*

Dual statements hold for $u \triangleleft_{m,n} v$.

Lemma 15. *Let $m, n \geq 2$ and let $u = u_- a u_+$ and $v = v_- a v_+$ be a-left factorizations. If $u \equiv_{m,n} v$, then $u_- \equiv_{m-1,n-1} v_-$ and $u_+ \equiv_{m,n-1} v_+$. A dual statement holds for the factors of the a-right factorizations of u and v.*

Proof. We first show $u_- \equiv_{m-1,n-1} v_-$. Consider a ranker $r \in R_{m-1,n-1}$, supposing first that $r \in R^{\mathsf{X}}_{m-1,n-1}$. Then r is defined on u_- if and only if r is defined on u and $\operatorname{ord}(r'(u), \mathsf{X}_a(u))$ is $<$ for every nonempty prefix r' of r. By definition of $\equiv_{m,n}$, this is equivalent to r being defined on v_-. If instead $r \in R^{\mathsf{Y}}_{m-1,n-1}$, then r is defined on u_- if and only if $\mathsf{X}_a\, r \in R_{m,n}$ is defined on u and $\operatorname{ord}(\mathsf{X}_a\, r'(u), \mathsf{X}_a(u))$ is $<$ for every nonempty prefix r' of r. Again, this is equivalent to r being defined on v_- since $u \equiv_{m,n} v$. Thus, the same rankers in $R_{m-1,n-1}$ are defined on u_- and v_-.

Now consider rankers $r \in R^{\mathsf{X}}_{m-1,n-1}$ and $s \in R^{\mathsf{Y}}_{m-1,n-2}$, which we can assume to be defined on both u_- and v_-. Then the order types induced by r and s on u_- and v_- are equal, since $\operatorname{ord}(r(u_-), s(u_-)) = \operatorname{ord}(r(u), \mathsf{X}_a\, s(u)) = \operatorname{ord}(r(v), \mathsf{X}_a\, s(v)) = \operatorname{ord}(r(v_-), s(v_-))$ and $\mathsf{X}_a\, s \in R^{\mathsf{X}}_{m,n-1}$.

The same reasoning applies if $r \in R^{\mathsf{Y}}_{m-1,n-1}$ and $s \in R^{\mathsf{X}}_{m-1,n-2}$ (resp. if $r \in R^{\mathsf{X}}_{m-1,n-1}$ and $s \in R^{\mathsf{X}}_{m-1,n-2}$, if $r \in R^{\mathsf{Y}}_{m-1,n-1}$ and $s \in R^{\mathsf{Y}}_{m-2,n-2}$) since in that case, $\operatorname{ord}(r(u_-), s(u_-)) = \operatorname{ord}(\mathsf{X}_a\, r(u), s(u))$ (resp. $\operatorname{ord}(r(u), s(u))$, $\operatorname{ord}(\mathsf{X}_a\, r(u), \mathsf{X}_a\, s(u))$). Therefore, $u_- \equiv_{m-1,n-1} v_-$.

We now verify that $u_+ \equiv_{m,n-1} v_+$. The proof is very similar to the first part and deviates only in technical details. Consider a ranker $r \in R_{m,n-1}$, say, in $R^{\mathsf{X}}_{m,n-1}$. Then r is defined on u_+ if and only if $\mathsf{X}_a\, r \in R_{m,n}$ is defined on u and $\mathrm{ord}(\mathsf{X}_a\, r'(u), \mathsf{X}_a(u))$ is $>$ for every nonempty prefix r' of r. Again, this is equivalent to r being defined on v_+ since $u \equiv_{m,n} v$. If instead $r \in R^{\mathsf{Y}}_{m,n-1}$, then r is defined on u_+ if and only if r is defined on u and $\mathrm{ord}(r'(u), \mathsf{X}_a(u))$ is $>$ for every nonempty prefix r' of r, which is equivalent to r being defined on v_+. Thus, the same rankers in $R_{m,n-1}$ are defined on u_+ and v_+.

Now consider rankers $r \in R^{\mathsf{X}}_{m,n-1}$ and $s \in R^{\mathsf{Y}}_{m,n-2}$, both defined on u_+ and v_+. Then the order types induced by r and s on u_+ and v_+ are equal, since $\mathrm{ord}(r(u_+), s(u_+)) = \mathrm{ord}(\mathsf{X}_a\, r(u), s(u))$ and $\mathsf{X}_a\, r \in R^{\mathsf{X}}_{m,n}$.

Again, a similar verification guarantees that the order types induced by r and s on u_+ and v_+ are equal also if $r \in R^{\mathsf{Y}}_{m,n-1}$ and $s \in R^{\mathsf{X}}_{m,n-2}$, or if $r \in R^{\mathsf{X}}_{m,n-1}$ and $s \in R^{\mathsf{X}}_{m-1,n-2}$, or if $r \in R^{\mathsf{Y}}_{m,n-1}$ and $s \in R^{\mathsf{Y}}_{m-1,n-2}$. This shows $u_+ \equiv_{m,n-1} v_+$ which completes the proof. $\square$

Lemma 16. *Let $m, n \geq 2$ and let $u = u_- a u_0 b u_+$ and $v = v_- a v_0 b v_+$ describe b-left and a-right factorizations (that is, $a \notin \mathsf{alph}(u_0 b u_+) \cup \mathsf{alph}(v_0 b v_+)$ and $b \notin \mathsf{alph}(u_- a u_0) \cup \mathsf{alph}(v_- a v_0)$). If $u \equiv_{m,n} v$, then $u_0 \equiv_{m-1,n-1} v_0$.*

Proof. A ranker $r \in R^{\mathsf{X}}_{m-1,n-1}$ is defined on u_0 if and only if $\mathsf{Y}_a\, r \in R_{m,n}$ is defined on u and $\mathrm{ord}(\mathsf{Y}_a\, r'(u), \mathsf{Y}_a(u))$ is $>$ and $\mathrm{ord}(\mathsf{Y}_a\, r'(u), \mathsf{X}_b(u))$ is $<$ for every nonempty prefix r' of r. Similarly, a ranker $r \in R^{\mathsf{Y}}_{m-1,n-1}$ is defined on u_0 if and only if $\mathsf{X}_b\, r \in R_{m,n}$ is defined on u and $\mathrm{ord}(\mathsf{X}_b\, r'(u), \mathsf{Y}_a(u))$ is $>$ and $\mathrm{ord}(\mathsf{X}_b\, r'(u), \mathsf{X}_b(u))$ is $<$ for every nonempty prefix r' of r. Thus, if $u \equiv_{m,n} v$, then the same rankers in $R_{m-1,n-1}$ are defined on u_0 and v_0.

Now consider rankers $r \in R^{\mathsf{X}}_{m-1,n-1}$ and $s \in R^{\mathsf{Y}}_{m-1,n-2}$ (resp. $r \in R^{\mathsf{Y}}_{m-1,n-1}$ and $s \in R^{\mathsf{X}}_{m-1,n-2}$), defined on both u_0 and v_0. Then $\mathrm{ord}(r(u_0), s(u_0)) = \mathrm{ord}(\mathsf{Y}_a\, r(u), \mathsf{X}_b\, s(u))$ (resp. $\mathrm{ord}(\mathsf{X}_b\, r(u), \mathsf{Y}_a\, s(u))$). Since $u \equiv_{m,n} v$, $\mathsf{Y}_a\, r \in R^{\mathsf{Y}}_{m,n}$ and $\mathsf{X}_b\, s \in R^{\mathsf{X}}_{m,n_1}$ (resp. $\mathsf{X}_b\, r \in R^{\mathsf{X}}_{m,n}$ and $\mathsf{Y}_a\, s \in R^{\mathsf{Y}}_{m,n_1}$), the order types defined by r and s on u_0 and v_0 are equal.

If $m = 2$, we are done proving that $u_0 \equiv_{m-1,n-1} v_0$. We now assume that $m \geq 3$. Let $r \in R^{\mathsf{X}}_{m-1,n-1}$ and $s \in R^{\mathsf{X}}_{m-2,n-2}$ (resp. $r \in R^{\mathsf{Y}}_{m-1,n-1}$ and $s \in R^{\mathsf{Y}}_{m-2,n-2}$) be defined on both u_0 and v_0. Then $\mathrm{ord}(r(u_0), s(u_0)) = \mathrm{ord}(\mathsf{Y}_a\, r(u), \mathsf{Y}_a\, s(u))$ (resp. $\mathrm{ord}(\mathsf{X}_b\, r(u), \mathsf{X}_b\, s(u))$). By the same reasoning as above, the order type defined by v on u_0 and v_0 is the same since $\mathsf{Y}_a\, r \in R^{\mathsf{Y}}_{m,n}$ and $\mathsf{Y}_a\, s \in R^{\mathsf{Y}}_{m-1,n-1}$ (resp. $\mathsf{X}_b\, r \in R^{\mathsf{X}}_{m,n}$ and $\mathsf{X}_b\, s \in R^{\mathsf{X}}_{m-1,n-1}$). This concludes the proof of the lemma. $\square$

$$
\begin{tikzcd}
 & & A^* \arrow[ddll] \arrow[ddl, bend right, "\rho"'] \arrow[d, "\varphi"] \arrow[ddr, bend left, "\lambda"] \arrow[ddrr] \arrow[dddrrr, bend left] & & & \\
 & & M \arrow[dl, "\pi_{\mathbf{D}}"'] \arrow[dr, "\pi_{\mathbf{K}}"] & & & \\
A^*/\rhd_{m,n} \arrow[r] & M/{\sim_{\mathbf{D}}} \arrow[dr] & & M/{\sim_{\mathbf{K}}} \arrow[dl] & A^*/\lhd_{m,n} \arrow[l] & \\
 & & A^*/(\equiv_\rho \vee \equiv_\lambda) & & & A^*/{\equiv_{m-1,n}} \arrow[lll]
\end{tikzcd}
$$

Figure 4: A commutative diagram

3.2 Proof of Proposition 11

The proof is by induction on m. We already observed that L is $\mathrm{FO}_1^2[<]$-definable if and only if it is piecewise testable, if and only if it is accepted by a monoid in $\mathbf{J}$. Since $\mathbf{J} = \mathbf{R}_2 \cap \text{Ł}2$, Proposition 11 holds for $m = 1$. We now assume that $m \geq 2$.

Let $\varphi\colon A^* \to M$ be a morphism with $M \in \mathbf{R}_{m+1} \cap \text{Ł}m+1$. We note that it suffices to prove Proposition 11 for the morphism $\varphi'\colon A^* \to M \times 2^A$ given by $\varphi'(u) = (\varphi(u), \mathsf{alph}(u))$. Observe that, for $u, v \in A^*$,

$$\varphi'(u) \sim_{\mathbf{D}} \varphi'(v) \text{ (resp. } \varphi'(u) \sim_{\mathbf{K}} \varphi'(v)) \quad \text{implies} \quad \mathsf{alph}(u) = \mathsf{alph}(v). \tag{1}$$

Indeed we have $\varphi'(u)\varphi'(u)^\omega = \varphi'(u)^\omega$ (since M is aperiodic): then $\varphi'(u) \sim_{\mathbf{D}} \varphi'(v)$ implies that $\varphi'(v)\varphi'(u)^\omega = \varphi'(u)\varphi'(u)^\omega$ and by definition of φ', $\mathsf{alph}(v)$ is contained in $\mathsf{alph}(u)$. By symmetry, u and v have the same alphabetical content and the same holds for $\sim_{\mathbf{K}}$.

To lighten up the notation, we dispense with the consideration of φ' and we assume that φ satisfies Property (1).

Let $\pi_{\mathbf{D}} : M \to M/{\sim_{\mathbf{D}}}$ and $\pi_{\mathbf{K}} : M \to M/{\sim_{\mathbf{K}}}$ be the natural morphisms. By definition of $\mathbf{R}_{m+1}$ and $\text{Ł}m+1$, we have $M/{\sim_{\mathbf{D}}} \in \mathbf{R}_m$ and $M/{\sim_{\mathbf{K}}} \in \text{Ł}m$. Let $\rho = \pi_{\mathbf{D}} \circ \varphi$ and $\lambda = \pi_{\mathbf{K}} \circ \varphi$, see Figure 4. The monoid $A^*/(\equiv_\rho \vee \equiv_\lambda)$ is a quotient of both $M/{\sim_{\mathbf{D}}}$ and $M/{\sim_{\mathbf{K}}}$, so $A^*/(\equiv_\rho \vee \equiv_\lambda) \in \mathbf{R}_m \cap \text{Ł}m$ and there exists $n \geq 1$ such that

- $\rhd_{m,n}$ is contained in $\equiv_\rho$ and $\lhd_{m,n}$ is contained in $\equiv_\lambda$ (by Proposition 4),
- $\equiv_{m-1,n}$ is contained in $\equiv_\rho \vee \equiv_\lambda$ (by induction).

We show that $\equiv_{m,n+2|M|}$ is contained in $\equiv_\varphi$. Let $u \equiv_{m,n+2|M|} v$. Consider the $\mathcal{R}$-factorization of u, i.e., $u = s_1 a_1 \cdots s_k a_k s_{k+1}$ with $a_i \in A$ and $s_i \in A^*$ such that $1 = \varphi(s_1)$ and for all $1 \le i \le k$:

$$\varphi(s_1 a_1 \cdots s_i) >_{\mathcal{R}} \varphi(s_1 a_1 \cdots s_i a_i) \mathrel{\mathcal{R}} \varphi(s_1 a_1 \cdots s_i a_i s_{i+1}).$$

Since the number of $\mathcal{R}$-classes is at most $|M|$, we have $k < |M|$. Similarly, let $v = t_1 b_1 \cdots t_{k'} b_{k'} t_{k'+1}$ with $b_i \in A$ and $t_i \in A^*$ be the $\mathcal{L}$-factorization of v such that $\varphi(t_{k'+1}) = 1$ and for all $1 \le i \le k'$:

$$\varphi(t_i b_i t_{i+1} \cdots b_{k'} t_{k'+1}) \mathrel{\mathcal{L}} \varphi(b_i t_{i+1} \cdots b_{k'} t_{k'+1}) <_{\mathcal{L}} \varphi(t_{i+1} \cdots b_{k'} t_{k'+1}).$$

As before, we have $k' < |M|$. By Lemma 13 (applied with $x = s_1 \cdots s_{i-1} a_{i-1}$, $y = s_i$ and $z = a_i$), we have $a_i \notin \mathsf{alph}(s_i)$; and similarly, $b_i \notin \mathsf{alph}(t_{i+1})$. Therefore, the positions of the a_i's in u are exactly the positions visited by the ranker $r = \mathsf{X}_{a_1} \cdots \mathsf{X}_{a_k}$, and the positions of the b_i's in v are exactly the positions visited by the ranker $s = \mathsf{Y}_{b_{k'}} \cdots \mathsf{Y}_{b_1}$. Since $u \equiv_{m,n+2|M|} v$, each of the rankers r and s is defined on both u and v, and all the positions visited by the rankers r and s occur in the same order in u as in v. We call these positions *special*. Let

$$\begin{aligned} u &= u_1 c_1 \cdots u_\ell c_\ell u_{\ell+1} \\ v &= v_1 c_1 \cdots v_\ell c_\ell v_{\ell+1} \end{aligned}$$

be obtained by factoring u and v at all the special positions. We have $\ell \le k + k' < 2|M|$. We say that a special position is *red* if it is visited by r, and that it is *green* if it is visited by s. Some special positions may be both red and green, which means that more than one of the cases below may apply.

For u the above factorization is a refinement of the $\mathcal{R}$-factorization; and for v it is a refinement of the $\mathcal{L}$-factorization. In particular, $\varphi(u_1) = 1$, $\varphi(v_{\ell+1}) = 1$ and

$$\begin{aligned} \varphi(u_1 \cdots u_{i-1} c_{i-1}) &\mathrel{\mathcal{R}} \varphi(u_1 \cdots u_{i-1} c_{i-1} u_i) \qquad \text{for } 1 < i \le \ell + 1, && (\mathrm{Eq}(\mathcal{R})) \\ \varphi(v_i c_i v_{i+1} \cdots c_\ell) &\mathrel{\mathcal{L}} \varphi(c_i v_{i+1} \cdots c_\ell) \qquad \text{for } 1 \le i \le \ell. && (\mathrm{Eq}(\mathcal{L})) \end{aligned}$$

In order to prove $u \equiv_\varphi v$, we show that we can gradually substitute u_i for v_i in the product $v_1 c_1 \cdots v_\ell c_\ell v_{\ell+1} = v$, starting from $i = 1$, while maintaining $\equiv_\varphi$-equivalence. Namely we show that, for each i, it holds

$$u_1 \cdots u_{i-1} c_{i-1}\, u_i\, c_i v_{i+1} \cdots v_{\ell+1} \equiv_\varphi u_1 \cdots u_{i-1} c_{i-1}\, v_i\, c_i v_{i+1} \cdots v_{\ell+1}. \qquad (\mathrm{Eq(i)})$$

Let h_0 be the leftmost red position: then $c_{h_0} = a_1$ and $s_1 = u_1 c_1 \cdots u_{h_0}$. Since $\varphi(s_1) = 1$ and M is aperiodic, the φ-image of every letter in s_1 is 1. Applying Lemma 15 to the a_1-left factorizations of u and v, we find that $u_1 c_1 \cdots u_{h_0 - 1} \equiv_{m-1,n-1} v_1 c_1 \cdots v_{h_0-1}$ and in particular, these words have the same alphabet. It follows that $\varphi(u_i) = \varphi(v_i) = 1$ for all $i \leq h_0$, and hence (Eq(i)) holds for all $i \leq h_0$.

The right-left dual of this reasoning establishes that $\varphi(u_i) = \varphi(v_i) = 1$ for all the u_i, v_i to the right of the last (rightmost) green position, say j_0. In particular, (Eq(i)) also holds for all $i > j_0$.

We now assume that $h_0 < i \leq j_0$ and we let $h-1$ be the first red position to the left of i and j be the first green position to the right of i: we have $h_0 < h \leq i \leq j \leq j_0$.

Case 1: $h = i$ ($i-1$ is red) We have $u \triangleright_{m,n+2|M|} v$. By Lemma 14 (1), a sequence of at most $i-1$ left-factorizations yields $u_i c_i \cdots u_{\ell+1} \triangleright_{m,n+2|M|-i+1} v_i c_i \cdots v_{\ell+1}$. If i is red, then by Lemma 14 (1), after one c_i-left-factorization, we see that $u_i \triangleright_{m,n+2|M|-i} v_i$. If i is not red, then i is green and by Lemma 14 (2), after at most $\ell - i$ right-factorizations, we find that u_i and v_i are $\triangleright_{m,n+2|M|-i-(\ell-i)}$-equivalent. In any case, we have $u_i \triangleright_{m,n} v_i$ and thus $u_i \equiv_\rho v_i$ (i.e., $\varphi(u_i) \sim_{\mathbf{D}} \varphi(v_i)$) by the choice of n. In view of (Eq($\mathcal{L}$)), Lemma 12 now implies

$$u_i c_i v_{i+1} \cdots c_\ell v_{\ell+1} \equiv_\varphi v_i c_i v_{i+1} \cdots c_\ell v_{\ell+1}$$

and left multiplication by $u_1 c_1 \cdots c_{i-1}$ yields (Eq(i)).

Case 2: $j = i$ (i is green) As in Case 1, we see that $u_i \equiv_\lambda v_i$. (Eq($\mathcal{R}$)) and Lemma 12 then imply

$$u_1 c_1 \cdots u_{i-1} c_{i-1} u_i \equiv_\varphi u_1 c_1 \cdots u_{i-1} c_{i-1} v_i,$$

and right multiplication by $c_i v_{i+1} \cdots v_{\ell+1}$ yields (Eq(i)).

Case 3: $h < i < j$ ($i-1$ is not red and i is not green) By Lemma 15, after at most $h-1$ left factorizations and $\ell - j + 1$ right factorizations, we obtain $u_h c_h \cdots u_j \equiv_{m,n+j-h} v_h c_h \cdots v_j$ (since $n + j - h \leq n + 2\,|M| - (h - 1) - (\ell - j + 1)$). Lemma 16, applied with $a = c_{i-1}$ and $b = c_i$, then yields $u_i \equiv_{m-1,n} v_i$. Since $\equiv_{m-1,n}$ is contained in $\equiv_\lambda \vee \equiv_\rho$, there exist words $w_1, \ldots, w_d$ such that

$$v_i = w_1 \equiv_\rho w_2 \equiv_\lambda w_3 \equiv_\rho \cdots \equiv_\lambda w_{d-2} \equiv_\rho w_{d-1} \equiv_\lambda w_d = u_i.$$

After the discussion at the beginning of this section, we have $\mathsf{alph}(v_i) = \mathsf{alph}(w_2) = \cdots = \mathsf{alph}(w_{d-1}) = \mathsf{alph}(u_i)$. Thus, by Lemma 13, we have $\varphi(pu_i) \mathrel{\mathcal{R}} \varphi(p)$ if and only if $\varphi(pw_g) \mathrel{\mathcal{R}} \varphi(p)$, and $\varphi(v_i q) \mathrel{\mathcal{L}} \varphi(q)$ if and only if $\varphi(w_g q) \mathrel{\mathcal{L}} \varphi(q)$ for all $p, q \in A^*$. As in Cases 1 and 2, we conclude that for each $1 \leq e < d$,

- if $w_e \equiv_\rho w_{e+1}$, then
$$w_e c_i \cdots c_\ell v_{\ell+1} \equiv_\varphi w_{e+1} c_i \cdots c_\ell v_{\ell+1}, \text{ and thus}$$
$$u_1 c_1 \cdots u_i c_{i-1} w_e c_i \cdots c_\ell v_{\ell+1} \equiv_\varphi u_1 c_1 \cdots u_i c_{i-1} w_{e+1} c_i \cdots c_\ell v_{\ell+1};$$
- and if $w_e \equiv_\lambda w_{e+1}$, then
$$u_1 c_1 \cdots c_{i-1} w_e \equiv_\varphi u_1 c_1 \cdots c_{i-1} w_{e+1}, \text{ and thus}$$
$$u_1 c_1 \cdots c_{i-1} w_e c_i v_{i+1} \cdots c_\ell v_{\ell+1} \equiv_\varphi u_1 c_1 \cdots c_{i-1} w_{e+1} c_i v_{i+1} \cdots c_\ell v_{\ell+1}.$$

It follows by transitivity of $\equiv_\varphi$ that (Eq(i)) holds.

Concluding the proof We have now established (Eq(i)) for every $1 \leq i \leq \ell + 1$. It follows immediately, by transitivity, that $u \equiv_\varphi v$. ☐

4 Conclusion

We have shown that for each $m \geq 1$, it is decidable whether a given regular language is $\mathrm{FO}^2_m[<]$-definable. Previous results in the literature only showed decidability for levels 1 and 2 of this quantifier alternation hierarchy. Our decidability result follows from the proof that $\mathbf{FO}^2_m$ (the pseudovariety of finite monoids corresponding to the $\mathrm{FO}^2_m[<]$-definable languages) is equal to the intersection $\mathbf{R}_{m+1} \cap \text{Ł}m + 1$, which was known to be decidable.

This result implies the decidability of the levels of the hierarchy given by $\mathbf{V}_1 = \mathbf{J}$ and $\mathbf{V}_{m+1} = \mathbf{V} ** \mathbf{J}$, since Straubing showed that $\mathbf{V}_m = \mathbf{FO}^2_m$ [27]. Straubing used general results of Almeida and Weil on two-sided semidirect products to deduce from this that $\mathbf{FO}^2_2$ is decidable, but these results do not extend to $\mathbf{FO}^2_m$ when $m > 2$ ([1, 37], see [27, Sec. 5] for a discussion).

We also showed that the decision procedure whether a regular language L is FO^2_m-definable, is in LOGSPACE on input the multiplication table of the syntactic monoid of L, and in PSPACE on input the minimal automaton of L. The result behind this statement is the fact that membership in $\mathbf{R}_m$ and in Łm is characterized by a small set of (rather complicated) identities. Straubing conjectured a different and simpler set of identities (Conjecture 7 above). Our results do not confirm this conjecture, which it would be interesting to settle.

References

[1] J. Almeida and P. Weil. Profinite categories and semidirect products. *Journal of Pure and Applied Algebra*, 123:1–50, 1998.

[2] R. S. Cohen and J. A. Brzozowski. Dot-depth of star-free events. *J. Comput. Syst. Sci.*, 5(1):1–16, 1971.

[3] V. Diekert and P. Gastin. First-order definable languages. In *Logic and Automata: History and Perspectives*, Texts in Logic and Games, pages 261–306. Amsterdam University Press, 2008.

[4] V. Diekert, P. Gastin, and M. Kufleitner. A survey on small fragments of first-order logic over finite words. *Int. J. Found. Comput. Sci.*, 19(3):513–548, 2008. Special issue DLT'07.

[5] T. Hall and P. Weil. On radical congruence systems. *Semigroup Forum*, 59:56–73, 1999.

[6] N. Immerman and D. Kozen. Definability with bounded number of bound variables. *Information and Computation*, 83(2):121–139, Nov. 1989.

[7] J. A. W. Kamp. *Tense Logic and the Theory of Linear Order*. PhD thesis, University of California, 1968.

[8] O. Klíma. Piecewise testable languages via combinatorics on words. *Discrete Mathematics*, 311(20):2124–2127, 2011.

[9] K. Krohn, J. L. Rhodes, and B. Tilson. Homomorphisms and semilocal theory. In M. A. Arbib, editor, *Algebraic Theory of Machines, Languages, and Semigroups*, chapter 8, pages 191–231. Academic Press, New York and London, 1968.

[10] M. Kufleitner and P. Weil. On the lattice of sub-pseudovarieties of **DA**. *Semigroup Forum*, 81(2):243–254, 2010.

[11] M. Kufleitner and A. Lauser. Languages of dot-depth one over infinite words. In *LICS'11, Proceedings*, pages 23–32. IEEE Computer Society, 2011.

[12] M. Kufleitner and A. Lauser. Lattices of logical fragments over words. Technical Report Computer Science 2012/03, University of Stuttgart, Faculty of Computer Science, Electrical Engineering, and Information Technology, Germany, March 2012.

[13] M. Kufleitner and P. Weil. On FO^2 quantifier alternation over words. In *MFCS'09, Proceedings*, volume 5734 of *LNCS*, pages 513–524. Springer, 2009.

[14] M. Kufleitner and P. Weil. On logical hierarchies within FO^2-definable languages. *Logical Methods in Computer Science*, 2012. to appear.

[15] K. Lodaya, P. K. Pandya, and S. S. Shah. Marking the chops: an unambiguous temporal logic. In G. Ausiello, J. Karhumäki, G. Mauri, and C.-H. L. Ong, editors, *Fifth IFIP International Conference On Theoretical Computer Science - TCS 2008, Proceedings*, volume 273 of *IFIP*, pages 461–476. Springer-Verlag, 2008.

[16] R. McNaughton and S. Papert. *Counter-Free Automata*. The MIT Press, 1971.

[17] D. Perrin and J.-É. Pin. *Infinite words*, volume 141 of *Pure and Applied Mathematics*. Elsevier, Amsterdam, 2004.

[18] J.-E. Pin. Propriétés syntactiques du produit non ambigu. In W. Kuich, editor, *Proc.7th International Colloquium Automata, Languages and Programming (ICALP'80)*, volume 85 of *Lecture Notes in Computer Science*, pages 483–499, Heidelberg, 1980. Springer-Verlag.

[19] J.-É. Pin. *Varieties of Formal Languages*. North Oxford Academic, London, 1986.

[20] J.-É. Pin. Syntactic semigroups. In *Handbook of Formal Languages*, volume 1, pages 679–746. Springer-Verlag, Berlin, 1997.

[21] J.-É. Pin and P. Weil. Polynomial closure and unambiguous product. *Theory Comput. Syst.*, 30(4):383–422, 1997.

[22] M. P. Schützenberger. On finite monoids having only trivial subgroups. *Inf. Control*, 8:190–194, 1965.

[23] Th. Schwentick, D. Thérien, and H. Vollmer. Partially-ordered two-way automata: A new characterization of DA. In *DLT'01, Proceedings*, volume 2295 of *LNCS*, pages 239–250. Springer, 2001.

[24] I. Simon. Piecewise testable events. In H. Barkhage, editor, *Automata Theory and Formal Languages, 2nd GI Conference, Kaiserslautern, May 22–23, 1975*, volume 33 of *Lecture Notes in Computer Science*, pages 214–222. Springer-Verlag, 1975.

[25] L. Stockmeyer. The complexity of decision problems in automata theory and logic. PhD thesis, TR 133, M.I.T., Cambridge, 1974.

[26] H. Straubing. A generalization of the Schützenberger product of finite monoids. *Theor. Comput. Sci.*, 13:137–150, 1981.

[27] H. Straubing. Algebraic characterization of the alternation hierarchy in $\mathrm{FO}^2[<]$ on finite words. In M. Bezem, editor, *CSL'11*, volume 12 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 525–537, Dagstuhl, Germany, 2011. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[28] H. Straubing and P. Weil. An introduction to finite automata and their connection to logic. In D. D'Souza and P. Shankar, editors, *Modern Applications of Automata Theory*, volume 2 of *IISc Research Monographs*, pages 3–43. World Scientific, 2012.

[29] P. Tesson and D. Thérien. Diamonds are forever: The variety DA. In *Semigroups, Algorithms, Automata and Languages 2001, Proceedings*, pages 475–500. World Scientific, 2002.

[30] P. Tesson and D. Thérien. Logic meets algebra: The case of regular languages. *Log. Methods Comput. Sci.*, 3(1):1–37, 2007.

[31] D. Thérien. Classification of finite monoids: The language approach. *Theor. Comput. Sci.*, 14(2):195–208, 1981.

[32] D. Thérien and Th. Wilke. Over words, two variables are as powerful as one quantifier alternation. In *STOC'98, Proceedings*, pages 234–240. ACM Press, 1998.

[33] D. Thérien and Th. Wilke. Temporal logic and semidirect products: An effective characterization of the until hierarchy. *SIAM J. Comput.*, 31(3):777–798, 2001–2002.

[34] D. Thérien and Th. Wilke. Nesting until and since in linear temporal logic. *Theory of Computing Systems*, 37(1):111–131, 2004.

[35] W. Thomas. Classifying regular events in symbolic logic. *J. Comput. Syst. Sci.*, 25:360–376, 1982.

[36] P. Trotter and P. Weil. The lattice of pseudovarieties of idempotent semigroups and a non-regular analogue. *Algebra Universalis*, 37(4):491–526, 1997.

[37] P. Weil. Profinite methods in semigroup theory. *International Journal of Algebra and Computation*, 12:137–178, 2002.

[38] Ph. Weis. *Expressiveness and succinctness of first-order logic on finite words.* PhD thesis, University of Massachusetts Amherst, 2011.

[39] Ph. Weis and N. Immerman. Structure theorem and strict alternation hierarchy for FO^2 on words. *Log. Methods Comput. Sci.*, 5(3), 2009.