Decidable Characterization of $\mathrm{FO}^2(<,+1)$ and locality of DA

Thomas Place[1] and Luc Segoufin[2]

[1]Bordeaux University, Labri
[2]INRIA & ENS ULM, Valda

March 20, 2018

Abstract

Several years ago Thérien and Wilke exhibited a decidable characterization of the languages of words that are definable in $\mathrm{FO}^2(<,+1)$ [7]. Their proof relies on three separate ingredients. The first one is the characterization of the languages that are definable in $\mathrm{FO}^2(<)$ as those whose syntactic semigroup belongs to the variety **DA**. Then, this result is combined with a *wreath product argument* showing that being definable in $\mathrm{FO}^2(<,+1)$ corresponds to having a syntactic semigroup in $\mathbf{DA} * \mathbf{D}$. Finally, proving that membership of a semigroup in $\mathbf{DA} * \mathbf{D}$ is decidable requires a third ingredient: the "locality" of **DA**, a result proved in [1]. In this note we present a new self-contained and simple proof that definability in $\mathrm{FO}^2(<,+1)$ is decidable. We obtain the locality of **DA** as a corollary.

1 Introduction

Regular languages form a robust class of languages characterized by completely dif and only iferent equivalent formalisms such as automata, finite semigroups or monadic second-order logic, MSO($<$). In particular, the connection between MSO($<$) definability and recognizability by semigroups has been used to investigate the expressive power of fragments of MSO($<$). For this purpose, finding *decidable characterizations* of such fragments often serves as a yardstick. A *decidable characterization* is an algorithm which, given as input a regular language, decides whether it can be defined in the fragment under investigation. More than the algorithm itself, the main motivation is the insight given by its proof. Indeed, in order to prove a decidable characterization, one needs to consider and understand *all* properties that can be expressed in the fragment.

Usually a decidable characterization is presented by exhibiting a variety of semigroups **V** such that a language is definable in the fragment if and only if its syntactic semigroup is in **V**. Ideally, membership of a semigroup in **V** is defined as a finite set of equations that need to be satisfied by all elements of the semigroup. Since the syntactic semigroup of a language is a finite canonical object that can effectively be computed from any representation of the language, this yields decidability. The most striking example, known as McNaughton-Papert-Schützenberger's Theorem [5, 4], is the characterization of first-order logic equipped with a predicate "$<$" denoting the linear-order over words, FO($<$). The result states that a regular language is definable in FO($<$) if and only if its syntactic semigroup is aperiodic (i.e. satisfies the identity $s^\omega = s^{\omega+1}$ where ω is the size of the syntactic semigroup).

Another successful story is the two-variable fragment of FO($<$). Actually two fragments are of interest: $\mathrm{FO}^2(<)$ and $\mathrm{FO}^2(<,+1)$. $\mathrm{FO}^2(<)$ is a restriction of FO($<$) where only two variables may be used (and reused). $\mathrm{FO}^2(<,+1)$ is then obtained by adding a predicate "$+1$" for the successor relation. Note that in full first-order logic, "$+1$" can be defined from the order "$<$." However, this requires more than two variables and therefore $\mathrm{FO}^2(<,+1)$ is strictly more expressive than $\mathrm{FO}^2(<)$.

In [7], Thérien and Wilke proved characterizations for both $\mathrm{FO}^2(<)$ and $\mathrm{FO}^2(<,+1)$. They show that a language is definable in $\mathrm{FO}^2(<)$ (resp. $\mathrm{FO}^2(<,+1)$) if and only if its syntactic semigroup is in the variety **DA** (resp. **DA** $*$ **D**). However, the arguments used for proving that these two characterizations are decidable, are very dif and only iferent. For $\mathrm{FO}^2(<)$, this is immediate as **DA** is defined by an equation: a semigroup belongs to **DA** if it satisfies $(st)^\omega t(st)^\omega = (st)^\omega$[1].

On the other hand, the variety **DA** $*$ **D** is constructed from the varieties **DA** and **D** using an agebraic product called the *wreath product* ("$*$"). The advantage of this definition is that Thérien and Wilke are able to obtain their characterization of $\mathrm{FO}^2(<,+1)$ (with **DA** $*$ **D**) as a consequence of their characterization of $\mathrm{FO}^2(<)$ (with **DA**) using a an algebraic argument known as the *wreath product principle*. The downside is that **DA** $*$ **D** is not defined using identities and decidability of its membership is not immediate. In fact there exist varieties **V** with decidable membership such that membership in **V** $*$ **D** is undecidable[2]. The special case of **DA** $*$ **D** is solved using the *locality* of **DA**, established in [1]. It follows from the locality of **DA** that **DA** $*$ **D** = **LDA** where **LDA** is the variety of semigroups S such that for all idempotents e of S, eSe is a semigroup in **DA**. From this definition, identities characterizing **LDA** can be derived from those of **DA**: $(esete)^\omega t(esete)^\omega = (esete)^\omega$ (where e is an idempotent) and the decidability of its membership follows.

In this paper we present a new proof of the characterization of $\mathrm{FO}^2(<,+1)$ by taking a dif and only iferent approach. We directly show that a language is definable in $\mathrm{FO}^2(<,+1)$ if and only if its syntactic semigroup satisfies the identity $(esete)^\omega s(esete)^\omega = (esete)^\omega$. Our proof remains simple and relies only on elementary combinatorial arguments. We essentially show that when the equation holds one can reduce the problem of constructing an $\mathrm{FO}^2(<,+1)$ formula for the language to constructing an $\mathrm{FO}^2(<)$ formula for another language over a modified alphabet.

The paper is organized as follows. We start with the necessary notations. The key part is Section 3 where we prove that the identity ensures definability in $\mathrm{FO}^2(<,+1)$. In Section 4 we give a standard game argument showing that the equation is implied by definability in $\mathrm{FO}^2(<,+1)$.

2 Notations

Words and Languages. We fix a finite alphabet A. We denote by A^+ the set of all nonempty finite words and by A^* the set of all finite words over A. We denote the empty word by ε. If u, v are words, we denote by $u \cdot v$ or by uv the word obtained from the concatenation of u and v.

For convenience, we only consider languages that do not contain the empty word. That is, a *language* is a subset of A^*. In this paper, we consider regular languages, i.e., languages that can be defined by a *nondeterministic finite automata* (NFA). In the paper, we work with the algebraic representation of regular languages in terms of monoids.

Semigroups and Monoids. A *semigroup* is a set S equipped with an associative operation $s \cdot t$ (often written st). A *monoid* is a semigroup M having a neutral element 1_M, i.e., such that $s \cdot 1_M = 1_M \cdot s = s$ for all $s \in M$.

An element e of a semigroup is *idempotent* if $e^2 = e$. Given a *finite* semigroup S, it is folklore and easy to see that there is an integer $\omega(S)$ (denoted by ω when S is understood) such that for all s of S, s^ω is idempotent.

Observe that the set A^* equipped with the concatenation operation is a monoid (the neutral element is the empty word "ε"). Given a monoid M and a morphism $\alpha : A^* \to M$, we say that a language L *is recognized by* α if there exists $F \subseteq M$ such that $L = \alpha^{-1}(F)$. It is well known that a language is regular if and only if it can be recognized by a morphism into a *finite* monoid. Finally, from any NFA recognizing some language L, one can compute a canonical morphism $\alpha : A^* \to M$ into a finite monoid recognizing L: the *syntactic morphism* of L (M is the transition monoid of

[1]The authors of [7] actually use the identity $(str)^\omega t(str)^\omega = (str)^\omega$ as the definition of **DA**. We use here a simpler identity that is equivalent to it, see for instance[3].

the minimal deterministic automaton recognizing it). Additionally, the monoid M is called the *syntactic monoid* of L and the semigroup $S = \alpha(A^+)$ is called the *syntactic semigroup* of L.

Logic. As usual a word can be seen as a logical structure whose domain is the sequence of positions in the word. We work with unary predicates P_a for all $a \in A$ denoting positions carrying the letter a and two binary predicates $+1$ and $<$ denoting the successor relation and the order relation among positions. First-order logic is then defined as usual and we denote by $\mathrm{FO}^2(<)$ the two variable restriction of $\mathrm{FO}(<)$ and by $\mathrm{FO}^2(<,+1)$ the two variable restriction of $\mathrm{FO}(<,+1)$. We shall use the two following classical closure properties of $\mathrm{FO}^2(<)$.

Lemma 1. *Let A be an alphabet and $K, L \subseteq A^*$ which are definable in $\mathrm{FO}^2(<)$. Then, $K \cup L$ is definable in $\mathrm{FO}^2(<)$.*

Proof. Immediate: we may combine formulas defining K and L using disjunction. □

Lemma 2. *Let A be an alphabet and $a \in A$ a letter. Let $K \subseteq (A \setminus \{a\})^*$ and $L \subseteq A^*$ which are definable in $\mathrm{FO}^2(<)$. Then, KaL and LaK are definable in $\mathrm{FO}^2(<)$.*

Proof. We show that KaL is definable in $\mathrm{FO}^2(<)$ (the proof for LaK is symmetrical). By hypothesis we have $\mathrm{FO}^2(<)$ formulas ψ and Γ which define K and L respectively. Since $K \subseteq (A \setminus \{a\})^*$ by construction, a formula φ defining KaL is as follows:

$$\varphi = \exists x \; P_a(x) \wedge \psi^{\leq} \wedge \Gamma^{\geq},$$

where $\psi^{\leq}$ is constructed from ψ by replacing all quantifications $\exists y$ by $\exists y(\forall x \leq y \neg P_a(x))$ while $\Gamma^{\geq}$ is constructed from Γ by replacing all quantifications $\exists y$ by $\exists y(\exists x < y P_a(x))$. It follows from the definitions that φ defines KaL. □

3 Characterization of $\mathbf{FO}^2(<,+1)$

In this section we prove the characterization of $\mathrm{FO}^2(<,+1)$:

Theorem 3. *A regular word language L is definable in $\mathrm{FO}^2(<,+1)$ if and only if its syntactic semigroup S satisfies, for all $s,t,e \in S$ with e idempotent:*

$$(esete)^\omega = (esete)^\omega t (esete)^\omega \tag{1}$$

There are two directions to prove. That (1) is necessary follows from a classical Ehrenfeucht-Fraïssé argument. We state it in the next proposition whose proof is is postponed to Section 4.

Proposition 4. *If a language L is definable in $\mathrm{FO}^2(<,+1)$, its syntactic semigroup satisfies* (1).

The remainder of this section is devoted to the proof of the other direction. We formalize it with the following proposition.

Proposition 5. *Consider a finite monoid M, a morphism $\alpha : A^* \to M$ and $S = \alpha(A^+)$. Moreover, assume that S satisfies* (1). *Then, any language recognized by α is definable in $\mathrm{FO}^2(<,+1)$.*

We fix the morphism $\alpha : A^* \to M$ and $S = \alpha(A^+)$ satisfying (1) for the proof. Our argument is based on two steps. We first build another alphabet B and a new morphism $\beta : B^* \to M$. Then, we use our hypothesis on S to prove that any language recognized by β can be "approximated" with another language definable in $\mathrm{FO}^2(<)$ (we make this notion precise below). This suffices to show that the languages recognized by α are definable in $\mathrm{FO}^2(<,+1)$.

We begin with the definition of the new alphabet B. We let $\Box$ as some symbol which does not correspond to any element in M. Moreover, we write $E(S)$ for the set of idempotents in the semigroup S and fix an arbitrary linear order over it. Consider the new alphabet

$$B = \{(e,s,f) \mid e,f \in E(S) \cup \{\Box\}, s \in M\},$$

Observe that the morphism α can be generalized as a monoid morphism $\beta : B^* \to M$. Given $e, f \in E(S)$ and $s \in M$, we let $\beta((e, s, f)) = esf$, $\beta((\Box, s, f)) = sf$, $\beta((e, s, \Box)) = es$ and $\beta((\Box, s, \Box)) = s$.

We shall mainly be interested in special words of B^* that we call "*well-formed*". A word $u = (e_0, s_0, f_0) \cdots (e_n, s_n, f_n) \in B^*$ is *well-formed* if and only if the three following conditions are satisfied:

1. u is non-empty.
2. $e_0 = f_n = \Box$.
3. For all $i < n - 1$, $f_i = e_{i+1} \in E(S)$ (in particular $e_i = f_i \neq \Box$).

Given three languages $H, K, L \subseteq B^*$, we say that H *coincides with* K *over* L when $H \cap L = K \cap L$. In particular, when L is the language of all well-formed words, we say that H coincides with K over well-formed words. We may now come back to the proof of Proposition 5. It is proved as a corollary of the two following lemmas:

Lemma 6. *There exists a map $\eta : A^* \to B^*$ which satisfies the two following properties:*

- *For every $w \in A^*$, $\eta(w)$ is well-formed and $\alpha(w) = \beta(\eta(w))$.*
- *For every language $K \subseteq B^*$ which is $\mathrm{FO}^2(<)$-definable, $\eta^{-1}(K) \subseteq A^*$ is $\mathrm{FO}^2(<, +1)$-definable.*

Lemma 7. *For every $s \in M$, there exists a language $K \subseteq B^*$ which is $\mathrm{FO}^2(<)$-definable and coincides with $\beta^{-1}(s)$ over well-formed words.*

Before proving the lemmas, let us use them to finish the proof of Proposition 5. Let $L \subseteq A^*$ which is recognized by α. We have to show that L is $\mathrm{FO}^2(<, +1)$-definable. By definition, we have $F \subseteq M$ such that $L = \alpha^{-1}(F)$. Consequently,

$$L = \bigcup_{s \in F} \alpha^{-1}(s)$$

By Lemma 1, it remains to show that $\alpha^{-1}(s)$ is $\mathrm{FO}^2(<, +1)$-definable for every $s \in M$. By Lemma 7, we get $K \subseteq B^*$ which is $\mathrm{FO}^2(<)$-definable and coincides with $\beta^{-1}(s)$ over well-formed words. One may verify from the first assertion in Lemma 6 that $\eta^{-1}(K) = \eta^{-1}(\beta^{-1}(s)) = \alpha^{-1}(s)$. Moreover, it follows from the second assertion in Lemma 6 that $\eta^{-1}(K)$ is $\mathrm{FO}^2(<, +1)$-definable. Altogether, we get that $\alpha^{-1}(s)$ is $\mathrm{FO}^2(<, +1)$-definable, concluding the proof.

It remains to prove Lemma 6 and Lemma 7. We devote a subsection to each proof.

3.1 Proof of Lemma 6

We have to define a map $\eta : A^* \to B^*$ satisfying the two assertions in the lemma. Let us point out beforehand that η will **not** be a morphism. The definition is inspired by [6].

Consider a word $w \in A^*$. We define $\eta(w)$. If w has length smaller than $|S|$ then $\eta(w) = (\Box, \alpha(w), \Box)$.

Otherwise, assume that $w = a_1 \cdots a_\ell$ with $\ell > |S|$. Fix k such that $1 \leq k \leq \ell - |S|$. It follows from a pigeon-hole principle argument that there exist $k \leq i < j \leq k + |S|$ such that: $\alpha(a_k \cdots a_i) = \alpha(a_k \cdots a_j)$. We then have $\alpha(a_k \cdots a_i) = \alpha(a_k \cdots a_i)(\alpha(a_{i+1} \cdots a_j))^\omega$. This implies that there is an idempotent e such that $\alpha(a_k \cdots a_i) = \alpha(a_k \cdots a_i)e$. We set i_k as the smallest such $i \geq k$ and e_k as smallest such idempotent for i_k. Doing this for all k yields a set $\{i_1, \ldots, i_{\ell-|S|}\}$ of indices together with associated idempotents: $e_1, \ldots, e_{\ell-S}$. Observe that it may happen that $i_k = i_{k+1}$. For this reason we rename the set of indices as $\{j_1, \ldots, j_h\} = \{i_1, \ldots, i_{\ell-|S|}\}$ with associated idempotents $f_1, \ldots, f_h$ and such that for all k, $j_k < j_{k+1}$.

We then decompose w as $w = w_1 \cdots w_{h+1}$ where: $w_1 = a_1 \dots a_{j_1} \in A^+$, for all $k \in \{1, \dots, h\}$, $w_k = a_{j_{k-1}+1} \cdots a_{j_k} \in A^+$ and $w_{h+1} = a_{j_h+1} \cdots a_\ell \in A^+$. Observe that by construction, for all k, w_k has length smaller than $|S|$ and

$$\alpha(w) = \alpha(w_1) f_1 \alpha(w_1) \cdots f_h \alpha(w_{h+1}) \tag{2}$$

We define $\eta(w) = b_1 \cdots b_{h+1} \in B^*$ with $b_k = (f_{k-1}, \alpha(w_k), f_k)$ (we let $f_0 = f_{h+1} = \Box$). This concludes the definition of $\eta : A^* \to B^*$. Before we show that the two assertions in Lemma 6 are satisfied, let us provide some more terminology that we shall need for this proof.

Consider a word $w \in A^*$ and the construction described above. We say that a position x in w is *distinguished* if it corresponds to the leftmost position of one of the factors w_k of w. To any distinguished position x in w, one can associate the corresponding position $\widehat{x}$ in $\eta(w)$.

The following observation will be crucial in the proof. It essentially states that one can test in $\mathrm{FO}^2(<, +1)$ whether a position x of a word in A^+ is distinguished as well as the label of the corresponding position $\hat{x}$ in $\lfloor w \rfloor$.

Claim 8. *For any $b \in B$ there exists a formula $\alpha_b(x)$ of $\mathrm{FO}^2(<, +1)$ such that for any $w \in A^+$ and any position x of w we have*
$w \models \alpha_b(x)$ *if and only if x is a distinguished position of w such that $\widehat{x}$ has label b in $\lfloor w \rfloor$.*

Proof sketch. This is because by construction the neighborhood of x of size $|S|$ determines whether x is distinguished and the label of $\widehat{x}$. □

We may now prove that the two assertions in Lemma 6 are satisfied. Observe that for any $w \in A^*$, $\eta(w)$ is well-formed by construction and by (2), we have $\beta(\eta(w)) = \alpha(w)$. Consequently, the first assertion in Lemma 6 is satisfied. We now concentrate on proving the second assertion.

Consider a language $K \subseteq B^*$ which is $\mathrm{FO}^2(<)$-definable. We have to show that the language $\eta^{-1}(K)$ is $\mathrm{FO}^2(<, +1)$-definable. By hypothesis, we have a formula φ of $\mathrm{FO}^2(<)$ defining K. We use φ to construct $\psi \in \mathrm{FO}^2(<, +1)$ defining $\eta^{-1}(K)$. The construction is based on Claim 8.

We know from Claim 8 that being a distinguished position is definable in $\mathrm{FO}^2(<, +1)$. Let ψ be the formula constructed from φ by restricting all quantifications to quantifications over distinguished positions and replacing all tests $P_b(x)$ by $\alpha_b(x)$. It is immediate from Claim 8 that ψ defines $\eta^{-1}(K)$.

3.2 Proof of Lemma 7

We have to show that for every $s \in M$, $\beta^{-1}(s) \subseteq B^*$ coincides over well-formed words with a language definable in $\mathrm{FO}^2(<)$. The proof requires to consider words in B^* that are slightly more general than well-formed words. They correspond to infixes of well-formed words:

A word $w \in B^*$ is pseudo well-formed if either $w = \varepsilon$ or $w = (e_0, s_0, f_0) \cdots (e_n, s_n, f_n) \in B^+$ where for all $i < n - 1$, $f_i = e_{i+1} \in E(S)$. Observe that here is no constraint on e_0 and f_n, they may be any element in $E(S) \cup \{\Box\}$. We call e_0 the left guard of w and f_n its right guard (they are undefined if $w = \varepsilon$).

We now present three sets of pseudo well-formed words that we shall use in the proof. Consider two elements $e, f \in E(S) \cup \{\Box\}$ and a sub-alphabet $C \subseteq B$. We define three sets of words in C^*: $P^C[e]$, $S^C[f]$ and $T^C[e, f]$:

- If $e \in E(S)$ then $P^C[e]$ contains the empty word ϵ and all pseudo-well words whose right guard is e. If $e = \Box$, then $P^C[\Box] = \{\varepsilon\}$.
- If $e \in E(S)$ then $S^C[f]$ contains the empty word ϵ and all pseudo-well words whose left guard is f. If $e = \Box$ then $S^C[\Box] = \{\varepsilon\}$.
- $T^C[e, f]$ contains all non-empty pseudo well-formed words with left guard e and right guard f. Additionally, if $e = f \neq \Box$, then we add the empty word ε to $T^C[e, f]$.

Observe that by definition, $T^B[\Box, \Box]$ is the set of all well-formed words in B^*.

We may now come back to the proof of Lemma 7. Consider $C \subseteq B$ and $t_1, t_2, s \in M$. We define,

$$L_s^C[t_1, t_2] = \{u \in C^* \mid t_1 \cdot \beta(u) \cdot t_2 = s\}$$

Observe that for all $e \in E(S) \cup \{\Box\}$, $1_M = \beta(\epsilon) \in P^C(e)$. Observe also that $L_s^B[1_M, 1_M] = \beta^{-1}(s)$. We prove Lemma 7 as a corollary of the following lemma which we prove by induction.

Lemma 9. *Let $C \subseteq B$. Consider $e_1, e_2 \in E(S) \cup \{\Box\}$, $t_1 \in \beta(P^C[e_1])$, $t_2 \in \beta(S^C[e_2])$. For every $s \in M$. There exists $K \subseteq C^*$ definable in $\mathrm{FO}^2(<)$ which coincides with $L_s^C[t_1, t_2]$ over $T^C[e_1, e_2]$.*

Before we prove Lemma 9, we use it to finish the main argument for Lemma 7. Consider $s \in M$. We apply the lemma in the case when $C = B$, $e_1 = e_2 = \Box$, and $t_1 = t_2 = 1_M$. This yields $K \subseteq B^*$ definable in $\mathrm{FO}^2(<)$ which coincides with $L_s^B[1_M, 1_M]$ over $T^B[\Box, \Box]$. This exactly says that $K \subseteq B^*$ is definable in $\mathrm{FO}^2(<)$ and coincides with $\beta^{-1}(s)$ over well-formed words, concluding the proof of Lemma 7.

We now concentrate on proving Lemma 9. We fix $C \subseteq B$, $e_1, e_2 \in E(S) \cup \{\Box\}$, $t_1 \in \beta(P^C[e_1])$, $t_2 \in \beta(S^C[e_2])$. Finally let $s \in M$. We have to construct the language $K \subseteq C^*$ described in the lemma. The argument is an induction on the three following parameters listed by order of importance:

1. $|C|$.
2. $|t_1 M|$.
3. $|M t_2|$.

We distinguish two cases based on the following definitions.

- We say that t_1 is left saturated when for every $f \in E(S) \cup \{\Box\}$ and every $u \in T^C[e_1, f]$, $t_1 \in t_1 \beta(u) M$.
- We say that t_2 is right saturated when for every $f \in E(S) \cup \{\Box\}$ and every $u \in T^C[f, e_2]$, $t_2 \in M \beta(u) t_2$.

We start with the base which happens when t_1 and t_2 are respectively left and right saturated. Then, we use induction to handle the case when either t_1 is not left saturated or t_2 is not right saturated.

Base case: t_1 is left saturated and t_2 is right saturated. We use our hypothesis to prove the following lemma:

Lemma 10. *There exists $r \in M$ such that for $t_1 \beta(w) t_2 = r$ for every $w \in T^C[e_1, e_2]$.*

Before we prove the lemma, let us use it to conclude the base case. We let $r \in M$ be as defined in Lemma 10. If $r = s$, we define $K = C^*$ and if $r \neq s$, we define $K = \emptyset$. Clearly, K is $\mathrm{FO}^2(<)$-definable in both cases. Moreover, by definition of r in the lemma, it is immediate that,

$$L_s^C[t_1, t_2] \cap T^C[e_1, e_2] = K \cap T^C[e_1, e_2]$$

This exactly says that K coincides with $L_s^C[t_1, t_2]$ over $T^C[e_1, e_2]$, finishing the proof. It remains to prove Lemma 10.

Proof of Lemma 10. We show that for every $w, w' \in T^C[e_1, e_2]$, we have $t_1 \beta(w) t_2 = t_1 \beta(w') t_2$. This clearly implies the lemma.

Recall that by definition $t_1 \in \beta(P^C[e_1])$, $t_2 \in \beta(S^C[e_2])$. Hence, there exists $v_1 \in P^C[e_1]$ and $v_2 \in S^C[e_2]$ such that $t_1 = \beta(v_1)$ and $t_2 = \beta(v_2)$. This yields $f, f' \in E(S) \cup \{\Box\}$ such that $v_1 w' \in T^C[f, e_2]$ and $w v_2 \in T^C[e_1, f']$.

Since t_1 and t_2 are right and left saturated respectively, it follows that $t_1 \in t_1\beta(wv_2)M = t_1\beta(w)t_2M$ and $t_2 \in M\beta(v_1w')t_2 = Mt_1\beta(w')t_2$. This yields $x, y \in M$ such that $t_1\beta(w')t_2 = t_1\beta(w)t_2x$ and $t_1\beta(w')t_2 = yt_1\beta(w)t_2$. We now obtain,

$$\begin{array}{rcll} t_1\beta(w)t_2 & = & yt_1\beta(w)t_2x & \\ & = & y^\omega t_1\beta(w)t_2x^\omega & \\ & = & y^\omega t_1\beta(w)t_2x^{\omega+1} & \text{as (1) implies } x^{\omega+1} = x^\omega \\ & = & t_1\beta(w)t_2x & \\ & = & t_1\beta(w')t_2 & \text{by definition of } x \end{array}$$

This concludes the proof. □

Induction step: Either t_1 is not left saturated or t_2 is not right saturated. We assume that t_1 is not left saturated (the other case is symmetrical). We use induction on the first and second parameters (note that induction on the third parameter is used in the symmetrical case). First, we use our hypothesis to prove the following fact.

Lemma 11. *There exists $c = (e, x, f) \in C$ such that for every $v \in C^*$ satisfying $vc \in T^C[e_1, f]$, $t_1 \notin t_1\beta(vc)M$.*

Proof. By hypothesis, t_1 is not left saturated. Hence, there exists $u \in T^C[e_1, f]$ for some $f \in E(S) \cup \{\Box\}$ such that $t_1 \notin t_1\beta(u)M$. Note that u has to be non-empty (clearly, $t_1 \in t_1M$). Finally, we may choose u of minimal length: $u = u'c$ with $c = (e, x, f) \in C$ and $t_1 \in t_1\beta(u')M$. It remains to show that $c \in C$ satisfies the desired property. Consider $v \in C^*$ such that $vc \in T^C[e_1, f]$, we have to show that $t_1 \notin t_1\beta(vc)M$. There are two cases depending on whether $e \in E(S)$ or $e = \{\Box\}$.

If $e = \Box$, then, $u'c = u \in T^C[e_1, f]$ and $vc \in T^C[e_1, f]$ imply that $u' = v = \varepsilon$ and $e_1 = \Box$. Hence $vc = u$ and we get by definition of u that $t_1 \notin t_1\beta(vc)M$. We turn to the case when $e \in E(S)$. We proceed by contradiction: assume that $t_1 \in t_1\beta(vc)M$. This yields $r \in M$ such that $t_1 = t_1\beta(vc)r$. We have the following fact,

Fact 12. *There exists an idempotent $g \in E(S)$ such that $g\beta(c) = \beta(c)$ and $t_1\beta(u')g = t_1\beta(u')$.*

Proof. There are two cases depending on whether $t_1\beta(u') = 1_M$ or not. In the former case, we get $1_M = t_1\beta(vc)r\beta(u')$. Clearly $t_1\beta(vc)r\beta(u') \in S$ since $\beta(c) \in S$ as $e \in E(S)$. Hence, $1_M \in E(S)$ and it suffices to choose $g = 1_M$.

We now assume that $t_1\beta(u') \neq 1_M$. We choose $g = e \in E(S)$ Clearly, $e\beta(c) = \beta(c)$ since $c = (e, x, f)$. Moreover, we have $t_1 \in \beta(P^C[e_1])$ by definition and $u'c = u \in T^C[e_1, f]$. This yields, $t_1\beta(u') \in \beta(P^C[e])$ and since $t_1\beta(u') \neq 1_M$ this implies $t_1\beta(u')e = t_1\beta(u')$. □

We may now finish the proof. Recall that $t_1 \in t_1\beta(u')M$ by hypothesis which yields $r' \in M$ such that $t_1 = t_1\beta(u')r'$. Since we also have $t_1 = t_1\beta(vc)r$, this yields the following,

$$\begin{array}{rcll} t_1\beta(u') & = & t_1\beta(u')r'\beta(vc)r\beta(u') & \\ & = & t_1\beta(u')gr'\beta(v)g\beta(c)r\beta(u')g & \text{Using Fact 12} \\ & = & t_1\beta(u')(gr'\beta(v)g\beta(c)r\beta(u')g)^\omega & \\ & = & t_1\beta(u')\beta(c)r\beta(u')(gr'\beta(v)g\beta(c)r\beta(u')g)^\omega & \text{Using (1)} \end{array}$$

Consequently, we get $y \in M$ such that $t_1\beta(u') = t_1\beta(u'c)y = t_1\beta(u)y$. Since $t_1 = t_1\beta(u')r'$, we then obtain $t_1 = t_1\beta(u)yr'$. Hence, $t_1 \in t_1\beta(u)M$ which contradicts the definition of u. □

We may now finish the proof. We first use induction to build several $\mathrm{FO}^2(<)$-definable languages. We then combine them into another $\mathrm{FO}^2(<)$-definable language K that coincides with $L_s^C[t_1, t_2]$ over $T^C[e_1, e_2]$ as desired.

Let $D = C \setminus \{c\}$. We first handle the words in D^*: we build a language $H \subseteq D^*$ which coincides with $L_s^C[t_1, t_2]$ over $T^D[e_1, e_2]$. For every $r \in M$, induction on our first parameter (the

size of C) yields a language $H_r \subseteq D^*$ definable in $\mathrm{FO}^2(<)$ which coincides with $L_r^D[1_M, 1_M]$ over $T^D[e_1, e_2]$. We define,

$$H = \bigcup_{\{r \in M \mid t_1 r t_2 = s\}} H_r$$

Clearly, $H \subseteq D^*$ is definable in $\mathrm{FO}^2(<)$ by Lemma 1. Moreover, one may verify the following fact from the definition.

Fact 13. *H coincides with $L_s^C[t_1, t_2]$ over $T^D[e_1, e_2]$.*

We now take care of the words in $C^* \setminus D^*$ (i.e. the ones that contain at least one letter "c"). Recall that $c = (e, x, f)$.

Let $R \subseteq M$ be as follows:

$$R = \{\beta(v) \mid v \in C^* \text{ and } vc \in T^C[e_1, f]\}$$

For every $r \in R$, induction on our first parameter (the size of C), yields a language $U_r \subseteq D^*$ definable in $\mathrm{FO}^2(<)$ which coincides with $L_r^D[1_M, 1_M]$ over $T^D[e_1, e]$.

Moreover, by Lemma 11, we know that for every $r \in R$, $t_1 \notin t_1 r \beta(c) M$. Clearly, this yields that $|t_1 r \beta(c) M| < |t_1 M|$. Hence, induction on our second parameter (the size of $t_1 M$) yields a language $V_r \subseteq C^*$ definable in $\mathrm{FO}^2(<)$ which coincides with $L_s^C[t_1 r \beta(c), t_2]$ over $T^C[f, e_2]$.

We are now ready to define the language $K \subseteq C^*$ described in Lemma 9. We let,

$$K = H \cup \bigcup_{r \in R} U_r c V_r$$

Let us first explain why K is definable in $\mathrm{FO}^2(<)$. By Lemma 1, it suffices to show that every language in the union is definable in $\mathrm{FO}^2(<)$. We already know this for H. Moreover, given $r \in R$, U_r, V_r are definable in $\mathrm{FO}^2(<)$ by definition and $U_r \subseteq D^*$ with $c \notin D$. Hence, Lemma 2 yields that $U_r c V_r$ is definable in $\mathrm{FO}^2(<)$. Altogether, we get that K is definable in $\mathrm{FO}^2(<)$.

It remains to verify that K coincides with $L_s^C[t_1, t_2]$ over $T^C[e_1, e_2]$. Hence, we fix $w \in T^C[e_1, e_2]$ and show that $w \in K$ if and only if $w \in L_s^C[t_1, t_2]$.

Assume first that $w \in K$. We show that $w \in L_s^C[t_1, t_2]$. If $w \in H \subseteq D^*$, this is immediate by Fact 13. Otherwise, $w \in U_r c V_r$ for some $r \in R$. Hence, $w = w_1 c w_2$ with $w_1 \in U_r \subseteq D^*$ and $w_2 \in V_r$. Since $c = (e, x, f)$ and $w \in T^C[e_1, e_2]$, it is immediate that $w_1 \in T^D[e_1, e]$ and $w_2 \in T^C[f, e_2]$. Therefore, by definition of U_r and V_r, we get that $w_1 \in L_r^D[1_M, 1_M]$ (i.e. $\beta(w_1) = r$) and $w_2 \in L_s^C[t_1 r \beta(c), t_2]$ (i.e. $t_1 r \beta(c) \beta(w_2) t_2 = s$). Altogether, this yields,

$$t_1 \beta(w) t_2 = t_1 \beta(w_1) \beta(c) \beta(w_2) t_2 = t_1 r \beta(c) \beta(w_2) t_2 = s$$

Hence, $w \in L_s^C[t_1, t_2]$ by definition.

Assume now that $w \in L_s^C[t_1, t_2]$. We show that $w \in K$. If $w \in D^*$, it is immediate from Fact 13 that $w \in H \subseteq K$. Otherwise, w contains the letter c: $w = w_1 c w_2$ with $w_1 \in D^*$ and $w_2 \in C^*$ (i.e. the highlighted c is the leftmost one in w). Since $w \in T^C[e_1, e_2]$ and $c = (e, x, f)$, this yields $w_1 \in T^D[e_1, e]$, $w_1 c \in T^C[e_1, f]$ and $w_2 \in T^C[f, e_2]$. In particular, $w_1 c \in T^C[e_1, f]$ means that $\beta(w_1) = r \in R$ by definition. Hence, $w_1 \in L_r^D[1_M, 1_M]$ which yields $w_1 \in U_r$ by definition of U_r since $w_1 \in T^D[e_1, e]$. Moreover, since $w \in L_s^C[t_1, t_2]$, we have $t_1 \beta(w) t_2 = s$ which yields $t_1 r \beta(c) \beta(w_2) t_2 = s$. Consequently $w_2 \in L_s^C[t_1 r \beta(c), t_2]$ which yields $w_2 \in V_r$ by definition of V_r since $w_2 \in T^C[f, e_2]$. Altogether, we obtain $w = w_1 c w_2 \in H_r c V_r \subseteq K$ which concludes the proof.

4 Proof of necessity of (1)

The proof of Proposition 4 is a simple classical Ehrenfeucht-Fraïssé argument. We include a sketch below for completeness. We begin with the definition of the Ehrenfeucht-Fraïssé game associated to $\mathrm{FO}^2(<, +1)$.

There are two players, Duplicator and Spoiler and the board consists in two words and a number k of rounds that is fixed in advance. At any time during the game there is one pebble placed on a position of one word and one pebble placed on a position of the other word and both positions have the same label. If the initial position is not specified, the game starts with the two pebbles placed on the first position of each word. Each round starts with Spoiler moving one of the pebbles inside its word from its original position x to a new position y. Duplicator must answer by moving the pebble in the other word from its original position x' to a new position y'. Moreover, the positions x' and y' must satisfy the same atomic formulas as x and y, i.e. the same predicates among $<$, $+1$ and the label predicates.

If at some point Duplicator cannot answer Spoiler's move, then Spoiler wins the game. If Duplicator is able to respond to all k moves of Spoiler then she wins the game. Winning strategies are defined as usual. If Duplicator has a winning strategy for the k-round game played on the words w, w' then we say that w and w' are k-equivalent and denote this by $w \simeq_k^+ w'$. The following result is classical and simple to prove.

Lemma 14 (Folklore)**.** *If L is definable in $\mathrm{FO}^2(<,+1)$ then there is a k such that $w \simeq_k^+ w'$ implies $w \in L$ if and only if $w' \in L$.*

We can now use Lemma 14 to prove Proposition 4.

Proof of Proposition 4. Let L be a language definable in $\mathrm{FO}^2(<,+1)$. Let $\alpha : A^* \to M$ its syntactic morphism and $S = \alpha(A^+)$ its syntactic semigroup. Let s, t and e be elements of S with e idempotent. Let U, V, E be non-empty words such that $s = \alpha(U)$, $t = \alpha(V)$, $e = \alpha(E)$. For all $k \in \mathbb{N}$, let w_k be the word $(E^kUE^kVE^k)^{k\omega}$ and let w'_k be the word $(E^kUE^kVE^k)^{k\omega}V(E^kUE^kVE^k)^{k\omega}$. Note that for all k, $\alpha(w_k)$ is $(esete)^\omega$ while $\alpha(w'_k)$ is $(esete)^\omega t(esete)^\omega$.

In view of Lemma 14, it is enough for each number k and each words u_ℓ, u_r, to give a winning strategy for Duplicator in the k-move Ehrenfeucht-Fraïssé game played on $u_\ell w_k u_r$ and $u_\ell w'_k u_r$.

This is done by induction on the number i of remaining moves. At each step of the game one pebble is at position x of $u_\ell w_k u_r$ and another one is at position x' of $u_\ell w'_k u_r$. The inductive hypothesis $H(i)$ that Duplicator maintains is:

1. x and x' have the same label.
2. If x is in a copy of E (resp. u_ℓ, u_r, U, V) then x' is in a copy of E (resp. u_ℓ, u_r, U, V) at the same relative position as x.
3. If x has less than i blocks $(E^kUE^kVE^k)$ to its left (resp. to its right) then x' is at the same distance as x from the beginning of the word (resp. from the end of the word).

It is immediate to check that $H(i)$ holds at the beginning of the game. It is also simple to verify that this inductive hypothesis can be maintained during k moves of the game. □

5 Conclusion

We have shown that languages definable in $\mathrm{FO}^2(<,+1)$ are exactly those whose syntactic semigroup satisfies $(esete)^\omega t(esete)^\omega = (esete)^\omega$. In other words and with abuse of notations we have shown that $\mathrm{FO}^2(<,+1) = \mathbf{LDA}$.

Recall from [7] that languages definable in $\mathrm{FO}^2(<)$ are exactly those whose syntactic semigroup is in the variety $\mathbf{DA}$. From this and a "wreath product argument", essentially Lemma 6, it follows that languages definable in $\mathrm{FO}^2(<,+1)$ are exactly those whose syntactic semigroup is in $\mathbf{DA} * \mathbf{D}$.

Therefore it follows from our result that $\mathbf{DA} * \mathbf{D} = \mathbf{LDA}$. This in turns is equivalent to the locality of $\mathbf{DA}$ (see for example [8]).

References

[1] Jorge Almeida. A syntactical proof of locality of **DA**. *International Journal of Algebra and Computation*, 6(2):165–177, 1996.

[2] Karl Auinger. On the decidability of membership in the global of a monoid pseudovariety. *Intl. Journal of Algebra and Computation (IJAC)*, 20(2):181–188, 2010.

[3] Volker Diekert and Manfred Kufleitner. On First-Order Fragments for Words and Mazurkiewicz Traces. In *Intl. Conf. on Developments in Language Theory (DLT)*, pages 1–19, 2007.

[4] Robert McNaughton and Seymour Papert. *Counter-Free Automata*. MIT Press, 1971.

[5] Marcel Paul Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8:190–194, 1965.

[6] Howard Straubing. Finite semigroup varieties of the form V*D. *Journal of Pure and Applied Algebra*, 36:53–94, 1985.

[7] Denis Thérien and Thomas Wilke. Over words, two variables are as powerful as one quantifier alternation. In *Symp. on the Theory of Computing (STOC)*, pages 234–240, 1998.

[8] Bret Tilson. Categories as algebra: An essential ingredient in the theory of monoids. *Journal of Pure and Applied Algebra*, 48(1-2):83–198, 1987.