Two-Variable Logic over Countable Linear Orderings

Amaldev Manuel[1] **and A. V. Sreejith**[2]

1 **Chennai Mathematical Institute (CMI), Chennai, India**
amal@cmi.ac.in
2 **Chennai Mathematical Institute (CMI), Chennai, India**
sreejithav@cmi.ac.in

Abstract

We study the class of languages of finitely-labelled countable linear orderings definable in two-variable first-order logic. We give a number of characterisations, in particular an algebraic one in terms of circle monoids, using equations. This generalises the corresponding characterisation, namely variety DA, over finite words to the countable case. A corollary is that the membership in this class is decidable: for instance given an MSO formula it is possible to check if there is an equivalent two-variable logic formula over countable linear orderings. In addition, we prove that the satisfiability problems for two-variable logic over arbitrary, countable, and scattered linear orderings are NEXPTIME-complete.

1998 ACM Subject Classification F.4.3 Formal Languages

Keywords and phrases $\circ$-monoids, countable linear orderings, FO^2

Digital Object Identifier 10.4230/LIPIcs.MFCS.2016.66

1 Introduction

Countable linear orderings are linear orderings over countable domains. They are of primary interest in the context of satisfiability of logics due to a result of Shelah [24]: the satisfiability problem of monadic second-order (MSO) logic is undecidable over arbitrary linear orderings, and in particular over the Reals. But by Rabin's theorem [18] the problem remains decidable when considered over countable linear orderings. Thus the class of countable linear orderings sets a natural limit to the decidability of satisfiability problem for MSO over linear orderings. This is in sharp contrast with first-order (FO) logic, that has the corresponding question decidable over arbitrary linear orderings. A second and perhaps more important reason why the class of countable linear orderings are interesting is the logic-algebra connection on its subclasses – MSO definable languages over finite words (*resp.* ω-words) are precisely the class of languages definable by finite monoids (*resp.* ω-semigroups, equivalently Wilke algebras) – extends to countable linear orderings: the result due to Carton-Colcombet-Puppis [4] states that MSO definable languages of countable linear orderings are precisely the class of languages of countable linear orderings recognisable by $\circ$-monoids (recalled in the next section).

The principal import of such a connection is well displayed by the seminal theorem of Schützenberger [21]: over finite words, FO definable languages are precisely the languages recognisable by aperiodic finite monoids, in particular the syntactic monoids of FO definable languages are aperiodic. This immediately yields the decidability of membership in the class of FO definable languages: compute the syntactic monoid of the given language and check if

it is aperiodic. Since the time of Schützenberger numerous logics have been characterised algebraically, over finite words, ω-words etc.

However, unlike finite words or ω-words, characterising a logic over countable linear orderings has the following added advantage: An algebraic, in particular decidable, characterisation of a class of languages of countable linear orderings (for instance languages definable by FO) in terms of $\circ$-monoids, immediately provides decidable characterisations over restricted classes of countable linear orderings that are equationally definable (for instance finite words, ω-words, bi-infinite words, rationals etc.). In that sense, characterising a logic algebraically over the class of countable linear orderings in *one shot* characterises it over all equationally definable subclasses.

An elaborate study over a variety of sublogics over countable linear orderings was done in [6] where FO, FO[cut], WMSO, WMSO[cut], MSO[ordinals], MSO[scattered] etc. were characterised algebraically. These characterisations show that WMSO with "cut" quantifiers are equivalent to those with "ordinal" quantifiers, whereas the rest of the logics are expressively different from each other. The study also gives decidability of membership for all these logics.

As a continuation, in this work we consider the class of languages of countable linear orderings that are definable in two-variable first-order logic (FO^2). Two-variable FO is the fragment of FO with at most two variables x, y. While over abritrary structures FO has an undecidable satisfiable problem, FO^2 has a decidable, low complexity satisfiability problem. Yet FO^2 is expressive enough to contain modal logics. This feature of FO^2 has been thoroughly studied and the decidability of satisfiability has been extended to special classes of structures as well as particular vocabularies. FO^2 has been of significant interest over words (and ω-words) as well. Over finite words, FO^2 definable languages have numerous characterisations [26, 25]: they are precisely the class of languages (1) definable in unary LTL [26, 8], (2) recognisable by 2-way partially ordered DFA [22], (3) definable by turtle expressions [27], and (4) whose syntactic monoids are in the variety DA [26] (a finite monoid is in DA if it is aperiodic and all its regular D-classes are subsemigroups) etc. The last characterisation also gives a decision procedure for membership in the class. Not only that FO^2 languages have numerous characterisations, they also have a rich structure inside them [17]– they form an infinite hierarchy under quantifier alternations that is also decidable as shown recently [12].

Though FO^2 is well understood algebraically over finite words, its algebraic characterisation over countable orderings, in particular over infinite ones, is not immediate. This is because even with two variables one can express a variety of "infinitary" conditions: clearly with two variables we can express that letter a has a minimum occurrence (for instance by the formula $\varphi_1 = \exists y \forall x \, (a(x) \wedge a(y) \wedge x \geq y)$), as well as its negation, that is there is an infinite descending chain of a's. Consider the following formula φ_2 that says that if an a-position has an a-position before it, then it has two a-positions before it.

$$\varphi_2 = \forall x \, (a(x) \wedge \exists y \ (a(y) \wedge x > y) \rightarrow \exists y \, (a(y) \wedge x > y \wedge \exists x \, (a(x) \wedge y > x)))$$

The word aa, as well as a^{ω^*} (the ordering $(\mathbb{Z}^-, <)$ labelled with a) does not satisfy $\varphi_1 \wedge \varphi_2$ while the words a and aa^{ω^*} satisfy $\varphi_1 \wedge \varphi_2$. Thus, as $\varphi_1 \wedge \varphi_2$ exemplifies, with two variables one can stipulate both a minimum occurrence as well as existence of a descending chain of a letter. Therefore for the algebraic characterisation of FO^2 one has to make an intricate analysis of whether the letters appear as a minimum or as an infinite chain at different factors of the word.

In the rest of the section, we mention works that are related to the present paper and our contributions.

Related Work

Algebraic characterisations, in particular for FO, for scattered linear orderings are given in [1, 2, 5]. The connection between MSO over countable linear orderings and $\circ$-monoids was proved in [4]. It showed that MSO is equivalent to $\circ$-monoids. This gives an alternate proof of decidability of MSO over countable linear orderings. Moreover it showed that MSO collapses to the second level of the quantifier alternation hierarchy. An algebraic classification of MSO under various forms of set quantifications, in particular corresponding to the sublogics FO, FO[cut], WMSO, WMSO[cut], MSO[ordinals], MSO[scattered], was done in [6].

The literature on FO^2 over arbitrary structures is extensive and we don't mention it here. FO^2 over finite words as well as ω-words has been studied extensively [22, 26, 8, 25, 27, 12, 17]. A survey of various characterisations of FO^2 is given in [25]. The quantifier alternation hierarchy on FO^2 was proved in [11] and the decidability of the hierarchy was shown in [12].

Satisfiability of FO^2 over arbitrary structures were shown to be NEXPTIME-complete in [10]. The corresponding results (also NEXPTIME-complete) was shown for ω-words in [8], and for ordinals in [15]. More recently the satisfiability problem was studied for words with additional linear orderings/preorderings [3, 23, 14, 13].

Satisfiability of LTL over countable linear orderings is PSPACE-complete [7, 19].

Contributions

We study the two variable fragment of first order logic over countable linear orderings and give a number of different characterisations. The simplest characterisation is in terms of temporal logic (TL): FO^2 is equivalent to TL with only the modalities *Future* (F) and *Past* (P). Our major contribution is an algebraic characterisation for FO^2. We show that it corresponds to a subclass of $\circ$-monoids and give two algebraic characterisations for this subclass: (1) by equations, and (2) as the class of $\circ$-monoids that are aperiodic and whose regular $\mathcal{J}$ classes are sub $\circ$-monoids. It follows that the membership in the class is decidable.

Next we study the satisfiability problem for FO^2 over countable linear orderings. The models of FO^2 formulas could be infinite, but we show that a satisfiable formula always admits a scattered model that has a finite representation of small (exponential in the size of the formula) size. Thus we prove that the satisfiability of FO^2 over countable linear orderings is NEXPTIME-complete. From this we also deduce that the satisfiability problems for FO^2 over arbitrary and scattered orderings are NEXPTIME-complete.

Structure of the paper

In Section 2, we introduce words over countable linear orderings, two-variable first-order logic, and the algebra required to characterise FO^2, namely $\circ$-monoids. In Section 3 we prove our main result (Theorem 8) which characterises FO^2. Section 4 deals with the satisfiability of FO^2 over countable linear orderings. Finally we conclude our results in Section 5.

2 Preliminaries

In this section we recall the basic facts about (countable) linear orderings, $\circ$-monoids, logics and related notions.

Words over countable linear orderings. A *linear ordering* $\alpha = (Z, <)$ is a set Z equipped with a total order $<$. For $X, Y \subseteq Z$ we write $X < Y$ if $x < y$ for each x in X and y in Y. In particular $\emptyset < X < \emptyset$ for any set X. Also if $X < Y$, $Y < Z$ and Y is nonempty, then

$X < Z$. A *cut* of the linear ordering α is a pair (Z_1, Z_2) such that $Z = Z_1 \cup Z_2$ and $Z_1 < Z_2$. The set of all cuts are linearly ordered and has the least upper bound property [2]. A set L is a *prefix* of X if $X = L \cup K$ and $L < K$ for some $K \subseteq X$. Similarly if $X = L \cup K$ and $L < K$, then K is a *suffix* of X. Element $z \in Z$ is an *upperbound* (*resp. lowerbound*) of a set $X \subseteq Z$ if $x \leq z$ (*resp.* $z \leq x$) for each x in X. A set X is *right-open* (*resp. left-open*) if it has no maximum element (*resp.* minimum element). Nonempty suffixes of right-open sets are right-open and nonempty prefixes of left-open sets are left-open. The set X is *dense* if between any two elements in the set there is another element; set X is *scattered* if it has no dense subsets. An ordering is a *countable* (scattered) linear ordering if the set Z is countable (scattered). See [20] for further details.

For a finite alphabet A and a linear ordering $\alpha = (Z, <)$, we define a *word* $w : \alpha \to A$ to be a mapping from the set Z to A. We call α the *domain* of w, $dom(w)$. For a word w, we say a point/position x to denote an element $x \in dom(w)$. The notation $w[x]$ denote the letter at the x^{th} position in w. A word has a minimal (respectively maximal) element if its domain has a minimal (maximal) element. The word u is a suffix (prefix) of w if $dom(u)$ is a suffix (prefix) of $dom(w)$. If u and v are words, then uv denotes the unique word w such that $(dom(u), dom(v))$ is a cut of $dom(w)$. This operation is naturally extended to a set of words $\{w_i\}_\alpha$ indexed by a linear ordering α as $\prod_{i\in\alpha} w_i$ (see [6] for more details). For a set $S \subseteq A$, and a word w, we denote the restriction of w to the positions labelled by S as $w_{|S}$. That is $w_{|S} = \{i \in dom(w) \mid w[i] \in S\}$.

The following words are of special interest. ϵ stands for the empty word (the word over an empty domain). The word $\{a\}^\omega$ (denoted in short as a^ω) denotes the word over the domain $(\mathbb{N}, <)$ such that every position is mapped to the letter a. Similarly a^{ω^*} denotes the word over the domain $(\mathbb{N}^-, <)$ where every position is mapped to letter a. A *perfect shuffle* over a nonempty set $S \subseteq A$ of letters, denoted by S^η, is the word over domain $(\mathbb{Q}, <)$ such that any nonempty open interval contains each of the letters in S. This is a unique word (up to isomorphism) (see [4]) and is an example of a dense word, i.e. a word whose domain is dense.

For an alphabet A, the set of all words over nonempty countable domains is denoted by A°. For a word w, we define $alphabet(w)$ to be the set of all letters in w. A *language* over the alphabet A is a subset of A°. The language $\{a\}^\infty \subseteq \{a\}^\circ$ (or written as a^∞) denotes all words which are right open. Similarly for a set $S \subseteq A$, the language S^∞ is the set of all words whose letters come only from S and any letter from S can be seen arbitrarily towards the right. The sets $a^{-\infty}$ and $S^{-\infty}$ are defined analogously.

Circle monoids and algebras. A $\circ$-*semigroup* $\mathbf{M} = (M, \pi)$ consists of a set M with an operation $\pi : M^\circ \to M$ which satisfies the following two properties (1) $\pi(a) = a$ for all $a \in M$, (2) *generalised associativity property* – that is $\pi\big(\prod_{i\in\alpha} u_i\big) = \pi\big(\prod_{i\in\alpha} \pi(u_i)\big)$ for every countable linear ordering α. If $\mathbf{M}$ has an identity element, then it is called a $\circ$-*monoid*. An element $e \in \mathbf{M}$ is an *idempotent* if $\pi(ee) = e$.

For the rest of the paper, we assume that the monoid $\mathbf{M}$ is finite, that is M is a finite set. The product π is over countable linear orderings and hence it is not possible to finitely represent π. Fortunately, we are able to represent this by a $\circ$-algebra that uses only finite sets and finitely many operations. The following operations are derivable from a $\circ$-monoid $\mathbf{M} = (M, \pi)$:

- *Finite product*, $\cdot : M^2 \to M$ such that $\cdot(a, b) = \pi(ab)$
- *Omega*, $\omega : M \to M$ such that $\omega(a) = \pi(a^\omega)$
- *Omega**, $\omega^* : M \to M$ such that $\omega^*(a) = \pi(a^{\omega^*})$
- *Shuffle*, $\eta : \mathcal{P}(M) \to M$ such that $\{a_1, \ldots, a_k\}^\eta = \pi(\{a_1, \ldots, a_k\}^\eta)$

The resulting structure $(M, \cdot, \omega, \omega^*, \eta)$ is called a $\circ$-*algebra* if it satisfies some additional axioms relating the operations (for example $a \cdot a^\omega = a^\omega$, $(a^\eta)^\omega = a^\eta$ etc.). We skip these details and refer the reader to the paper by Carton et. al [4] for a detailed discussion. The relavant fact is that, for any $\circ$-monoid there exists a unique $\circ$-algebra and vice versa [4].

An important "tool" to understand finite monoids (in our case $\circ$-monoids) is *Green's relations*. In a $\circ$-monoid $\mathbf{M}$, we say that two elements $u \geq_{\mathcal{J}} v$ if there exists two elements $x, y \in \mathbf{M}$ such that $v = xuy$ and $u\mathcal{J}v$ (called J equivalent) if it is both $u \geq_{\mathcal{J}} v$ and $v \geq_{\mathcal{J}} u$. We also say that two elements are $u \geq_{\mathcal{R}} v$ (similarly $u \geq_{\mathcal{L}} v$) if there exists an element $x \in \mathbf{M}$ such that $v = ux$ ($v = xu$). Also $u\mathcal{R}v$ if $u \geq_{\mathcal{R}} v$ and $v \geq_{\mathcal{R}} u$. Similarly we can define $u\mathcal{L}v$. The relations $\mathcal{L}$ and $\mathcal{R}$ are right and left congruences respectively. If a $\mathcal{J}$ class contains an idempotent then it is called a *regular* $\mathcal{J}$ class. All elements in a $\mathcal{J}$ class can be described by an "eggbox" structure, such that $u\mathcal{J}v$ iff there exists elements $x, y \in \mathbf{M}$ such that $u\mathcal{R}x\mathcal{L}y\mathcal{R}v$. For a more detailed elaboration on this subject see [16].

The class of $\circ$-monoids that satisfies the property – there exists an $n \in \mathbb{N}$ such that $a^n = a^{n+1}$ for all $a \in \mathbf{M}$ – are called *aperiodic*. It is precisely the class of $\circ$-monoids which do not contain any non-trivial group as a subsemigroup of $(M, \cdot)$ (by Schützenberger's theorem [21]).

One way to denote a class of $\circ$-monoids is by equations. For instance, we say that $\mathbf{M}$ satisfies the equation $x^* = x^\omega x^{\omega^*}$, if for all elements $a \in \mathbf{M}$, $a^* = a^\omega a^{\omega^*}$, where a^* is the unique idempotent power of a.

We say that a language $L \subseteq A^\circ$ is recognised by the $\circ$-monoid $\mathbf{M}$, if there is a morphism, $\gamma : A^\circ \to \mathbf{M}$ and a subset $S \subseteq \mathbf{M}$ such that $L = \gamma^{-1}(S)$. The *syntactic* $\circ$-*monoid* of a language L is the minimal $\circ$-monoid $\mathbf{M}$ recognising L that has the following universal property: any $\circ$-monoid recognising L has a morphism onto $\mathbf{M}$.

Logics. Monadic second-order logic (MSO) over a finite alphabet A is a logic which can be inductively built using the following operations.

$$a(x) \mid x < y \mid x = y \mid \alpha_1 \vee \alpha_2 \mid \neg\alpha \mid x \in X \mid \exists x\ \alpha \mid \exists X\ \alpha$$

Here $a \in A$. If we remove the second-order quantification, we get first-order logic (FO). If we further restrict the logic to use only two variables (but allowing repetitions) we get FO^2. Note that, we do not have the *successor* relation in our logic.

A formula with no free variables is called a sentence. The language of a sentence φ (denoted by $L(\varphi)$) is the set of all $u \in A^\circ$ that satisfies φ.

Over finite words, FO^2 can talk about occurrence of letters and also about the order in which they appear [8, 27]. Over countable linear orders, FO^2 can also talk about an infinite sequence of a letter. For example, the language a^∞ is definable in FO^2 by stating that, every position is labelled by a and there is no maximum position.

$$\big(\forall x\ \exists y > x\big) \wedge \big(\forall x\ a(x)\big)$$

Also, for a subset $S \subseteq A$, we can also express the language S^∞ in FO^2.

$$\Big(\forall x \bigwedge_{a \in S} \exists y > x\ a(y)\Big) \wedge \Big(\forall x \bigvee_{a \in S} a(x)\Big)$$

Analogously, FO^2 can also talk about left open words.

The temporal logic $\{\mathtt{F}, \mathtt{P}\}$-TL over the alphabet A is the logic with the set of formulas – a when a is a letter in A, and $\mathtt{F}\varphi$ and $\mathtt{P}\varphi$ when φ is a formula – that is closed under Boolean

operations. To state the semantics fix a word $u \in A^\circ$. A position $i \in dom(u)$ satisfies – the formula a if i is labelled with the letter a, and the formula $\mathtt{F}\varphi$ (*resp.* $\mathtt{P}\varphi$) if there is a position $i < j \in dom(u)$ (*resp.* $i > j \in dom(u)$) that satisfies the formula φ. The semantics for Boolean connectives are defined in the usual way. The word u satisfies the formula φ if there is a position $i \in dom(u)$ that satisfies the formula (see [8] for a detailed presentation). The language of the formula φ is the set of all $u \in A^\circ$ that satisfies φ.

3 Characterisation

In this section, we give the algebraic characterisation for $\mathrm{FO}^2(<)$ over countable linear orderings. As we noted earlier, $\circ$-monoid captures MSO. Here we identify a subclass which will capture the two-variable first-order fragment. Our characterisation builds on the characterisation for FO^2 on finite words given in [26]. In particular, we crucially use a generalisation of the congruence given there.

▶ **Definition 1.** We define $\circ$-DA to be the subclass of $\circ$-monoids that satisfy the following equations.

1. $(xyz)^* y (xyz)^* = (xyz)^*$
2. $x^* = (x)^\omega (x)^{\omega^*}$
3. $\{x_1, \ldots, x_k\}^\eta = (x_1 \cdots x_k)^{\omega^*} (x_1 \cdots x_k)^\omega$

The first equation corresponds to the variety DA of finite monoids [25]. It identifies the constraints the product operation has to satisfy. The second equation corresponds to FO definable languages of countable linear orderings [6]. This equation states that a $\mathcal{J}$ class with an idempotent will also contain its omega and omega* powers. The last equation says that, $\circ$-DA cannot differentiate between dense and scattered orderings.

The connection between logic and algebra is established using the following congruence.

A congruence on words

Let $u \in A^\circ$ be an arbitrary word. $alphabet(u)$ is defined as the set of all letters occurring in u. For a letter a in $alphabet(u)$, let $P_u(a)$ denote the set of all positions in u labelled with a. Let $T_r^1(u) \subseteq alphabet(u)$ be the set of all letters a such that $P_u(a)$ has a maximal element. Furthermore, let $T_r^\omega(u)$ be the set $alphabet(u) \setminus T_r^1(u)$, i.e. the set of all letters that do not have a maximal occurrence. Similarly let $T_l^1(u) \subseteq alphabet(u)$ be the set of all letters a such that $P(a)$ has a minimal element, and let $T_l^{\omega^*}(u)$ be the set $alphabet(u) \setminus T_l^1(u)$.

▶ **Definition 2.** The relation $\lesssim_r$ over the set of letters $T_r^\omega(u)$ is defined as follows:

$a \lesssim_r b$ if each a-position i in u has a b-position j to its right (i.e. $j > i$).

▶ **Lemma 3.** *The relation $\lesssim_r$ is a total preorder on the set $T_r^\omega(u)$.*

We write $\sim_r$ to denote the equivalence relation associated with the preorder $\lesssim_r$. For a letter a in $T_r^\omega(u)$ we let $[a]_r \subseteq T_r^\omega(u)$ denote the equivalence class of a with respect to the total preorder $\lesssim_r$, i.e. $[a]_r = \{b \in T_r^\omega(u) : b \sim_r a\}$. Also, we extend the definition of P_u to equivalence classes by defining $P_u([a]_r) = \bigcup_{a \in [a]_r} P_u(a)$. We write $<_r$ to denote the total order on $\{[a]_r : a \in T_r^\omega(u)\}$.

By symmetry, the dual relation $\lesssim_l$ defined as,

$b \lesssim_l a$ if each a-position in u has a b-position to its left,

is also a total preorder. The corresponding equivalence relation and strict order relation are denoted as $\sim_l$ and $<_l$. Given a circle word u the preorders $\lesssim_r$ and $\lesssim_l$ associated with u are called the *right preorder* and *left preorder* of u respectively. As before we define $P_u([a]_l) = \bigcup_{a \in [a]_l} P_u(a)$.

▶ **Example 4.** Let $S = \{a, b\}$ and let $u \in S^{-\infty}$ be an arbitrary word. Consider the word $v = ua^{\omega^*}a^\omega ab^\omega \in \{a, b\}^\circ$. Then $T^1_l(u) = T^1_l(v) = \emptyset$ and $T^{\omega^*}_l(u) = T^{\omega^*}_l(v) = \{a, b\}$, since a and b occur infinitely often towards left in both u and v. It also follows that $a \lesssim_l b$ and $b \lesssim_l a$. Since u is an arbitrary word, we do not know about $T^1_r(u)$ and $T^\omega_r(u)$. But, since a has a maximum point in v, we have $T^1_r(v) = \{a\}$ and $T^\omega_r(v) = \{b\}$. Moreover $b \lesssim_r b$.

Consider another word $w = a^\omega b^\omega$. Here we have $T^1_l(w) = \{a, b\}$ and $T^{\omega^*}_l(w) = T^1_r(w) = \emptyset$. We also have $T^\omega_r(w) = \{a, b\}$ and $a \lesssim_r b$ but $b \not\lesssim_r a$.

We will now introduce left/right decomposition of words. The idea is to factorise a word in a particular way to capture the "pivot" points for an FO^2 formula.

▶ **Definition 5.** Let $a \in \mathit{alphabet}(u)$. If $a \in T^1_l(u)$, then there exists a unique factorisation of u as (u_0, a, u_1) such that $u = u_0 a u_1$ and $a \notin \mathit{alphabet}(u_0)$. This is called the a-left decomposition of u. Similarly there is a unique factorisation of u as (u_0, a, u_1) such that $a \notin \mathit{alphabet}(u_1)$, if $a \in T^1_r(u)$. This is called the a-right decomposition of u.

We are also interested in left decomposition obtained by a set of positions $P_u([a]_l)$, where $[a]_l \in T^{\omega^*}_l(u)/\sim_l$. That is for a subset of positions $P_u([a]_l)$ of u, we define the *$P_u([a]_l)$-left decomposition of a word u* to be the unique maximal cut (u_0, u_1) such that $P_u([a]_l) \cap \mathit{dom}(u_0) = \emptyset$. Note that if $S = \{b \mid b \sim_l a\}$, then there is a prefix of u_1 such that $u_1 \in S^{-\infty}$. This follows from the fact that, the decomposition (u_0, u_1) is a maximal cut. Similarly the *$P_u([a]_r)$-right decomposition of a word u* is defined to be the unique minimal cut (u_0, u_1) such that $P_u([a]_r) \cap \mathit{dom}(u_1) = \emptyset$.

With the left/right decomposition defined, we can define the *congruence on words*, $\equiv_n$ which essentially captures a sequence of unique decompositions.

▶ **Definition 6.** For an alphabet A, a natural number $n \in \mathbb{N}$ and words $u, v \in A^\circ$, we define $u \equiv_n v$ by induction on $m = n + |A|$ as follows.

1. If $n = 0$ (the base case): $u \equiv_0 v$ for all $u, v \in A^\circ$.
2. If $n > 0$: We say $u \equiv_n v$ if the following conditions are satisfied:
   - **a.** $\mathit{alphabet}(u) = \mathit{alphabet}(v)$, $T^1_r(u) = T^1_r(v)$, and $T^1_l(u) = T^1_l(v)$. (This condition implies that $T^\omega_r(u) = T^\omega_r(v)$ and $T^{\omega^*}_l(u) = T^{\omega^*}_l(v)$).
   - **b.** The right preorders of u and v (both on the same set by the previous observation) are the same. Similarly the left preorders of u and v are the same. (We denote the left and right preorders as $\lesssim_l, \lesssim_r$ respectively).
   - **c.** For each $a \in T^1_l(u) = T^1_l(v)$, let (u_0, a, u_1) be the a-left decomposition of u, and let (v_0, a, v_1) be the a-left decomposition of v, then $u_0 \equiv_n v_0$ and $u_1 \equiv_{n-1} v_1$. Note that the induction parameter has reduced in both cases: u_0 has at least one letter less than u; and we have a lesser congruence in u_1.
   - **d.** Similarly, for each $a \in T^1_r(u) = T^1_r(v)$, let (u_0, a, u_1) be the a-right decomposition of u and let (v_0, a, v_1) be the a-right decomposition of v, then $u_0 \equiv_{n-1} v_0$ and $u_1 \equiv_n v_1$.
   - **e.** For each class $[a]_l \in T^{\omega^*}_l(u)/\sim_l = T^{\omega^*}_l(v)/\sim_l$, let (u_0, u_1) be the $P_u([a]_l)$-left decomposition of u and let (v_0, v_1) be the $P_v([a]_l)$-left decomposition of v, then $u_0 \equiv_n v_0$ and $u_1 \equiv_{n-1} v_1$. Again, the induction parameter has reduced in both cases: u_0 has at least one letter less than u; and we have a lesser congruence in u_1.

f. Similarly for each class $[a]_r \in T^\omega_r(u)/\sim_r = T^\omega_r(v)/\sim_r$, let (u_0, u_1) be the $P_u([a]_r)$-right decomposition of u and let (v_0, v_1) be the $P_v([a]_r)$-right decomposition of v, then $u_0 \equiv_{n-1} v_0$ and $u_1 \equiv_n v_1$.

▶ **Lemma 7.** *The relation $\equiv_n$ is a congruence relation for every $n \in \mathbb{N}$.*

Main theorem

We are now in a position to state our main theorem.

▶ **Theorem 8.** *Let $L \subseteq A^\circ$. Then the following are equivalent:*

1. *L is definable in $\{\mathtt{F}, \mathtt{P}\}$-TL.*
2. *L is $\mathrm{FO}^2(A, \leq)$ definable.*
3. *L is a union of $\equiv_n$ congruent classes for some $n \in \mathbb{N}$.*
4. *L is recognised by a $\circ$-DA.*
5. *L is recognised by an aperiodic $\circ$-monoid where all regular $\mathcal{J}$ classes are sub $\circ$-monoids.*
6. *The syntactic $\circ$-monoid of L is in $\circ$-DA.*

The proof of $(1 \Leftrightarrow 2)$ follows easily (see [8, 7]).
In subsection 3.1 we show the equivalence of the different monoid views $(4 \Leftrightarrow 5 \Leftrightarrow 6)$.
In subsection 3.2 we show $(4 \Rightarrow 3)$.
To prove $(2 \Rightarrow 4)$, we use 2-pebble *Ehrenfeucht-Fraïssé* (EF) games [26]. The EF game gives a game congruence $\cong_n$ defined as: $u \cong_n v$ if the duplicator wins the n-round 2-pebble game on the pair of words (u, v). See [26] for the game congruence and its equivalence to FO^2. Thus it suffices to show that the game congruence satisfies the equations of $\circ$-DA.
To show direction $(3 \Rightarrow 2)$ we follow the proof in [26]. It suffices to show that if $L \subseteq A^\circ$ is a union of $\equiv_n$ congruent classes for some n, then it is definable in $\mathrm{FO}^2(<)$. More precisely we prove the following lemma (again using the equivalence of game congruence $\cong_n$ and FO^2).

▶ **Lemma 9.** *For words $u, v \in A^\circ$, If $u \not\equiv_n v$, then $u \not\cong_{n+alphabet(u)} v$ i.e. the spoiler has a winning strategy in the 2-pebble $n + alphabet(u)$-round EF game on u and v.*

Since the syntactic $\circ$-monoid (and its finite representation using $\circ$-algebra) is computable given an MSO formula [4], it follows that it is decidable to check whether the language is FO^2 definable.

▶ **Corollary 10.** *For a sentence ϕ in MSO[<], it is decidable whether $L(\phi)$ is $FO^2[<]$ definable.*

In the next subsection we show the equivalence of the different monoid views. The subsection after that shows that if a language is accepted by a $\circ$-monoid, then it is a union of congruence classes $\equiv_n$ for some $n \in \mathbb{N}$.

3.1 The different Monoid views

In this subsection we show that the different views of $\circ$-DA are equivalent. That is, $(4 \Leftrightarrow 5 \Leftrightarrow 6)$ of Theorem 8. The direction $(4 \Rightarrow 5)$, follows from standard ideas in semigroup theory and the reverse direction $(5 \Rightarrow 4)$, follows from the below lemma:

▶ **Lemma 11.** *Let $\mathbf{M}$ be an aperiodic $\circ$-monoid such that all regular $\mathcal{J}$ classes of $\mathbf{M}$ are sub $\circ$-monoids. Let $\gamma : A^\circ \to \mathbf{M}$ be a morphism and $u \in A^\circ$, such that $\gamma(u) = e$ an idempotent. Then, for all words $v \in \{alphabet(u)\}^\circ$, we have $\gamma(uvu) = \gamma(u)$.*

To prove direction $(4 \Rightarrow 6)$, assume L is recognised by a monoid in $\circ$-DA. Since, $\circ$-DA is closed under quotienting, it follows that the syntactic monoid of L satisfies the equations of $\circ$-DA (see [6] for more details about syntactic congruence and monoids).

3.2 Algebra to Congruence

In this subsection we show direction $(4 \Rightarrow 3)$ of Theorem 8. The proof improves on the equivalence of the congruence and algebra given in [26]. We show that a language recognisable by a $\circ$-monoid in $\circ$-DA, satisfies the congruence relation $\equiv_n$ for some $n \in \mathbb{N}$. Let L be recognised by the morphism $\gamma : A^\circ \to \mathbf{M}$, where $\mathbf{M}$ is in $\circ$-DA. It suffices to show that there exists an $n \in \mathbb{N}$ such that $\equiv_n$ is a finer congruence than the monoid congruence. That is for $u, v \in A^\circ$, if $u \equiv_n v$, then $\gamma(u) = \gamma(v)$. Since $\mathbf{M}$ is an aperiodic monoid (follows from equations of $\circ$-DA) it is sufficient to show that $u\mathcal{R}v$ and $u\mathcal{L}v$.

The left/right decomposition of words are closely related to how the $\mathcal{R}$ classes fall in the word. The following definition identifies a sequence of $\mathcal{R}$-smooth factors (those factors where there is no $\mathcal{R}$ fall), and the subsequent lemma shows there exists such a unique sequence.

▶ **Definition 12.** Let $\gamma : A^\circ \to \mathbf{M}$. Let $w \in A^\circ$. Then the $\mathcal{R}$ decomposition of w is defined as the sequence $(w_0, a_1, w_1, a_2, \ldots, a_k, w_k)$ such that

1. $a_i \in A \cup \{\epsilon\}$ and $w_i \in A^*$, for all $i \leq k$.
2. $w = w_0 a_1 \ldots a_k w_k$.
3. For each $0 < i \leq k$, if a_i is empty, then the following conditions hold:
   a. w_i does not have a left end point.
   b. $(w_0 a_1 \ldots a_i w_i') \mathcal{R} \gamma(w_0 a_1 \ldots a_i w_i)$, for all nonempty prefix w_i' of w_i.
   c. $\gamma(w_0 a_1 \ldots w_{i-1}) \not\mathcal{R} \gamma(w_0 a_1 \ldots w_{i-1} a_i w_i)$.
4. For each $0 < i \leq k$, if a_i is not empty, then the following holds:
   a. $\gamma(w_0 a_1 \ldots a_i) \mathcal{R} \gamma(w_0 a_1 \ldots a_i w_i)$.
   b. $\gamma(w_0 a_1 \ldots w_{i-1}) \not\mathcal{R} \gamma(w_0 a_1 \ldots w_{i-1} a_i)$.

▶ **Lemma 13.** *Let $w \in A^\circ$ be an arbitrary word. Then, there is a unique $\mathcal{R}$ decomposition $(w_0, a_1, \ldots, a_k, w_k)$ of w.*

The following Lemma connects $\mathcal{R}$ decompositions and left decompositions.

▶ **Lemma 14.** *Let $(w_0, a_1, \ldots, a_k, w_k)$ be the $\mathcal{R}$ decomposition of w. Then, for each $0 < i \leq k$,*

1. *If a_i is not empty, then $a_i \notin alphabet(w_{i-1})$.*
2. *If a_i is empty, then there exists an $a \notin alphabet(w_{i-1})$ such that $a \in T_l^{\omega^*}(w_i')$ for all nonempty prefix w_i' of w_i.*

We are now in a position to prove our claim.

Proof of Theorem 8, $(4 \Rightarrow 3)$. We show that if $u \equiv_m v$ for a sufficiently large m (depending only on $alphabet(u)$ and $\mathbf{M}$), then $\gamma(u)\mathcal{R}\gamma(v)$. The $\mathcal{L}$ equivalence can be shown symmetrically. As discussed in the beginning, this proves our claim. Our induction hypothesis is as follows:

$$\text{If } u \equiv_m v \text{ for an } m > |alphabet(u)| \times |\mathbf{M}|, \text{ then } \gamma(u) = \gamma(v).$$

The base case, when $m = 0$ is clearly true, since $u = v = \epsilon$ (note that, in this case $alphabet(u) = \emptyset$). Let us now consider the inductive step, for $m > 0$, we have $u \equiv_m v$. Our aim is to show that $\gamma(u) = \gamma(v)$. Consider the $\mathcal{R}$ decomposition of $u = (u_0, a_1, u_1, \ldots, a_k, u_k)$. We give a sequence $v = (v_0, a_1, v_1, \ldots, a_k, v_k)$ such that $\gamma(u_i) = \gamma(v_i)$ for all $i < k$ and hence $\gamma(u) \geq_{\mathcal{R}} \gamma(v)$.

Define $u_i' = u_i a_{i+1} \ldots u_k$, for all $i \leq k$. We do the following procedure for i ranging from $1, 2, \ldots, k$. During every iteration of i, we give v_i', a suffix of v_i such that the invariant $u_i' \equiv_{m-i} v_i'$ is maintained. To start the iteration we set $v_0' = v$ and $u_0' \equiv_m v_0'$

1. If a_i is non empty, then (u_{i-1}, a_i, u'_i) is the a_i-left decomposition of the word u'_{i-1} (follows from Lemma 14). Since $(u'_{i-1} \equiv_{m-(i-1)} v'_{i-1})$, there exists an a_i-left decomposition of $v'_{i-1} = (v_{i-1}, a_i, v'_i)$ such that $u_{i-1} \equiv_{m-(i-1)} v_{i-1}$ and $u'_i \equiv_{m-i} v'_i$.
2. If a_i is empty, then (u_{i-1}, u'_i) is an $[a]_l$-left decomposition of the word u'_{i-1} for an $[a]_l \in T_l^{\omega^*}(u'_{i-1})/\sim_l$ (follows from Lemma 14). Since $(u'_{i-1} \equiv_{m-(i-1)} v'_{i-1})$, there exists an $[a]_l$-left decomposition of $v'_{i-1} = (v_{i-1}, v'_i)$ such that $u_{i-1} \equiv_{m-(i-1)} v_{i-1}$ and $u'_i \equiv_{m-i} v'_i$.

Assign $v_k = v'_k$ obtained at the end of iteration.

Note that $k \leq |\mathbf{M}|$. For an $i < k$, we have $|alphabet(u_i)| = |alphabet(v_i)| < |alphabet(u)|$ (from Lemma 14) and therefore $m - i > |alphabet(u_i)| \times |\mathbf{M}|$. Since $u_i \equiv_{m-i} v_i$ from induction hypothesis, it follows $\gamma(u_i) = \gamma(v_i)$, for all $i < k$. Therefore $\gamma(u_0 \dots a_k) = \gamma(v_0 \dots a_k)$.

It remains to show that $\gamma(u) \geq_{\mathcal{R}} \gamma(v)$. Depending on whether a_k is empty or not, we get the following cases.

1. If a_k is non empty, then $\gamma(u_0 a_1 \dots a_k u_k)\ \mathcal{R}\ \gamma(u_0 a_1 \dots a_k) = \gamma(v_0 a_1 \dots a_k) \geq_{\mathcal{R}} \gamma(v)$. The first condition follows from the fact that the sequence $(u_0 a_1 \dots u_k)$ is an $\mathcal{R}$ decomposition, and the second condition follows from the fact that $\gamma(u_i) = \gamma(v_i)$ for all $i < k$.
2. If a_k is empty, then $(u_0 \dots u_{k-1}, u_k)$ and $(v_0 \dots v_{k-1}, v_k)$ are both S-left decomposition for an $S \in T_l^{\omega^*}(u_i)/\sim_l$. Hence there are prefixes u'_k of u_k and v'_k of v_k such that $u'_k, v'_k \in S^{-\infty}$. From Lemma 11 we know that $\gamma(u'_k)\mathcal{R}\gamma(v'_k)$. Therefore, $\gamma(u_0 a_1 \dots a_k u_k)\ \mathcal{R}\ \gamma(u_0 a_1 \dots u'_k)\ \mathcal{R}\ \gamma(v_0 a_1 \dots v'_k) \geq_{\mathcal{R}} \gamma(v_0 a_1 \dots a_k v_k) = \gamma(v)$.

We now have $\gamma(u) \geq_{\mathcal{R}} \gamma(v)$. By a symmetric argument we get $\gamma(v) \geq_{\mathcal{R}} \gamma(u)$ and therefore $\gamma(u)\ \mathcal{R}\ \gamma(v)$. By $\mathcal{L}$-$\mathcal{R}$ symmetry, $\gamma(u)\ \mathcal{L}\ \gamma(v)$ and since $\mathbf{M}$ is aperiodic $\gamma(u) = \gamma(v)$. ◀

4 Satisfiability

In this section we address the satisfiability problem of two-variable logic over countable linear orderings. The rest of the section is devoted to the proof of the below theorem. Take note of the fact that in this section Σ denotes a set of unary predicates (and not an alphabet). Our models are words over the alphabet $\mathcal{P}(\Sigma)$.

▶ **Theorem 15.** *The following problems are* NEXPTIME*-complete: Satisfiability of* $\mathrm{FO}^2(\Sigma, <)$ *over*

1. *arbitrary linear orderings,*
2. *countable linear orderings,*
3. *scattered linear orderings.*

First we deal with the hardness part of the theorem. By downward Löwenheim-Skolem theorem, every satisfiable first-order formula has a countable model, and therefore (1) reduces to (2). Similary by Lemma 16 (given below), if a two-variable logic formula has a countable model, then it has a scattered model. Therefore (2) reduces to (3). Secondly, satisfiability of $\mathrm{FO}^2(\Sigma)$ over arbitrary structures already is NEXPTIME-hard [9], and therefore (1), (2) and (3) are NEXPTIME-hard.

Next we prove that (2) and (3) are in NEXPTIME. The idea is to show that for any satisfiable formula there is a model of a particular form that admit at most exponentially big (in the size of the formula) description.

Let φ be a $\mathrm{FO}^2(\Sigma, <)$ formula. Using standard ideas we obtain a formula $\varphi' \in \mathrm{FO}^2(\Sigma', <)$ in Scott normal form, i.e.

$$\varphi' = \forall x \forall y\, \psi(x, y) \wedge \bigwedge_i \forall x \exists y\, \chi_i(x, y)\,, \tag{1}$$

where $\Sigma' \supseteq \Sigma$, $|\Sigma'| = |\Sigma| + \mathcal{O}(|\varphi|)$, $|\varphi'| = \mathcal{O}(|\varphi|)$, $\psi(x,y)$ and $\chi_i(x,y)$ are quantifier free, such that φ and φ' are equisatisfiable (one is satisfiable if and only if the other is satisfiable). More precisely, the sets of models of φ and φ' are isomorphic upto the erasure of the unary predicates $\Sigma' \setminus \Sigma$.

We introduce some notation. Given a set of unary predicates P, we define a unary type over P to be a maximal conjunction of literals (i.e. $U(x)$ or $\neg U(x)$ where U is a unary predicate in P) over the same variable that is satisfiable. When the set P is clear from the context we just use types to refer to the unary types over P. We write $\mathrm{tp}(P)$ to denote the types over the predicates P. Each position of a $\circ$-word satisfies exactly one type, called the *type of the position*. Models of φ' are $\circ$-words over the alphabet $\mathrm{tp}(\Sigma')$.

Next we prove that formulas φ' in Scott normal form possess particular kind of models.

▶ **Lemma 16.** *If φ' is satisfiable, then it has a model of the form $u_1^{\lambda_1} \cdots u_n^{\lambda_n}$ where $n \geq 1$ is a natural number, for each $1 \leq i \leq n$, u_i is a finite word over the alphabet $\mathrm{tp}(\Sigma')$ and λ_i is in $\{1, \omega, \omega^*\}$, such that*

1. *every type occurs at most once in each u_i, and*
2. *every type occurs in at most two u_i's.*

A model of the form $u = u_1^{\lambda_1} \cdots u_n^{\lambda_n}$ is finitely represented as a sequence of pairs $(u_1, \lambda_1) \cdots (u_n, \lambda_n)$. Lemma 16 guarantees that for every satisfiable formula φ' there is a representation of size at most $3 \cdot \mathrm{tp}(\Sigma) \leq 3 \cdot 2^{|\varphi'|}$.

▶ **Lemma 17.** *Given a sequence of pairs $(u_1, \lambda_1) \cdots (u_n, \lambda_n)$ and a formula φ' checking if the $\circ$-word $u_1^{\lambda_1} \cdots u_n^{\lambda_n}$ satisfies the formula φ in Scott normal form is in* Ptime.

To complete the proof of the Theorem 15 we describe a Nexptime algorithm for FO^2 formulas over countable linear orders: The algorithm converts the input formula to Scott normal form and guesses an atmost exponentially large representation of a model of the form described by Lemma 16 and checks that it is indeed a model by Lemma 17.

5 Conclusion

In this paper we characterised first-order logic with two variables over countable linear orderings. It is equivalent to a fragment of temporal logic and is characterised by a subclass of $\circ$-monoids, called $\circ$-DA. The class $\circ$-DA is the class of $\circ$-monoids whose regular $\mathcal{J}$ classes are sub $\circ$-monoids. We also proved an alternate characterisation of this class using equations and this yields decidability of membership in this class. Next we considered the satisfiability problem for FO^2 over arbitrary, countable and scattered linear orderings and showed that all the problems are Nexptime-complete.

Finally we note that FO^2 with order and *successor* relation (position $j > i$ is the successor of position i if there is no position between them) is strictly more powerful that FO^2 with only the order relation. To see this it is enough to note that a^ω and $a^\omega a^\omega$ are indistinguishable by any formula in the latter class, while there is a formula, namely "there is exactly one position without a predecessor" that separates them. We leave as future work the question of extending the characterisation in the present paper to handle the successor relation.

References

1 Nicolas Bedon, Alexis Bès, Olivier Carton, and Chloe Rispal. Logic and rational languages of words indexed by linear orderings. *Theory Comput. Syst.*, 46(4):737–760, 2010.

2 Alexis Bès and Olivier Carton. Algebraic characterization of FO for scattered linear orderings. In *Computer Science Logic, 25th International Workshop / 20th Annual Conference of the EACSL, CSL 2011*, pages 67–81, 2011.

3 Mikołaj Bojańczyk, Claire David, Anca Muscholl, Thomas Schwentick, and Luc Segoufin. Two-variable logic on data words. *ACM Trans. Comput. Log.*, 12(4):27, 2011.

4 Olivier Carton, Thomas Colcombet, and Gabriele Puppis. Regular languages of words over countable linear orderings. In *Automata, Languages and Programming – 38th International Colloquium, ICALP 2011, Proceedings, Part II*, pages 125–136, 2011.

5 Thomas Colcombet. Factorization forests for infinite words and applications to countable scattered linear orderings. *Theor. Comput. Sci.*, 411(4-5):751–764, 2010.

6 Thomas Colcombet and A. V. Sreejith. Limited set quantifiers over countable linear orderings. In *Automata, Languages, and Programming – 42nd International Colloquium, ICALP 2015, Proceedings, Part II*, pages 146–158, 2015.

7 Julien Cristau. Automata and temporal logic over arbitrary linear time. In *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2009*, pages 133–144, 2009.

8 Kousha Etessami, Moshe Y. Vardi, and Thomas Wilke. First-order logic with two variables and unary temporal logic. *Inf. Comput.*, 179(2):279–295, 2002.

9 Martin Fürer. The computational complexity of the unconstrained limited domino problem (with implications for logical decision problems). In *Logic and Machines: Decision Problems and Complexity, Proceedings of Symposium Rekursive Kombinatorik*, pages 312–319, 1983.

10 Erich Grädel, Phokion G. Kolaitis, and Moshe Y. Vardi. On the decision problem for two-variable first-order logic. *Bulletin of Symbolic Logic*, 3(1):53–69, 1997.

11 Manfred Kufleitner and Pascal Weil. On FO2 quantifier alternation over words. In *Mathematical Foundations of Computer Science 2009, 34th International Symposium, MFCS 2009*, pages 513–524, 2009.

12 Manfred Kufleitner and Pascal Weil. The FO2 alternation hierarchy is decidable. In *Computer Science Logic (CSL'12) – 26th International Workshop/21st Annual Conference of the EACSL, CSL 2012*, pages 426–439, 2012.

13 Amaldev Manuel. Two variables and two successors. In *Mathematical Foundations of Computer Science 2010, 35th International Symposium, MFCS*, pages 513–524, 2010.

14 Amaldev Manuel and Thomas Zeume. Two-variable logic on 2-dimensional structures. In *Computer Science Logic 2013 (CSL 2013), CSL*, pages 484–499, 2013.

15 Martin Otto. Two variable first-order logic over ordered domains. *J. Symb. Log.*, 66(2):685–702, 2001.

16 Jean-Éric Pin. Mathematical foundations of automata theory.

17 Jean-Eric Pin and Pascal Weil. Polynomial closure and unambiguous product. In *Automata, Languages and Programming, 22nd International Colloquium, ICALP95, Proceedings*, pages 348–359, 1995.

18 Michael O. Rabin. Decidability of second-order theories and automata on infinite trees. *Transactions of the American Mathematical Society*, 141:1–35, 1969.

19 Alexander Rabinovich. Temporal logics over linear time domains are in PSPACE. *Inf. Comput.*, 210:40–67, 2012.

20 Joseph G. Rosenstein. *Linear orderings*. Academic Press New York, 1981.

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

22 Thomas Schwentick, Denis Thérien, and Heribert Vollmer. Partially-ordered two-way automata: A new characterization of DA. In *Developments in Language Theory, 5th International Conference, DLT 2001*, pages 239–250, 2001.

23 Thomas Schwentick and Thomas Zeume. Two-variable logic with two order relations. *Logical Methods in Computer Science*, 8(1), 2012.

24 S.Shelah. The monadic theory of order. *Ann. of Math.*, 102:379–419, 1975.

25 Pascal Tesson and Denis Therien. Diamonds are forever: The variety DA. In *Semigroups, Algorithms, Automata and Languages*, pages 475–500. World Scientific, 2002.

26 Denis Thérien and Thomas Wilke. Over words, two variables are as powerful as one quantifier alternation. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC'98, pages 234–240. ACM, 1998.

27 Philipp Weis and Neil Immerman. Structure theorem and strict alternation hierarchy for FO^2 on words. *Logical Methods in Computer Science*, 5(3), 2009.