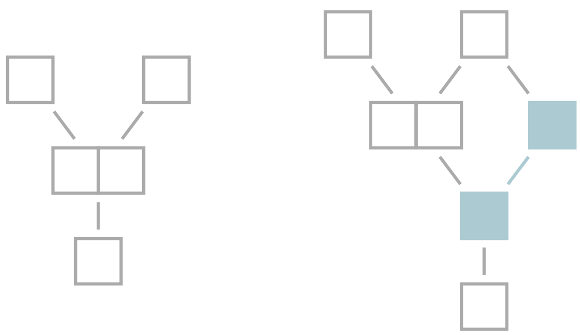
First-order separation of transfinite regular languages

Master Parisien de Recherche en Informatique
internship report



Rémi Morvan
École normale supérieure Paris-Saclay

under the supervision of

Thomas Colcombet & Sam van Gool
IRIF, CNRS & Université de Paris

March – August 2021

Contents

This report was written using the package `knowledge`: by clicking on a notion (ex: powerset), one is sent to its definition.

The general context

The key idea behind algebraic language theory is to study regular languages via algebraic notions (e.g. semigroups) instead of computational objects (e.g. finite automata). One particularly interesting family of results in this field consists of equivalences between logics (e.g. first-order logic) and algebra (e.g. aperiodic semigroups). More precisely, given a logic, two questions naturally arise: *(i)* give an algebraic characterisation of the definability in this logic, and of *(ii)* the separability by this logic. The former problem is simplier than the latter.

We have many definability results for languages of words: e.g. *(i)* for finite words (Schützenberger's theorem: FO = aperiodic [Sch65, MP71]), *(ii)* for ω-words (Perrin's theorem: FO = aperiodic [Per84]), *(iii)* for transfinite words (Bedon's theorem: FO = aperiodic [Bed98]), *(iv)* for scattered words (Bès-Carton's theorem: FO = gap-insensitive [BC11] & Bedon-Rispal's theorem: FO[cut] = aperiodic [BR12, CS15]) and *(v)* for countable words (Colcombet-Sreejith's theorem: many results, see [CS15]).

These two results on scattered words both rely on Carton & Rispal's scattered semigroups [Ris04, RC05], which is the suitable algebraic structure to talk about scattered regular languages.

Bedon & Rispal proved in [BR12] the equivalence between languages recognised by finite aperiodic scattered semigroups and star-free scattered languages. Colcombet & Sreejith introduced the logic FO[cut] — consisting of first-order logic enriched with monadic quantification over Dedekind cuts — latter, in [CS15].

The research problem

Among those five results, only two of them have a separability counterpart: for finite words, Henckell's theorem states that FO-separability is characterised by group saturation, and for ω-words, Place-Zeitoun's theorem gives a similar characterisation. For transfinite words and beyond, no such result is known.

Your contribution

We prove that the first-order separability problem for transfinite regular languages — which asks, given two languages of words indexed by countable ordinals and defined by monadic second-order formulæ, if there exists a first-order formula satisfied by every word of one of the two languages and by none of the other — is decidable (coro. 2.38). To do this, we first give an elementary proof of Henckell's theorem [Hen88] on pointlike sets (thm. 1.14), that we obtained by refining Place & Zeitoun's proof for finite words [PZ16] (§1). We then generalise this result to transfinite languages (§2 and thm. 2.37): we show that pointlike sets for the first-order logic over transfinite words corresponds to the (ordinal) group saturation.

While we focus, in this report, on definability and separability results for fragments of MSO for different monads (finite words, transfinite words, etc.), note that the work of Henckell and Rhodes [Hen88] gave rise to a prolific field, studying pointlikes with respect to some variety of semigroups — most of which do not correspond to fragments of MSO. See, e.g. [GS19], which studies varieties of semigroups determined by their subgroups.

Arguments supporting its validity

No mistakes were found in our proofs. Should you find one, please send an email to ($\lambda x.\, x$`@ens-paris-saclay.fr`) (`remi.morvan`).

Summary and future work

We plan on continuing this work by giving algebraic characterisations of separability by FO and by FO[cut] on scattered regular languages, to generalise Bès-Carton's and Bedon-Rispal's theorems. We conjecture the following result: for scattered regular languages, FO-pointlikes (resp. FO[cut]-pointlikes) coincides to the downward closure of the gap saturation (resp. group saturation). We could then study the general case of all countable words — for which we have many definability results by Colcombet & Sreejith [CS15], which all rely on Carton, Colcombet & Puppis' algebraic structure for countable words [CCP18].

Notations and conventions

We denote by $\mathbb{N}$, $\mathbb{N}_{>0}$ and $\mathbb{Z}$ the set of natural numbers, the set of strictly positive natural numbers and the set of integers, respectively. If $\sim$ is an equivalence relation over some set and x is an element of that set (resp. X is a subset of this set), then we denote by $[x]_\sim$ (resp. $[X]_\sim$) the equivalence class of x under $\sim$ (resp. the union of equivalence classes of elements of X under $\sim$). In a poset X, for every subset $Y \subseteq X$, we denote by $\downarrow Y$ the downward closure of Y. In a finite semigroup, we denote by x^π the unique idempotent power of an element x.

If X is a set, we denote by $\mathcal{P}(X)$ the powerset of X. Observe that if $(S, \cdot)$ is a semigroup, equipping $\mathcal{P}(S)$ with the internal law defined by

$$X \cdot Y := \{x \cdot y \mid x \in X \text{ and } y \in Y\}$$

for all $X, Y \in \mathcal{P}(S)$ yields a semigroup, called the *power semigroup* of $(S, \cdot)$. The map $-^{\mathrm{sgl}}$ from S to $\mathcal{P}(S)$ that sends $s \in S$ to $\{s\}$ defines an injective morphism: its image, which is isomorphic to S, is called the *subsemigroup of singletons* of $\mathcal{P}(S)$. Moreover, if $X \in \mathcal{P}(S)$, $\bigcup X$ denotes the union of the elements of X, which we call called support of X. This defines a semigroup morphism $\bigcup : \mathcal{P}(S) \to S$.

Observe that $\bigcup x^{\mathrm{sgl}} = x$ for all $x \in S$: i.e. $\bigcup : \mathcal{P}(S) \to S$ is a left-inverse of $-^{\mathrm{sgl}} : S \to \mathcal{P}(S)$.

Given an alphabet A, we denote by A^+ (resp. A^*) the semigroup (resp. monoid) of non-empty finite words (resp. all finite words) over the alphabet A. The set of all first-order (resp. monadic second-order) formulæ over the alphabet A is denoted by FO(A) (resp MSO(A)). Given a logic $\mathfrak{L} \subseteq$ MSO(A), we say that a language is *definable* in $\mathfrak{L}$ — or $\mathfrak{L}$-definable — when there exists a formula in $\mathfrak{L}$ that is exactly satisfied by the words of the language.

Given a logic $\mathfrak{L} \subseteq$ MSO(A) closed under negation, we say that two regular languages L_1 and L_2 over some alphabet A are $\mathfrak{L}$-*separable* when there exists a formula of $\mathfrak{L}$ satisfied by every word of L_1 but by no word of L_2. There are two classical problems associated to any logic: the $\mathfrak{L}$-*definability problem*, which asks whether a regular language is $\mathfrak{L}$-definable, and $\mathfrak{L}$-*separability problem*, which asks whether two regular languages are $\mathfrak{L}$-separable. The $\mathfrak{L}$-definability problem can be reduced to the $\mathfrak{L}$-separability problem: indeed, K and $A^+ \setminus K$ are $\mathfrak{L}$-separable if, and only if, K is $\mathfrak{L}$-definable.

1. Finite words

We say that a language $L \subseteq A^+$ is *regular* when it is accepted by a finite automaton. A semigroup S *recognises* a language L whenever, by definition, there exists a semigroup morphism $\varphi : A^+ \to S$ and a set $X \subseteq S$ such that $L = \varphi^{-1}[X]$. It is well-known that the following conditions are equivalent: *(i)* L is regular, *(ii)* L is recognised by a finite semigroup ; *(iii)* the syntactic semigroup of L is finite ; *(iv)* L is MSO-definable. The question then arises as to what happens to this equivalence between algebra, automata and logic when one restricts one of the classes, for instance, if we consider a fragment of MSO. *Schützenberger's theorem* provides an answer for FO, and establishes an equivalence between being accepted by a counter-free automaton [MP71], being FO-definable, and being recognised by a finite aperiodic semigroup [Sch65] — *aperiodic* means that every group in it is trivial. As a corollary, FO-definability is decidable.

For a proof, see, e.g., [Pin20, §IV.3.3] for the equivalence between automata and semigroups and [Pin20, §IX.3] for the equivalence between automata and MSO.

For a proof of the equivalence between FO and aperiodic semigroups, see [Pin20, §VI.3 & §IX.4.1].

The goal of this section is to state and prove Henckell's theorem, which, similarly to Schützenberger's theorem, states an equality between an object defined using logic (FO-pointlike sets, which are informally the subsets of a semigroup that cannot be distinguished using first-order logic), defined in §1.1, and an algebraic object (the group saturation of a semigroup, which is informally a semigroup in which one can merge a group into a single point), defined in §1.2. We then prove Henckell's theorem in §1.3, from which one can deduce that FO-separability is decidable for languages of finite words.

If one is interested in complexity results, Cho & Huynh [CH91] showed that FO-definability is PSpace-complete when the input is specified as a finite automaton. The problem is much simplier if the regular language given as input is specified by its syntactic monoid: in this case, the problem is NL — one only has to check that the syntactic monoid is aperiodic. For FO-separability, Place & Zeitoun proved [PZ18, ex. 7] that the complexity of the problem does not depend on whether the input is specified by automata, or by semigroup morphisms, and that the problem is between PSpace-hard and ExpTime. [PZ16]

1.1. First-order logic on finite words

We start be giving basic properties of first-order logic over finite words and define the $\equiv_k$-congruence, which allows us to characterise FO-separability (fact 1.5), and then define pointlike sets.

The *rank* — also called "quantifier depth" in the literature — of a first-order formula φ, denoted by $\mathrm{rk}(\varphi)$, is the maximal number of nested quantifiers: for example, the formula

$$\exists y.\, (\exists x.\, x < y) \wedge (\exists z.\, y < z),$$

which recognises words whose length is greater or equal to 3, has rank 2. The set of all first-order formulæ of rank at most $k \in \mathbb{N}$ over the alphabet A is denoted by $\mathrm{FO}_k(A)$.

Fact 1.1. There are finitely many $\mathrm{FO}_k(A)$ formulæ, up to logical equivalence.

For a proof, see [Ros82, lem. 13.10].

Given two words $w, w' \in A^+$, we say that w and w' are *FO_k-equivalent*, denoted by $w \equiv_k w'$, whenever w and w' satisfy exactly the same formulæ of FO_k. These equivalence relations are *semigroup congruences*: they are consistent with concatenation, in the sense that for all $u, u', v, v' \in A^+$, if $u \equiv_k u'$ and $v \equiv_k v'$ then $uv \equiv_k u'v'$. This can be proven either by using Ehrenfeucht-Fraïssé games — see [Ros82, lem. 6.5] — or can be seen as a corollary of Beth-Fraïssé theorem [Mak04, thm. 1.1]. Ehrenfeucht-Fraïssé games can also be used to prove the following property.

Observe that given two distinct finite words w and w', there always exists a first-order formula satisfied by w but not by w': i.e. there exists $k_0 \in \mathbb{N}$ such that for all $k \geq k_0$, $w \not\equiv_k w'$.

Fact 1.2. For every word $u \in A^+$, for $p, q \geq 2^k - 1$, we have $u^p \equiv_k u^q$.

Observe that every equivalence class L of $A^+/{\equiv_k}$ is FO_k-definable: simply consider the conjunction of all FO_k formulæ satisfied by a word of L, or, equivalently, every word of L — this makes sense since there are finitely many such formulæ, by fact 1.1.

Note that for $k \in \mathbb{N}_{>0}$ and $L, K \subseteq A^+$, if L and K are FO_k-definable, then their concatenation $L \cdot K$ is FO_{k+1}-definable. Indeed: let φ (resp. ψ) a FO_k formula defining L (resp. K). Then the first-order formula $\exists x. (\exists y. y < x) \land \varphi^{<x} \land \psi^{\geq x}$ has rank $k+1$ (since $k \neq 0$) and defines $L \cdot K$.

The concatenation of two languages corresponds to their product in the power semigroup of A^+. The notation $\varphi^{<x}$ refers to the relativisation of φ with respect to $\square < x$. For a formal definition, see [Ros82, def. 13.27].

The equivalences classes of A^+ under FO_k-equivalence $a^+ \cong \mathbb{N}_{>0}$ are extremely easy to describe on single-letter alphabets — of course, if A contains a single letter, then A^+ is isomorphic, as a semigroup, to $\mathbb{N}_{>0}$: we are simply talking about first-order logic on strictly positive integers.

Lemma 1.3. Let a be a letter and $k \in \mathbb{N}$. By letting $n := 2^k - 1$, we have:

$$a^+/{\equiv_k} = \Big\{\{a\}, \{a^2\}, \dots, \{a^{n-1}\}, \{a^p \mid p \geq n\}\Big\}.$$

Sketch of proof. By fact 1.2, $[a^n]_{\equiv_k} = \{a^p \mid p \geq n\}$. Moreover, by an easy induction on $r \in \mathbb{N}$ using relativisation, one can show that for all $m \leq 2^r - 1$, there exists an FO_r-formula φ_m satisfied exactly by $\{a^p \mid p \geq m\}$. Then for every $m < 2^k - 1$, the formula $\varphi_m \land (\neg\varphi_{m+1})$ has rank at most k and is satisfied exactly by $\{a^m\}$. Hence, $[a^m]_{\equiv_k} = \{a^m\}$. ☐

Example 1.4. We will illustrate the different notions on the following semigroup: consider the language $L := b^+(aa)^*$; Then one can check that its syntactic semigroup S_L contains six elements, and that its egg-box diagram is the one given in figure 1. Let $L_1 := L = b^+(aa)^*$, $L_2 := (aa)^+$ and $L_3 := a(aa)^*$. All three languages are recognised by the syntatic morphism of L: L_1 is the preimage of $\{baa\}$, L_2 is the preimage of $\{aa\}$ and L_3 is the preimage of $\{a\}$. None of these languages are FO-definable by Schützenberger's theorem: their syntactic semigroup contains the group $\mathbb{Z}/2\mathbb{Z}$ — in fact, $\mathbb{Z}/2\mathbb{Z}$ is precisely the syntactic semigroup of L_2 and L_3. Then, observe that L_1 and L_2 can be separated in first-order logic by the formula

$$\varphi := \exists x.\ \mathrm{first}(x) \land b(x),$$

where $\mathrm{first}(x) := \forall y. x \leq y$. On the other hand, L_2 and L_3 are not FO-separable — otherwise they would be FO-separable over the alphabet $\{a\}$, but since L_3 is the complement of L_2 in a^+, L_2 and L_3 would be FO-definable: *que nenni!*.

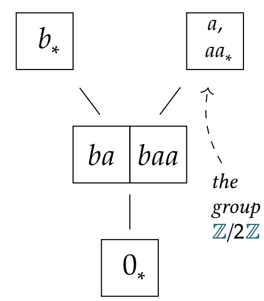


Figure 1: Egg-box diagram of the syntactic semigroup S_L of $L = b^+(aa)^*$.
We follow the same conventions as [Pin20] for egg-box diagrams.

Fact 1.5. For $L_1, L_2 \subseteq A^+$, the following propositions are equivalent:

i. L_1 and L_2 are FO-separable ;
ii. there exists an FO-definable language K such that $L_1 \subseteq K$ and $L_2 \cap K = \emptyset$;
iii. $[L_1]_{\equiv_k} \cap L_2 = \emptyset$ for some $k \in \mathbb{N}$;
iv. $[L_1]_{\equiv_k} \cap [L_2]_{\equiv_k} = \emptyset$ for some $k \in \mathbb{N}$.

Proof: each implication in *(i)* ⇒ *(ii)* ⇒ *(iii)* ⇒ *(iv)* ⇒ *(i)* is easy.

Likewise, L_1 and L_2 are FO_k-separable iff $[L_1]_{\equiv_k} \cap [L_2]_{\equiv_k} = \emptyset$, or equivalently, for every $w_1 \in L_1$ and $w_2 \in L_2$, $w_1 \not\equiv_k w_2$.

Definition 1.6. Let $\varphi : A^+ \to U$ be a semigroup morphism where U is a finite semigroup. We define the collection of FO-pointlike sets for φ by

$$\mathrm{Pl}_{\mathrm{FO}}(\varphi) := \Big\{X \subseteq U \mid \forall k \in \mathbb{N}, \exists L \in A^+/{\equiv_k}, X \subseteq \varphi[L]\Big\}.$$

Our notion of FO-pointlike for $\varphi : A^+ \to U$ is very closely related to Henckell's notion of pointlikes for a collection of relations [Hen88, def. 2.2]. More precisely, define for every $k \in \mathbb{N}$, *(continuing on the next page...)*

Our main motivation to introduce pointlike sets for φ is that being able to compute them allows us to decide if two languages recognised by φ are FO-separable, as explained in the following proposition — this was noticed in [Alm99] by Almeida, who was the first to notice the link between pointlike pairs with respect to a given variety of finite semigroups, and separability.

(...) the relation (in the sense of [Hen88, def. 1.3])

$$U \xrightarrow{R_k(\varphi)} A^+/\equiv_k$$

by $(u, L) \in R_k(\varphi)$ iff $u \in \varphi[L]$. Then pointlike sets for φ (under our terminology) corresponds precisely to pointlike sets for $(R_k(\varphi))_{k\in\mathbb{N}}$ (under Henckell's terminology). Those sets are also called "imprints of φ" ([PZ16]) or "aperiodic pointlikes of U" (e.g. [vGS19]).

Proposition 1.7. Two languages L_1 and L_2 recognised by a surjective morphism φ, are FO-separable if, and only if, no pointlike set for φ intersects both $\varphi[L_1]$ and $\varphi[L_2]$.

Proof. If no pointlike intersect both $\varphi[L_1]$ and $\varphi[L_2]$, then observe that since U is finite, we have

$$\mathrm{Pl}_{\mathrm{FO}}(\varphi) := \left\{X \subseteq U \mid \exists L \in A^+/\equiv_k,\ X \subseteq \varphi[L]\right\}.$$

for some $k \in \mathbb{N}$. Thus, for $w_1 \in L_1$ and $w_2 \in L_2$, if we had $w_1 \equiv_k w_2$, then $\{\varphi(w_1), \varphi(w_2)\}$ would be pointlike and would intersect both L_1 and L_2. Hence L_1 and L_2 are FO_k-separable.

Conversely, if L_1 and L_2 are FO-separable, say FO_l-separable for some $l \in \mathbb{N}$, then let $Y \in \mathrm{Pl}_{\mathrm{FO}}(\varphi)$, and assume, by contradiction, that Y intersects both $\varphi[L_1]$ and $\varphi[L_2]$. Then we would have $y_i \in Y \cap \varphi[L_i]$, and thus, since Y is pointlike — and since L_1 and L_2 are recognised by φ — we would have $w_1 \equiv_l w_2$ for some $w_1 \in L_1$ and $w_2 \in L_2$ such that $y_i = \varphi(w_i)$. Contradiction. □

1.2. Merging groups

Now that we have a correct grasp on first-order logic for finite words, we focus on the algebraic notions associated with finite words. More precisely, we define what the group saturation is. Informally, it is an algebraic process taking a semigroup and merging groups into a single point — this process is relevant to study first-order logic since this logic is not able to grasp group-like phenomena. Fix a finite semigroup U.

Definition 1.8. Given a subset $\mathcal{A}$ of $\mathcal{P}(U)$, its group saturation $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ is the least subsemigroup $\mathcal{S}$ of $\mathcal{P}(U)$ containing $\mathcal{A}$ and stable under *cyclic group merging*: if $\mathcal{G} \subseteq \mathcal{S}$ is a cyclic group, then $\bigcup \mathcal{G} \in \mathcal{S}$, or, equivalently, for every $X \in \mathcal{S}$, we have $X^\pi \cup X^{\pi+1} \cup \dots \cup X^{2\pi-1} \in \mathcal{S}$. We denote by $\mathrm{Sat}^*_{\mathrm{grp}}(\mathcal{A})$ the monoid obtained from the semigroup $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ by *always* adding an identity, denoted by ε.

Beware: contrary to Place & Zeitoun [PZ16, §4.2] and Henckell [Hen88, def. 3.4], we do not require the group saturation to be downward closed, so with our definition, the downward closure appears in the statement of Henckell's theorem (thm. 1.14).

Note that if S is an aperiodic semigroup, then $\mathrm{Sat}^+_{\mathrm{grp}}(S^{\mathrm{sgl}}) = S^{\mathrm{sgl}}$. Often — in the next example, for instance —, if X is a subset of U, we will abusively write $\mathrm{Sat}^+_{\mathrm{grp}}(X)$ instead of $\mathrm{Sat}^+_{\mathrm{grp}}(X^{\mathrm{sgl}})$.

Example 1.9: continuing ex. 1.4. We want to compute $\mathrm{Sat}^+_{\mathrm{grp}}(S_L)$. First, the group saturation of S_L contains every singleton $\{0\}$, $\{ba\}$, $\{baa\}$, $\{b\}$, $\{a\}$ and $\{aa\}$. Then, since $\{\{a\}, \{aa\}\}$ is a cyclic group, its support $\{a, aa\}$ is also an element of $\mathrm{Sat}^+_{\mathrm{grp}}(S_L)$, which is closed under product, so it must also contain $\{b\} \cdot \{a, aa\} = \{ba, baa\}$. One can check that there are no more elements: for example $\{ba, baa\} \cdot \{a, aa\} = \{ba, baa\}$ and $\{a, aa\} \cdot \{ba, baa\} = \{0\}$. The egg-box diagram of $\mathrm{Sat}^+_{\mathrm{grp}}(S_L)$ is represented in figure 2.

Moreover, note that the group saturation is not called "cyclic group saturation": this is because being stable under cyclic group merging or by *group merging* — meaning that for every group $\mathcal{G} \subseteq \mathcal{S}$, we have $\bigcup \mathcal{G} \in \mathcal{S}$ — is equivalent, as stated in proposition 1.10. In practice, it is often much easier to check that a semigroup is stable under cyclic group merging rather than under group merging.

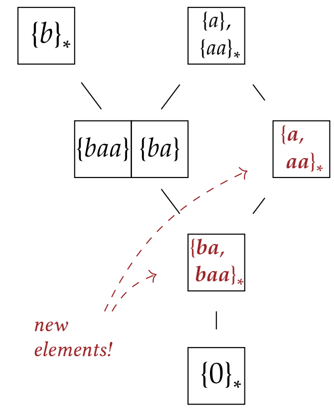


Figure 2: Egg-box diagram of the group saturation $\mathrm{Sat}^{+}_{\mathrm{grp}}(S_L)$ of the syntactic semigroup S_L of $L = b^{+}(aa)^{*}$.

Proposition 1.10. A subsemigroup $\mathcal{S}$ of $\mathcal{P}(U)$ is stable under cyclic group merging if, and only if, is it stable under group merging.

Proof. The implication from right to left is trivial since every cyclic group is is a group. Conversely assume that a semigroup $\mathcal{S}$ is stable under cyclic group merging, let $\mathcal{G}$ be a group in $\mathcal{S}$ and let us show that $\bigcup \mathcal{G} \in \mathcal{S}$. Let $\{X_1, \ldots, X_n\}$ denote the elements of $\mathcal{G}$ and let $\mathcal{G}_i := \{X_i^{\pi}, X_i^{\pi+1}, \ldots, X_i^{2\pi-1}\} = \langle X_i \rangle^{\cdot}$ be the group generated by X_i. Then $\bigcup \mathcal{G}_i \in \mathcal{S}$ for every i, and consider $M := (\bigcup \mathcal{G}_1) \cdots (\bigcup \mathcal{G}_n) \in \mathcal{S}$: for every i,

$$X_i = 1_{\mathcal{G}} \cdots 1_{\mathcal{G}} \cdot X_i \cdot 1_{\mathcal{G}} \cdots 1_{\mathcal{G}} \in \mathcal{G}_1 \cdots \mathcal{G}_n$$

and thus $X_i \subseteq M$. Hence $\bigcup \mathcal{G} \subseteq M$, and since the converse inclusion is trivial, we can deduce $\bigcup \mathcal{G} = M \in \mathcal{S}$. □

Exercise 1.11: Another example. Let $A = \{a, b\}$ and L be the language of words containing an even number of 'a' and 'b'.

1. Show that L is regular and compute its syntactic semigroup S_L.
2. Compute the group saturation of S_L, and draw its egg-box diagram.

Solution in §C.1

Proposition 1.12. For every $\mathcal{A} \subseteq \mathcal{P}(U)$, we have:

$$\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) = \mathcal{A} \cdot \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A}) = \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A}) \cdot \mathcal{A}.$$

This is a generalisation of the tautology $A^{+} = A \cdot A^{*} = A^{*} \cdot A$.

Proof. The inclusion $\mathcal{A} \cdot \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A}) \subseteq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ is trivial, since group saturation is always a semigroup. Then, we prove the converse inclusion by structural induction on $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$: first, $\mathcal{A} = \mathcal{A} \cdot \varepsilon \subseteq \mathcal{A} \cdot \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A})$; moreover, if Y, Y' are in $\mathcal{A} \cdot \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A})$, say $Y = X \cdot Z$ and $Y' = X' \cdot Z'$ then $Y \cdot Y' = X \cdot (Z \cdot X' \cdot Z') \in \mathcal{A} \cdot \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A})$; and finally, if $\mathcal{G}$ is a group whose elements are in $\mathcal{A} \cdot \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A})$, then for any $Y \in \mathcal{G}$ we have $\bigcup \mathcal{G} = \bigcup Y \cdot \mathcal{G} = Y \cdot \bigcup \mathcal{G} \in \mathcal{A} \cdot \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A})$. □

We insist on the following lemma — however, note that we only use it in the appendix, and more precisely in §B.1, to prove theorem 1.18 — because this is were our proof differs from the proof of Place & Zeitoun [PZ16, §6] of the completeness of Henckell's theorem.

Place & Zeitoun do the following case disjunction: either *(i)* there exists $a \in \mathcal{A}$ such that $a \cdot (\bigcup \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})) \subsetneq \bigcup \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$, *(ii)* there exists $a \in \mathcal{A}$ such that $(\bigcup \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})) \cdot a \subsetneq \bigcup \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ or *(iii)* $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ is a pseudogroup — where, by definition, a pseudogroup is a subsemigroup of the power semigroup that does not satisfy *(i)* and *(ii)*. Unfortunately, this case disjunction is hardly generalisable to ordinal semigroups — or at least not in any way that is usefull to prove a result on separability — while ours can: see thm. 2.36.

Lemma 1.13: Induction principle. Let $\mathcal{A} \subseteq \mathcal{P}(U)$. Then either:

i. there exists $a \in \mathcal{A}$ such that $a \cdot \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \subsetneq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$, or
ii. there exists $a \in \mathcal{A}$ such that $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \cdot a \subsetneq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$, or
iii. $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ has a maximum.

Proof. If *(i)* and *(ii)* do not hold, then every translation (both left and right) of $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ by $a \in \mathcal{A}$ is a permutation of a finite set. By restricting those translations to the semigroup $\langle \mathcal{A} \rangle^{\cdot}$ generated by $\mathcal{A}$, it follows that $\langle \mathcal{A} \rangle^{\cdot} =: G$ is a group. Hence $\bigcup G \in \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$. It is then routine to check that $\bigcup G$ is indeed maximal in $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$. □

We are now ready to state this equivalence between the algebraic structure that merges groups (group saturation) and the sets of points that first-order logic cannot distinguish (FO-pointlike sets).

If $\varphi : A^+ \to U$ is a semigroup morphism and U is a finite semigroup, then we denote by $\mathrm{Sat}^+_{\mathsf{grp}}(\varphi)$ the group saturation of the image of φ, i.e. $\mathrm{Sat}^+_{\mathsf{grp}}(\varphi) := \mathrm{Sat}^+_{\mathsf{grp}}(\varphi[A^+]^{\mathrm{sgl}})$.

Theorem 1.14: Henckell's theorem [Hen88]. Let $\varphi : A^+ \to U$ be a semigroup morphism where U is a finite semigroup. Then $\mathrm{Pl}_{\mathrm{FO}}(\varphi) = {\downarrow}\,\mathrm{Sat}^+_{\mathsf{grp}}(\varphi)$.

Example 1.15: continuing ex. 1.9. By theorem 1.14 and proposition 1.7, two regular languages recognised by the same morphism are FO-separable if, and only if, no element of the group saturation of the morphism intersects both images. Recall that L_2 and L_3 are recognised by $\{aa\}$ and $\{a\}$, respectively: their non-FO-separability is witnessed by the element $\{a, aa\}$, which belongs to the group saturation $\mathrm{Sat}^+_{\mathsf{grp}}(S_L)$ and hence is pointlike. On the other hand, the FO-separability of L_1 and L_2 — recognised by $\{baa\}$ and $\{aa\}$, respectively —, is witnessed by the absence of a pointlike set in $\mathrm{Sat}^+_{\mathsf{grp}}(S_L)$ containing both baa and aa.

Corollary 1.16. The FO-separability problem is decidable for regular languages of finite words.

Proof. By theorem 1.14 and proposition 1.7, since ${\downarrow}\,\mathrm{Sat}^+_{\mathsf{grp}}(\varphi)$ is computable. □

We prove Henckell's theorem by double inclusion: see lemma 1.17 (correctness) and lemma 1.21 (completeness).

One can think of sets in ${\downarrow}\,\mathrm{Sat}^+_{\mathsf{grp}}(\varphi)$ as "constructible pointlike sets" — this is in fact the terminology used by Henckell in [Hen88] — so the double inclusion can be thought as "every constructible pointlike is pointlike" (hence the name "correctness") and "every pointlike is constructible" (hence the name "completeness").

Lemma 1.17: Correctness of Henckell's theorem. ${\downarrow}\,\mathrm{Sat}^+_{\mathsf{grp}}(\varphi) \subseteq \mathrm{Pl}_{\mathrm{FO}}(\varphi)$.

Proof. By definition of pointlike sets, $\mathrm{Pl}_{\mathrm{FO}}(\varphi)$ is downward closed, so, by definition of group saturation, we only have to show that $\mathrm{Pl}_{\mathrm{FO}}(\varphi)$ contains every singleton of the form $\{\varphi(w)\}$, for $w \in A^+$, and that it is a semigroup stable under cyclic group merging.

Points are pointlike!

If $w \in A^+$, the singleton $\{\varphi(w)\}$ is included in $\varphi[[w]_{\equiv_k}]$ for every $k \in \mathbb{N}$, and hence is pointlike. Moreover, if X, X' are pointlike, say for every $k \in \mathbb{N}$, $X \subseteq \varphi[L_k]$ and $X' \subseteq \varphi[L'_k]$, then $X \cdot X' \subseteq \varphi[L_k \cdot L'_k]$. But since $\equiv_k$ is a semigroup congruence, $L_k \cdot L'_k$ is included in an $\equiv_k$-equivalence class and hence $X \cdot X'$ is pointlike.

Finally, let us show that pointlike sets are stable under cyclic group merging: let X be a pointlike set. Let $k \in \mathbb{N}$. There exists $L \in A^+/{\equiv_k}$ such that $X \subseteq \varphi[L]$. Let $p \in \mathbb{N}_{>0}$ be such that $\varphi[X]^p = \varphi[X]^\pi$ and $p \geq 2^k - 1$. By fact 1.2, for all $u, v \in A^+$, $u^p \equiv_k u^{p+q}$ for $q \in \mathbb{N}$: it follows that $L^p \cup L^{p+1} \cup \ldots L^{2p-1}$ is included in an $\equiv_k$-class, say L', so that $X^\pi \cup \ldots \cup X^{2\pi-1} \subseteq \varphi[L']$. Therefore, $X^\pi \cup \ldots \cup X^{2\pi-1}$ is also pointlike. □

We denote by $\pi : \mathcal{P}(U)^+ \to \mathcal{P}(U)$ the generalised product of $\mathcal{P}(U)$. We say that a map from a free semigroup A^+ to a set is FO-*definable* whenever every preimage by this map is an FO-definable language. The key technical result used to prove the completeness (lemma 1.21) of Henckell's theorem is the following theorem.

Theorem 1.18: FO-approximation. For every alphabet A, for every finite semigroup U, for every semigroup morphism $\varphi : A^+ \to U$, there exists an FO-definable function $\hat{\varphi} : A^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(U)$ such that $\varphi(w) \in \hat{\varphi}(w)$ for all $w \in A^+$.

This theorem states that every morphism can be upper-approximated by an FO-definable function.

Example 1.19: continuing ex. 1.15. Consider the syntactic morphism $\varphi : A^+ \to S_L$ of the language L defined in ex. 1.4. It is not FO-definable: for example, the preimages of $\{aa\}$ and $\{a\}$ are not FO-definable. Informally, the non-FO-definability can be explained because φ — or, more precisely, the restriction of φ to a^+ — counts modulo 2, which is a group-like phenomenon. To make it FO-definable, we must forbid it to count modulo 2. One way of doing this is by sending $L_2 = (aa)^+$ and $L_3 = a(aa)^*$ on the same element, $\{a, aa\} \in \mathrm{Sat}^+_{\mathrm{grp}}(S_L)$. More generally, one can check that the map $\hat{\varphi} : A^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(S_L)$ defined as

$$A^+ \xrightarrow{\varphi} S_L \xrightarrow{\mu} \mathrm{Sat}^+_{\mathrm{grp}}(S_L)$$

satisfies the desired property, where μ is defined by $\mu(a) := \mu(aa) := \{a, aa\}$, $\mu(ba) := \mu(baa) := \{ba, baa\}$ and $\mu(b) := \{b\}$, $\mu(0) := \{0\}$. Then one can check that, for example, the preimages of $\{a\}$ and $\{aa\}$ by $\hat{\varphi} = \mu \circ \varphi$ are both empty — which is FO-definable —, while the preimage of $\{a, aa\}$ is a^+ — which is also FO-definable.

Proof of 1.18. The full proof can be found in §B.1. The main technical difficulty lies in proving that the generalised product has an FO-approximation (lem. B.1). We prove this for every product $\pi : \mathcal{A}^+ \to \langle \mathcal{A} \rangle^{\cdot}$ where $\mathcal{A} \subseteq \mathcal{P}(U)$, by induction on $|\mathcal{A}|$ and $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$. The base case $|\mathcal{A}| = 1$ is easy, and follows from what we known about $a^+/{\equiv_k}$ (lem. 1.3). The inductive case $|\mathcal{A}| \geq 2$ is more tricky. We do a case disjunction on $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ using the induction principle (lem. 1.13). Case *(iii)* (when $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ has a maximum) is trivial. The other two cases, namely *(i)* and *(ii)*, — when one letter, say a, makes us fall into a smaller structure — is much more technical. The main idea is to decompose a word w into blocks of 'a' and non-'a', use the induction hypothesis on the size of the alphabet to treat the blocks of non-'a', and use the induction hypothesis on the size of the group saturation to "glue" the blocks together. □

This idea of "decomposing" a word into blocks and then "merging" the result, already present in Place & Zeitoun's proof [PZ16], was in fact described algebraically by van Gool & Steinberg as the "merge decomposition" [vGS19], which allowed them to obtain a purely algebraic, and succinct, proof of Henckell's theorem.

Exercise 1.20. Let φ be the syntactic morphism of $L := a(aa)^+ = a(aa)^* \setminus \{a\}$. Show that there is a unique function $\hat{\varphi} : a^+ \to S_L$ such that $\varphi(w) \in \hat{\varphi}(w)$ for all w, and that this function is not a semigroup morphism. A solution can be found in §C.2.

We can finally prove the completeness of Henckell's theorem.

Lemma 1.21: Completeness of Henckell's theorem. $\mathrm{Pl}_{\mathrm{FO}}(\varphi) \subseteq {\downarrow}\mathrm{Sat}^+_{\mathrm{grp}}(\varphi)$.

Proof. By theorem 1.18, the semigroup morphism $\varphi : A^+ \to U$ can be approximated by an FO-definable $\hat{\varphi} : A^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(\varphi)$. Let $k \in \mathbb{N}$ be an upperbound on the rank of a fixed family of first-order formulæ defining the preimages of $\hat{\varphi}$.

Such a k exists since U is finite, and hence there are finitely many preimages.

Consider a pointlike set $X \in \mathrm{Pl}_{\mathrm{FO}}(\varphi)$. Then there exists $L \in A^+/{\equiv_k}$ such that $X \subseteq \varphi[L]$, say $L = [w]_{\equiv_k}$. Observe that for $w' \in L$, since $w \equiv_k w'$, we have $\hat{\varphi}(w) = \hat{\varphi}(w')$, so $\hat{\varphi}[L] = \{\hat{\varphi}(w)\}$. Hence, we get

The equality $\hat{\varphi}(w) = \hat{\varphi}(w')$ follows from the fact that $\hat{\varphi}^{-1}[\hat{\varphi}(w)]$ is FO_k-definable.

$$X \subseteq \varphi[L] \subseteq \bigcup \hat{\varphi}[L] = \hat{\varphi}(w) \in \mathrm{Sat}^+_{\mathrm{grp}}(\varphi).$$

and thus $X \in {\downarrow}\mathrm{Sat}^+_{\mathrm{grp}}(\varphi)$, which concludes the proof of lem. 1.21 and of thm. 1.14. □

We finish this section by explaining how theorem 1.18 can also be used to prove the difficult implication of Schützenberger's theorem. Let $L \subseteq A^+$ be a language recognised by a finite aperiodic semigroup S, say $L = \varphi^{-1}[X]$ for some morphism $\varphi : A^+ \to S$ and some set $X \subseteq S$. By aperiodicity of S, we have that $\mathrm{Sat}^+_{\mathrm{grp}}(S) = S^{\mathrm{sgl}}$. Hence, by theorem 1.18, φ is FO-definable, from which it follows that L is also FO-definable.

2. Transfinite words

Many results for finite words can be generalised to ω-languages: regular ω-languages corresponds to MSO-definable languages, which are precisely the languages recognised by finite Wilke's algebras [Wil93] or finite ω-semigroups [PP04, §II.4]. Moreover, Perrin proved [Per84, §2] an extension of Schützenberger's theorem: FO-definable ω-languages are precisely the languages recognised by finite aperiodic Wilke's algebras, or, equivalently, by finite aperiodic ω-semigroups. Concerning FO-separability, Place & Zeitoun gave [PZ16, prop 9.3] an extension of Henckell's theorem: pointlike sets of an ω-semigroup morphism coincides with the downward closure of its omega group saturation, from which one can deduce the decidability of FO-separability for ω-languages — see exo. 2.43.

Recall that there is a small difference of terminology between Place & Zeitoun [PZ16] and us: our group saturation is not necessarily downward closed.

In this section, we focus on the generalisation of those results to transfinite languages: we start by explaining the results of Bedon [Bed98, Bed01] on the algebraic characterisation of MSO and FO-definability, and then prove a new result, which is a generalisation of Henckell's theorem to transfinite languages (thm. 2.37), from which one can immediately deduce the decidability of FO-separability for transfinite languages. To do this, we first introduce the algebraic structure (ordinal semigroups) that recognises transfinite regular languages in §2.1, before studying the local structure of finite ordinal semigroups in §2.2 and their idempotents in 2.3. We then emphasise a few properties of first-order logic on transfinite words and pointlike sets in §2.4 and introduce the notion of group saturation for ordinal semigroups §2.5. Finally, in §2.6, we claim and prove that these two notions are equivalent.

The complexity of Place & Zeitoun's algorithm for ω-languages is also ExpTime.

We assume that the reader is familiar with ordinals and ordinal arithmetic. Recall that given a family of ordinals indexed by an ordinal, say $(\alpha_\iota)_{\iota<\kappa}$, the sum of this family — in the sense of linear orders, see [Ros82, def. 1.38] for example —, is itself an ordinal, denoted by $\sum_{\iota<\kappa}\alpha_\iota$. The collection of all countable ordinals — or, equivalently, the least uncountable ordinal — is denoted by ω_1.

If needs be, the necessary definitions and elementary properties can be found in [Ros82, §3] or [Deh17, §II].

Why do we restrict ourselves to countable ordinals, and not study all ordinals? First, Büchi proved that the monadic second-order theory of countable ordinals was decidable [Büc73]. More generally, Rabin showed that the monadic theory of all countable linear orders was decidable [Rab69]. On the other hand, Gurevich and Shelah proved that the MSO-theory of the real line, and thus the monadic theory of all linear orders, was undecidable [GS82, She75].

Note that that there is a difference between the monadic theory of all countable ordinals and the monadic theory of ω_1: the former consists of all monadic formulæ true for every countable ordinal, while the latter consits of the formulæ that are true in ω_1. (But the latter theory is also decidable: see [Büc73].)

2.1. Ordinal semigroups

We start by introducing two key algebraic structures (ordinal semigroups and finitary ordinal semigroups) and then explain how those structures are related to transfinite languages.

A *transfinite word*, over the set X, is a map from a countable ordinal (called domain) to X. The set of all transfinite words (resp. non-empty transfinite words) over X is denoted by X^{ord} (resp. $X^{\mathsf{ord}+}$). These objects have stronger algebraic properties than X^* (resp. X^+): it is not only a monoid (resp. semigroup), but an ordinal monoid (resp. ordinal semigroup): not only can we concatenate two words, but we can concatenate any family of words, as long as this family is indexed by a (countable) ordinal.

Moreover, one can always consider a transfinite word whose letters are themselves transfinite words over X: thus we obtain a word $w \in (X^{\mathsf{ord}})^{\mathsf{ord}}$. By forgetting the parentheses, we obtain a word w^{flat} in X^{ord}. For example if $X = \{a, b, c\}$, then $w = (abbaab)(ccc\ldots)(aaa\ldots) \in (X^{\mathsf{ord}})^{\mathsf{ord}}$ has three letters, the last two of which are infinite words, and $w^{\mathsf{flat}} = abbaabccc\ldots aaa\ldots$ is a word of length $\omega 2$.

Definition 2.1. An *ordinal monoid* is a pair (M, π) where $\pi : M^{\mathsf{ord}} \to M$, called *generalised product*, satisfy the following axioms:

(OM$_1$). $\pi(x) = x$ for all $x \in M$,

(OM$_2$). $\pi((u_\iota)^{\mathsf{flat}}_{\iota<\kappa}) = \pi((\pi(u_\iota))_{\iota<\kappa})$ for every word $(u_\iota)_{\iota<\kappa} \in (M^{\mathsf{ord}})^{\mathsf{ord}}$.

The product of the empty word $\pi(\varepsilon)$ is denoted by 1, and called the identity of M.

Observe that this definition generalises the definition of a monoid since the product of a monoid can be seen as a map $\pi : M^* \to M$.

The axiom (OM$_2$), also called generalised associativity, is depicted as a commutative diagram in figure 3 and should be understood as follows: given a word whose elements belong to the monoid, one can arbitrarily decompose the word into smaller words, evaluate these smaller words, and then evaluate the result. Doing this should yield the same as evaluating the whole word at once.

$$\begin{array}{ccc} (M^{\mathsf{ord}})^{\mathsf{ord}} & \xrightarrow{-^{\mathsf{flat}}} & M^{\mathsf{ord}} \\ \downarrow{\scriptstyle \pi^{\mathsf{ord}}} & & \downarrow{\scriptstyle \pi} \\ M^{\mathsf{ord}} & \xrightarrow{\pi} & M \end{array}$$

Figure 3: Generalised associativity, diagrammatically.

We define ordinal semigroups in the same way, except that we do not talk about the empty word: an *ordinal semigroup* is a pair (S, π) where $\pi : S^{\mathsf{ord}+} \to S$ satisfies the axioms (OS$_1$) $\pi(x) = x$ for all $x \in S$, and (OS$_2$) $\pi((u_\iota)^{\mathsf{flat}}_{\iota<\kappa}) = \pi((\pi(u_\iota))_{\iota<\kappa})$ for every word $(u_\iota)_{\iota<\kappa} \in (S^{\mathsf{ord}+})^{\mathsf{ord}+}$.

One might notice that $-^{\mathsf{ord}}$ and $-^{\mathsf{ord}+}$ are monads in the category of sets, just like $-^*$ and $-^+$, and that ordinal monoids (resp. semigroups) are just objects of the Eilenberg-Moore category associated with the monad $-^{\mathsf{ord}}$ (resp. $-^{\mathsf{ord}+}$), which is what figure 3 expresses. A pedagogical introduction to monads in algebraic language theory can be found in [Boj20, §4].

Example 2.2. The set of all countable ordinals under the generalised sum $(\omega_1, \sum)$ is an ordinal monoid.

Given a set X, X^{ord} and $X^{\mathsf{ord}+}$ are the free ordinal monoid and the free ordinal semigroup over X. Observe that the free ordinal monoid generated by one element is isomorphic to $(\omega_1, \sum)$. Ordinal monoid (resp. ordinal semigroup) morphisms, congruences, etc. are defined as usual.

Just like one can see a monoid (M, π) with $\pi : M^* \to M$ as a triplet $(M, \cdot, 1)$ with $x \cdot y := \pi(xy)$ and $1 := \pi(\varepsilon)$, we can (try to) see ordinal monoids as finitary algebraic structures. However, in this case, the resulting structure (finitary ordinal monoids) will be not be equivalent to the original structure (ordinal monoids) — see example 2.7 — unless the underlying set is finite — see theorem 2.8.

This situation is quite similar to what is happening for ω-words, whose infitary algebraic structures (ω-semigroups, introduced in [PP04, §II.4]) are only equivalent to the fitary algebraic structures (Wilke's algebras, introduced in [Wil93]) when the underlying set is finite.

Given an ordinal monoid (M, π), define the product $\cdot : M \times M \to M$ and the omega power $-^\omega : M \to M$ by $x \cdot y := \pi(xy)$ and $x^\omega := \pi((x)_{i<\omega})$. For example, observe that, for $a, b \in M$, $(a \cdot b)^\omega$ is, by definition, the generalised product of the word containing ω copies of 'ab', which coincides with the word starting by an 'a', and then followed by ω copies of the word 'ba': we just proved that $(a \cdot b)^\omega = a \cdot (b \cdot a)^\omega$.

Definition 2.3. A *finitary ordinal monoid* is quadruple $(M, \cdot, -^\omega, 1)$ where $\cdot : M \times M \to M$, $-^\omega : M \to M$ and $1 \in M$ satisfy the following axioms, where x, y, z range over M:

Finite finitary ordinal monoids admit, by construction, a finite representation.

(FOM$_1$). $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(FOM$_2$). $(x^n)^\omega = x^\omega$ for $n < \omega$,

(FOM$_3$). $(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega$,

(FOM$_4$). $x \cdot 1 = x = 1 \cdot x$,

(FOM$_5$). $1^\omega = 1$.

Likewise, a *finitary ordinal semigroup* is a triple $(S, \cdot, -^\omega)$ satisfying the axioms (FOS$_1$) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, (FOS$_2$) $(x^n)^\omega = x^\omega$ for $n < \omega$ and (FOS$_3$) $(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega$, where x, y, z range over S. Morphisms, congruences, etc. are defined as usual.

See, e.g., [Boj20, lem. 4.11] for the definition of a congruence for algebras defined by a monad.

Example 2.4. Equip the set $\mathbb{N}$ of natural numbers with the product $\max : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and the omega power $S : \mathbb{N} \to \mathbb{N}$ defined by $S(n) := n+1$ for all $n \in \mathbb{N}_{>0}$ and $S(0) := 0$. This yields a finitary ordinal monoid T_ω whose identity is 0. It is abelian, and, moreover, every element of T_ω is idempotent.

For $n \in \mathbb{N}$, the equivalence relation on $\mathbb{N}$, defined by $x \sim_n y$ iff $x = y$ or both x and y are greater or equal to n, defines a finitary ordinal monoid congruence on T_ω. Hence, the quotient $T_\omega/{\sim_n}$ is itself a finitary ordinal monoid, denoted by T_n.

Indeed: $x \sim_n y$ and $x' \sim_n y'$ implies $\max(x, x') \sim_n \max(y, y')$ and $x \sim_n y$ implies $S(x) \sim_n S(y)$.

Exercise 2.5. Show that the following map defines a (finitary ordinal monoid) morphism:

$$\varphi : \begin{array}{ccc} (\omega_1, \sum) & \to & T_\omega \\ \alpha & \mapsto & \begin{cases} 0 & \text{if } \alpha = 0, \\ k & \text{if } \omega^{k-1} \leq \alpha < \omega^k \text{ with } k \in \mathbb{N}_{>0}. \end{cases} \end{array}$$

Fact 2.6. Every ordinal monoid (M, π) induces a finitary ordinal monoid, namely $(M, \cdot, -^\omega, 1)$, where $\cdot$ and $-^\omega$ are defined as before, and $1 := \pi(\varepsilon)$.

Fact 2.6 defines a faithful functor from the category of ordinal monoids to the category of finitary ordinal monoids.

Observe that the reason why ordinal monoids satisfy axiom (FOM$_2$) is because of the equality $n \cdot \omega = \omega$ from ordinal arithmetic. Likewise, the equality $1 + \omega = \omega$ induces the equality $x \cdot x^\omega = x^\omega$ for all $x \in M$ — which can also be deduced from (FOM$_3$) by taking $x = y$ and then applying (FOM$_2$).

For example, the finitary ordinal monoid induced by $(\omega_1, \sum)$ is $(\omega_1, +, - \cdot \omega, 0)$, where $+$ is the addition over ordinals and $- \cdot \omega$ is the right multiplication by ω. Unfortunately, in the process of going from an ordinal monoid to a finitary ordinal monoid, one can lose many information.

"One can lose many information" should be understood, formally, as "the forgetful functor is not injective on objects".

Example 2.7. Equip the set $\bar{\mathbb{R}}_{>0}$ of strictly positive real numbers together with $+\infty$ with the same generalised sum as usual, i.e. $\sum_{\iota<\kappa} x_\iota$ is the supremum of the finite sums $\sum_{i \in I} x_i$ where I ranges over finite subsets of κ. This yields an ordinal semigroup $(\bar{\mathbb{R}}_{>0}, \sum)$, and observe that the finitary ordinal semigroup it induces has a trivial omega power — in this context, we denote the omega power by $- \cdot \omega$ for sanity's sake — indeed, for every $x \in \bar{\mathbb{R}}_{>0}$, we have $x \cdot \omega = \sum_{i<\omega} x = +\infty$.

Consider a different generalised sum $\tilde{\sum}$, which is more lazy: $\tilde{\sum}_{\iota<\kappa} x_\iota$ is defined as $\sum_{\iota<\kappa} x_\iota$ if κ is finite, and $+\infty$ otherwise. Again, we obtain an ordinal semigroup. It is routine to check that $(\bar{\mathbb{R}}_{>0}, \sum)$ and $(\bar{\mathbb{R}}_{>0}, \tilde{\sum})$ are non-isomorphic, yet they induce the same finitary ordinal semigroup.

Hint: To prove that these two ordinal semigroups are non-isomorphic, one can consider the word $(2^{-i})_{i<\omega}$.

However, just like ω-semigroups and Wilke's algebras, when the underlying set is finite, the infinitary and finitary structures are equivalent.

Theorem 2.8: [Bed98, thm. 3.5.6]. Every finite finitary ordinal monoid is induced by a unique finite ordinal monoid.

As a corollary, finite ordinal monoids admit a finite representation.

Brief sketch of proof. A full proof can be found in [Bed98]. We quickly explain this equivalence as follows: given a finite finitary ordinal monoid $(S, \cdot, -^{\omega})$

- first, one can define a product $\pi : S^{\text{ord}+} \to S$ that extends $\cdot$ and $-^{\omega}$ — this part is rather easy: one can define π by transfinite induction on the length of the words since ω is cofinal in every countable limit ordinal and by using Ramsey's infinite theorem ;
- secondly, prove that (S, π) is an ordinal semigroup, by showing that the product π defined previously does not depend on the factorisation of the word used in the induction — this part is *much* more technical. □

The forgetful functor from the category of ordinal monoids to the category of finitary ordinal monoids induces an isomorphism of categories between finite ordinal monoids and finite finitary ordinal monoids.
For basic results on cofinality, see, e.g., [Deh17, §V.3.1].

In the rest of this report, we will often use finite ordinal semigroup and finite finitary ordinal semigroup interchangeably. Given a subset X of an ordinal semigroup (resp. finitary ordinal semigroup), we denote by $\langle X \rangle^{\pi}$ (resp. $\langle X \rangle^{\cdot,\omega}$) the ordinal subsemigroup (resp. finitary ordinal subsemigroup) generated by X. A corollary of 2.8 is that, in a finite ordinal semigroup, $\langle X \rangle^{\pi} = \langle X \rangle^{\cdot,\omega}$ for all X.

Note that not every (infinite) finitary ordinal monoid is induced by an ordinal monoid: for instance T_{ω} cannot be equipped with a generalised product π: otherwise $\pi(1\,2\,3\,\ldots)$ should be equal to $\max(1, 2, \ldots, n, \pi((n+1)\,(n+2)\,\ldots)) \geq n$ for every $n \in \mathbb{N}_{>0}$.

This sketch of proof of thm. 2.8 is very classical: Perrin & Pin [PP04, §II, thm. 5.1] used it to prove the equivalence between finite ω-semigroups and finite Wilke's algebra, and Carton, Colcombet & Puppis [CCP18, thm. 11] used it to prove the equivalence between infinitary and finitary finite algebraic structures for countable words. (Despite what the date of publication might suggest, Perrin & Pin's proof for omega words predates Bedon's proof for transfinite words.)

We now focus on the relation between those algebraic structures and transfinite languages. A transfinite language is said to be *regular* whenever it is recognised by a finite ordinal semigroup. We admit the following theorem.

Theorem 2.9: [Bed98, thm. 3.5.18]. A transfinite language is regular if, and only if, it is MSO-definable.

Short remark about the proof. Bedon proved ([Bed98, thm 3.5.17]) that a transfinite language is recognised by finite ordinal semigroup if, and only if, it can be defined using D-automata, and Büchi proved (see [Bed98, thm 4.3.1] or [Büc73]) that the latter condition is equivalent to being MSO-definable. □

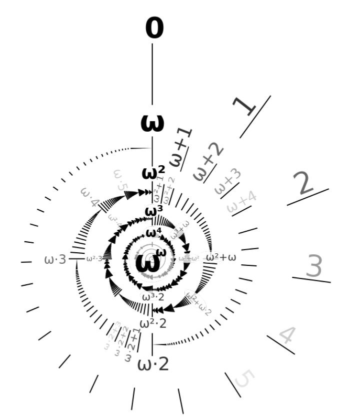


Figure 4: "Spirale représentant tous les nombres ordinaux inférieurs à ω^{ω}", licensed under CC 0, obtained from Wikimedia Commons.

Exercise 2.10. Let A be an alphabet, and consider the first-order formula

$$\forall x. \neg\, \text{first}(x) \Rightarrow \exists y.\ \text{pred}(y, x)$$

where $\text{pred}(y, x) := y < x \wedge (\forall z. z \leq y \vee x \leq z)$. Show that this formula defines all finite words over A and give a morphism recognising this language.

Exercise 2.11: ω^{ω}.

1. Prove that the finitary ordinal submonoid generated by A in A^{ord} is a finitary ordinal submonoid of $A^{[0,\omega^{\omega}[}$.
2. Given two regular transfinite languages L_1, L_2, show that $L_1 = L_2$ if, and only if, L_1 and L_2 coincides on words of length strictly less than ω^{ω}.

For a solution, see §C.3.

The ordinal ω^{ω} will play a quite important role in §2.4. In fact, ω^{ω} is rather fun: ω^{ω}, ω_1 and the proper class of all ordinals are WMSO-equivalent — see [Ros82, thm. 15.14]. However, note that Litman showed [Lit72, Büc73] that ω_1 is not MSO-equivalent with any countable ordinal: in particular ω^{ω} and ω_1 are not MSO-equivalent.

Just like for finite words, there is a canonical algebraic structure recognising a transfinite regular language L: its syntactic ordinal semigroup, which can be computed as a quotient of $A^{\mathsf{ord+}}$ by the syntactic congruence of L, denoted by $\sim_L$.

There is a general reason why everything works for ordinal semigroups just as they did for semigroups: monads. Bojańczyk proved [Boj15, thm. 1.1] that languages recognised by finitary algebras have a syntactic morphism. This result handles every language of finite words, every regular ω-language and regular transfinite languages. Note that in general, non-regular ω-languages and transfinite languages need not have a syntactic congruence: see, [Boj15, running ex. 2] or [Boj20, exercises 69 & 70].

Example 2.12. Let $L := a^*$. First, observe that $\varepsilon \not\sim_L u$ for any non-empty word $u \in a^{\mathsf{ord+}}$ since $\varepsilon^{\omega} = \varepsilon \in L$ while $u^{\omega} \notin L$. It follows that the syntactic congruence of L has three equivalence classes: $\{\varepsilon\}$, a^+ and $a^{\geq\omega}$. One can check that the syntactic ordinal monoid of L is T_2 — defined in example 2.4.

Exercise 2.13. More generally, show that over the alphabet $\{a\}$, the syntactic ordinal monoid of the language $L = a^{<\omega^n}$ is T_{n+1}, for every $n \in \mathbb{N}$.

For transfinite words, we also have a very nice characterisation of FO-definable transfinite regular language, which generalises Schützenberger's theorem.

Theorem 2.14: Bedon's theorem [Bed01]. A transfinite regular language is FO-definable if, and only if, its syntactic ordinal semigroup is aperiodic.

Example 2.15. Let $L = (aa)^{\mathsf{ord+}}$. Observe that L can be defined in MSO by:

$$\exists X.\, (\forall x.\, \mathrm{lim}(x) \Rightarrow X(x)) \wedge (\forall x.\, X(x) \Leftrightarrow \neg X(\mathrm{succ}(x))) \wedge (\forall x.\, \mathrm{last}(x) \Rightarrow \neg X(x)),$$

where:

$$\begin{aligned} \mathrm{lim}(x) &:= \neg\exists y.\ \mathrm{pred}(y,x), \\ X(\mathrm{succ}(x)) &:= \exists y.\ \mathrm{pred}(x,y) \wedge X(y), \\ \mathrm{last}(x) &:= \forall y.\, y \leq x. \end{aligned}$$

Moreover, for every $p, q \in \mathbb{N}$, $a^{2p} \sim_L a^{2q}$, $a^{2p+1} \sim_L a^{2q+1}$ and $a^{2p} \not\sim_L a^{2q+1}$. Then, for $p \in \mathbb{N}$, $a^{2p} \not\sim_L a^{\omega}$ since $a \cdot a^{2p} \notin L$ while $a \cdot a^{\omega} = a^{\omega} = (aa)^{\omega} \in L$, and, likewise, $a^{2p+1} \not\sim_L a^{\omega}$. Since $a^{\omega} \cdot a \notin L$, it follows that $a^{\omega} \cdot a \not\sim_L a^{\omega}$. We then claim that for any infinite ordinal $\alpha = \omega \cdot \alpha_1 + \alpha_0$, we have $a^{\alpha} \sim_L a^{\omega}$ if α_0 is even and $a^{\alpha} \sim_L a^{\omega} \cdot a$ otherwise. Hence, the syntactic ordinal semigroup has four elements, and its egg-box diagram is represented in figure 5.

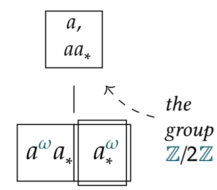


Figure 5: Egg-box diagram of the syntactic ordinal semigroup of $L = (aa)^{\mathsf{ord+}}$. The meaning of the box around a^{ω} is explained in §2.2.

Exercise 2.16. Let $A = \{a, b\}$.

1. Show that the egg-box diagram of the syntactic ordinal semigroup of $(ab)^{\mathsf{ord+}}$ is the one given in figure 6.
2. Compute the egg-box diagram of the syntactic ordinal semigroup of the language $A^{\mathsf{ord+}} \smallsetminus (A^{\mathsf{ord}}aaA^{\mathsf{ord}} + A^{\mathsf{ord}}bbA^{\mathsf{ord}})$ of words whose consecutive letters are not equal.

The solution can be found in §C.4

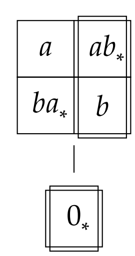


Figure 6: Egg-box diagram of the syntactic ordinal semigroup of $(ab)^{\mathsf{ord+}}$.

The curious reader can find more (fun) examples of ordinal semigroups and finitary ordinal semigroups in §A. We conclude the study of ordinal semigroups by introducing the notion power ordinal semigroup.

Definition 2.17. Let (U, π) be an ordinal semigroup. The map $\mathcal{P}(U)^{\mathsf{ord+}} \to \mathcal{P}(U)$ defined by

$$\Pi((X_\iota)_{\iota<\kappa}) := \left\{\pi((x_\iota)_{\iota<\kappa}) \mid x_\iota \in X_\iota \text{ for all } \iota < \kappa\right\}$$

gives an ordinal semigroup structure to $\mathcal{P}(U)$, called *power ordinal semigroup*.

Observe that the set union $\bigcup : \mathcal{P}(U) \to U$ defines an ordinal semigroup morphism and the singleton map $-^{\text{sgl}} : U \to \mathcal{P}(U)$ defined by $u^{\text{sgl}} := \{u\}$ is an injective morphism — hence, U can be seen as an ordinal subsemigroup of $\mathcal{P}(U)$.

Proposition 2.18. Let U be a finite ordinal semigroup. Then the finitary ordinal semigroup induced by the power ordinal semigroup of U is characterised by

$$X \cdot Y := \{x \cdot y \mid x \in X \text{ and } y \in Y\},$$
$$X^{\omega} := \{x \cdot y^{\omega} \mid x, y \in \langle X \rangle^{\cdot}\}.$$

As a corollary, given a finite representation of a finite ordinal semigroup, one can compute a finite representation of its power ordinal semigroup.

Proof. This first point is trivial, and the second one follows from Ramsey's infinite theorem. □

2.2. Green's relations on ordinal semigroups

We assume that the reader is familiar with basic properties of *Green's relations* $\leq_{\mathcal{L}}$, $\leq_{\mathcal{R}}$, $\leq_{\mathcal{J}}$ and $\leq_{\mathcal{H}}$ — say what is covered in [Pin20, §5.1, 5.2] (location theorem, egg-box diagrams and regular elements). Unless indicated otherwise, we follow the terminology of [Pin20]. The property stating that "if S is a finite semigroup, for all $s, t \in S$, then $s \leq_{\mathcal{L}} t \leq_{\mathcal{J}} s$ if, and only if, $s \mathrel{\mathcal{L}} t$", the dual property for $\leq_{\mathcal{R}}$, and their corollary for $\leq_{\mathcal{H}}$ are called *stability properties*.

In this subsection, we work in a finite ordinal semigroup S. In classical semigroup theory, the location theorem allows us to know whether to product of two elements of the same $\mathcal{J}$-class falls into a smaller $\mathcal{J}$-class — this is always the case if the class is not *regular*, i.e. does not contain an idempotent — and otherwise, one can compute the product up to $\mathcal{H}$-equivalence. In this subsection, we define the notion of ω-stability — which is the counterpart of regularity but for the omega power — and give a location theorem for the omega power. Moreover, we explain how we represent and read this information on an egg-box diagram.

Of course, we are in fact talking about $\mathcal{D}$-classes, but since we focus on finite semigroups $\mathcal{D} = \mathcal{J}$, so we do not bother ourselves with these details.

Recall that idempotent elements behave like the identity for elements that are smaller than them: formally, if e is idempotent and $s \leq_{\mathcal{L}} e$ (resp. $s \leq_{\mathcal{R}} e$) then $se = s$ (resp. $es = s$).

Fact 2.19. If $e \mathrel{\mathcal{J}} f$ are two idempotents in a finite semigroup, then there exists x, y such that $e = xy$ and $f = yx$.

For a proof, see [Pin20, prop 2.22].

Observe that if $x \in S$ then $x^{\omega} = (x^{\pi})^{\omega}$: the omega power is uniquely determined by its value on idempotents. In fact, this can be slightly refined.

Fact 2.20. If $e \mathrel{\mathcal{R}} f$ are idempotents, then $e^{\omega} = f^{\omega}$.

Proof. Since $e \mathrel{\mathcal{R}} f$ are idempotents, $ef = f$ and $fe = e$, so $e^{\omega} = (fe)^{\omega} = f \cdot (ef)^{\omega} = f \cdot f^{\omega} = f^{\omega}$ by (FOS$_3$). □

For example, in the ordinal semigroup defined in example 2.15 and depicted in figure 5, $a^{\omega}a$ and a^{ω} are two $\mathcal{R}$-equivalent idempotent, and have the same omega power, which is a^{ω} itself.

Proposition 2.21: [CS15, lemma 7]. If $s \mathrel{\mathcal{J}} ss \mathrel{\mathcal{J}} tt \mathrel{\mathcal{J}} t$, then $s^{\omega} \mathrel{\mathcal{L}} t^{\omega}$.

Proof. Let $e := s^\pi$ and $f := t^\pi$. Then the hypothesis $s \mathcal{J} ss$ yields, by stability, $s \mathcal{L} ss$ and hence $s \mathcal{L} s^n$ for all $n \in \mathbb{N}_{>0}$, from which we deduce $s \mathcal{J} e$. Likewise, $t \mathcal{J} f$ and hence $e \mathcal{J} f$. So, by proposition 2.19, there exists $x, y \in S$ such that $e = xy$ and $f = yx$. It follows that $e^\omega = xf^\omega$ and $f^\omega = ye^\omega$. □

For example, in the syntactic ordinal semigroup of $(ab)^{\mathsf{ord}+}$ (see exo. 2.16 & fig. 6), by letting $s := ab$ and $t := ba$ we have $s = ss \mathcal{J} tt = t$ and $s^\omega = ab \mathcal{L} b = t^\omega$.

Definition 2.22. We say that a $\mathcal{J}$-class J is *ω-stable* if one of the following equivalent conditions holds:

i. $\pi(x_0 x_1 \dots) \in J$ for some word $(x_i)_{i<\omega} \in J^\omega$;
ii. $x^\omega \in J$ for some $x \in J$;
iii. $e^\omega \in J$ for every idempotent $e \in J$ and J is regular.

The implications *(iii)* ⇒ *(ii)* ⇒ *(i)* are trivial. To prove that *(i)* ⇒ *(iii)*, one can use Ramsey's infinite theorem and proposition 2.21. See [CS15, lem. 10]

Observe that if G is a group in S, whose neutral element is denoted by 1_G, then for all $x \in G$, ($\textsc{fos}_2$) gives $x^\omega = (x^\pi)^\omega = 1_G^\omega$: the elements of a group all have the same omega power — in particular, the only ordinal semigroup that is also a group is the trivial group.

Proposition 2.23: [CS15, lem. 8, item 4]. Every ω-stable $\mathcal{J}$-class is $\mathcal{H}$-trivial.

Proof. Let J be an ω-stable $\mathcal{J}$-class, and let $a \in J$. For $b \mathcal{H} a$, we have $b^2 \mathcal{J} a^2$ so $a \mathcal{J} aa \mathcal{J} bb \mathcal{J} b$ and proposition 2.21 yields $a^\omega \mathcal{L} b^\omega$ and hence $b \mathcal{H} a \mathcal{J} a^\omega \mathcal{J} b^\omega$.

But observe that $b^\omega \leq_{\mathcal{R}} b$ — indeed, $b^\omega = b \cdot b^\omega$ — so, by stability, $b^\omega \mathcal{R} b$, and thus there exists $c \in S$ such that $b = b^\omega \cdot c$. Then $bb = b \cdot b^\omega \cdot c = b^\omega \cdot c = b$. Hence, every element of $H(a)$ is idempotent, so $H(a)$ is trivial. □

Indeed, if $e \leq_{\mathcal{H}} f$ are idempotents, then $ef = e = fe$, so every $\mathcal{H}$-class contains at most one idempotent.

Observe that by proposition 2.23 if a $\mathcal{J}$-class J is ω-stable, then it has a unique $\mathcal{L}$-class containing every omega power of elements of J that stays in J. This class is denoted by $\mathcal{L}_\omega(J)$.

Theorem 2.24: ω-location theorem. Let $x \in S$. If x is idempotent and $J(x)$ is ω-stable, then x^ω is the unique element of $R(x) \cap \mathcal{L}_\omega(J(x))$. Otherwise, $x^\omega <_{\mathcal{J}} x$.

Proof. First, since $x^\omega = x \cdot x^\omega$, we have $x^\omega \leq_{\mathcal{R}} x$ and thus $x^\omega \leq_{\mathcal{J}} x$. If x is not idempotent or $J(x)$ is not ω-stable, then $x^\omega <_{\mathcal{J}} x$ by prop. 2.23. Otherwise, if x is idempotent and $J(x)$ is ω-stable $x^\omega \mathcal{J} x$ so $x^\omega \mathcal{R} x$ by stability. Proposition 2.21 and the definition of $\mathcal{L}_\omega$ yield $x^\omega \in R(x) \cap \mathcal{L}_\omega(J(x))$. Finally, this $\mathcal{H}$-class indeed contains a unique element by proposition 2.23. □

Theorem 2.24 justifies the following choice: in the egg-box diagram of an ordinal semigroup, if a $\mathcal{J}$-class J is ω-stable, then we frame the $\mathcal{L}$-class $\mathcal{L}_\omega(J)$.

For example, in the syntactic ordinal semigroup of $(ab)^{\mathsf{ord}+}$ (see exo. 2.16 & fig. 6), both $\mathcal{J}$-class are ω-stable. The elements a and b are not idempotent, and hence $a^\omega <_{\mathcal{J}} a$ and $b^\omega <_{\mathcal{J}} b$ — from which we deduce $a^\omega = b^\omega = 0$. On the other hand, ab and ba are idempotents and belond to an ω-stable $\mathcal{J}$-class, and hence their ω-power can be read on the egg-box diagram as the unique element in the $\mathcal{R}$-class of ab (resp. ba) and in the framed $\mathcal{L}$-class. It follows that $(ab)^\omega = ab$ and $(ba)^\omega = b$.

In finite semigroups, every element x has a unique idempotent power x^π — which satisfies, by definition, $x^\pi = x^\pi \cdot x^\pi$ — but in an ordinal semigroup, this element need not satisfy $(x^\pi)^\omega = x^\pi$. We introduce the notion of ordinal idempotency and show that every element has a unique ordinal idempotent power. Finally, we give bounds on the ordinal power that reaches this ordinal idempotent power.

Definition 2.25: [CS15, §3.3]. In an ordinal semigroup, we say that an element x is *ordinal idempotent* when $x^\alpha = x$ for every countable ordinal $\alpha > 0$.

Proposition 2.26. In a finite ordinal semigroup, x is ordinal idempotent if, and only if, $x^\omega = x$.

Proof. The implication from left to right is trivial. For the converse implication, assume that $x^\omega = x$. Then observe that $x \cdot x = x \cdot x^\omega = x^\omega = x$ so x is idempotent. For $\alpha > 0$:

$$\begin{aligned} x^\alpha &\in \langle x \rangle^\pi && \text{by definition of } \langle x \rangle^\pi, \\ &= \langle x \rangle^{\cdot,\omega} && \text{by theorem 2.8}, \\ &= \{x\} && \text{since } x = x \cdot x = x^\omega. \end{aligned}$$ □

For example, in the finite ordinal semigroup T_n, every element is idempotent. However, only 0 and n are ordinal idempotent.

We define an *ordinal idempotent power* of x as an ordinal power, i.e. an element of the form x^α, $\alpha > 0$ — that is ordinal idempotent.

Theorem 2.27. In a finite ordinal semigroup S, every element $x \in S$ has a unique ordinal idempotent power, denoted by x^ρ. Moreover, the least ordinal $\alpha > 0$ such that $x^\alpha = x^\rho$ satisfies $\alpha \leq \omega^{|S|} < \omega^\omega$.

This theorem fails for infinite ordinal semigroups: for every non-empty alphabet A, no element of $A^{\mathsf{ord}+}$ has an ordinal idempotent power. We give a proof that uses Green's relations (and that does prove the bound $\alpha \leq \omega^{|S|}$). However, an elementary proof (which also proves the inequality $\alpha \leq \omega^{|S|}$) can be found in §B.2.

Proof. The uniqueness is straightforward: if $\alpha, \beta > 0$ are countable and such that both x^α and x^β are ordinal idempotent, then there exists a countable ordinal γ such that $\alpha \cdot \gamma = \gamma = \beta \cdot \gamma$ — one can build γ as follows: wlog. assume $\alpha \leq \beta$ and take $\gamma := \beta^\omega$ so that $\gamma \leq \alpha \cdot \gamma \leq \beta \cdot \gamma = \beta^{1+\omega} = \gamma$. Then:

$$x^\alpha = (x^\alpha)^\gamma = x^{\alpha\gamma} = x^\gamma = x^{\beta\gamma} = (x^\beta)^\gamma = x^\beta.$$

For the existence, consider the sequence $(x^\alpha)_{\alpha<\omega_1}$. It is decreasing wrt. the $\leq_\mathcal{R}$-preorder, but since S is finite, the sequence $(R(x^\alpha))_{\alpha<\omega_1}$ is stationary, and by letting R be its limit, we know that there is some ordinal α such that for all $\beta \geq \alpha$, $x^\beta \in R$. It follows that $J(R)$ is ω-regular, so by applying the ω-location theorem to $(x^\alpha)^\pi$ and $((x^\alpha)^\omega)^\pi$, we get that both elements belong the (trivial) $\mathcal{H}$-class $R \cap \mathcal{L}_\omega(J(R))$, and hence are equal. Therefore, $(x^\alpha)^\pi$ is an ordinal idempotent power of x. □

Proposition 2.28. In a finite ordinal semigroup S, for every $x \in S$ and $n \in \mathbb{N}$, either x^{ω^n} is ordinal idempotent, or the semigroup $\langle x^{\omega^n} \rangle^{\cdot}$ has size at most $|S| - n$.

Proof. See §B.3. □

This bound is tight: see figure 7.

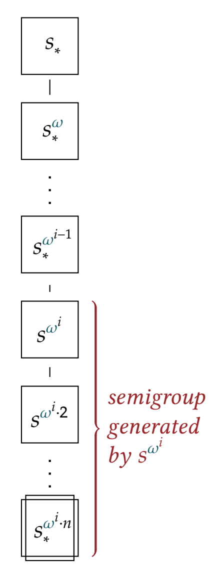


Figure 7: Egg-box diagram of a cyclic ordinal semigroup for which the bound of prop. 2.28 is tight.

We finally have a sufficiently good understanding of ordinal semigroups to be able to study the first-order logic over transfinite words. More precisely, we start by recalling what the equivalence classes of $A^{\mathsf{ord}+}$ under the first-order equivalence — this is a classical result —, before describing approximations of the $\textsc{fo}_k$ equivalence.

Define the $\textsc{fo}$-equivalence $\equiv$ and the $\textsc{fo}_k$-equivalence $\equiv_k$, where $k \in \mathbb{N}$, by $w \equiv w'$ (resp. $w \equiv_k w'$) whenever w and w' satisfy exactly the same formulæ of $\textsc{fo}$ (resp. $\textsc{fo}_k$). By Feferman-Vaught's theorem [Mak04, thm 1.3], both $\equiv$ and $\equiv_k$ are ordinal semigroup congruences. This can also be proven using Ehrenfeucht-Fraïssé games.

Fact 2.29. Let $u \in A^{\mathsf{ord}+}$ and $k \in \mathbb{N}$. For all $p, q \geq 2^k - 1$, we have $u^p \equiv_k u^q$.

The proof is similar to the proof for finite words.

Recall that over $\mathbb{N}_{>0}$, first-order logic was able to define every singleton $\{x\}$. This is trivially not true for ordinals — there are uncountably many countable ordinals but only countably many first-order formulæ! We emphasise a few ordinals and languages (subsets of $\omega_1 \setminus \{0\} \cong a^{\mathsf{ord}+}$) that are $\textsc{fo}$-definable.

Lemma 2.30. For each $n \in \mathbb{N}$ and $k \in \mathbb{N}_{>0}$, the languages $\{\omega^n \cdot k\}$, $[\omega^n \cdot k, \omega_1[$, and $]0, \omega^n \cdot k]$ are $\textsc{fo}$-definable.

Proof. See §B.4. □

This lemma can be used to prove the following proposition — that will not be used in the rest of the report, we only mention it because we think it is interesting!

Proposition 2.31: [Ros82, thm. 6.21]. Given two ordinals $\alpha = \omega^\omega \cdot \alpha_1 + \alpha_2$ and $\beta = \omega^\omega \cdot \beta_1 + \beta_2$ with $\alpha_2, \beta_2 < \omega^\omega$ we have $\alpha \equiv \beta$ if, and only if, $\alpha_2 = \beta_2$ and either α_1 and β_1 are both zero or both non-zero.

It is a good time to think back about exercise 2.11!

Finally, pointlike sets are defined exactly as before: given an ordinal semigroup morphism $\varphi : A^{\mathsf{ord}+} \to U$ where U is a finite ordinal semigroup

$$\mathrm{Pl}_{\textsc{fo}}(\varphi) := \left\{X \subseteq U \mid \forall k \in \mathbb{N},\ \exists L \in A^{\mathsf{ord}+}/{\equiv_k},\ X \subseteq \varphi[L]\right\}.$$

They satisfy exactly the same properties as do pointlike sets for finite words. In particular, to prove the decidability of $\textsc{fo}$-separability for transfinite words, it suffices to show that pointlike sets are computable.

Example 2.32: Running example. Let $L := b^{\mathsf{ord}+}(aa)^{\mathsf{ord}}$. One can check that the syntactic ordinal semigroup S_L of L has ten elements, which are split between six $\mathcal{J}$-classes. Among those classes, four are regular, and three of these regular classes are ω-stable. The syntactic ordinal semigroup of S_L is represented in figure 8.

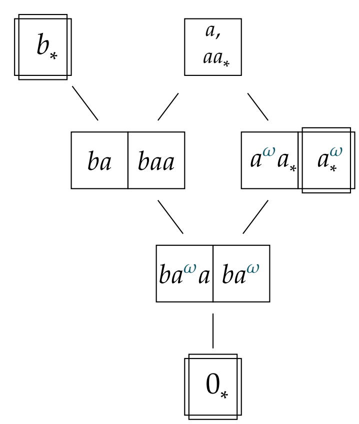


Figure 8: Egg-box diagram of the syntactic ordinal semigroup of $L := b^{\mathsf{ord}+}(aa)^{\mathsf{ord}}$.

Let $L_1 := L = b^{\mathsf{ord}+}(aa)^{\mathsf{ord}}$, $L_2 := (aa)^{\mathsf{ord}+}$ and $L_3 := (aa)^{\mathsf{ord}}a$. The syntactic ordinal semigroup S_L of L_1, and the syntactic ordinal semigroup of L_2 and L_3 (see ex. 2.15 & fig. 5) both contain the non-trivial group $\mathbb{Z}/2\mathbb{Z}$. Hence, by Bedon's theorem (thm. 2.14), none of these three languages are $\textsc{fo}$-definable.

However, L_1 and L_2 are $\textsc{fo}$-separable: indeed, one can express "the word starts with the letter b" in first-order logic. However, by fact 2.29, for every $k \in \mathbb{N}$, there exists $l \in \mathbb{N}$ such that $a^l \equiv_k (aa)^l$. It follows that $\{a, aa\} \in \mathrm{Pl}_{\textsc{fo}}(\varphi)$ where $\varphi : A^{\mathsf{ord}+} \to S_L$ is the syntactic morphism of L. This witnesses the non-$\textsc{fo}$-separability of L_2 and L_3.

We introduce the notion of group saturation for transfinite words and for words of length ω: the proof of the generalisation of Henckell's theorem to transfinite words relies on Henckell's theorem for finite words and Place & Zeitoun's generalisation of it to ω-words. We fix a finite ordinal semigroup U.

Definition 2.33. Let $\mathcal{A}$ be a subset of the power ordinal semigroup $\mathcal{P}(U)$. We define the following saturation operators:

- $\mathrm{Sat}^{\omega}_{\mathrm{grp}}(\mathcal{A}) := \{X \cdot Y^{\omega} \mid X, Y \in \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})\} = \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})^{\omega}$;
- $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathcal{A})$ is the least ordinal subsemigroup $\mathcal{S}$ of $\mathcal{P}(U)$ and stable under group merging, or equivalently, under cyclic group merging ;
- $\mathrm{Sat}^{\mathrm{ord}}_{\mathrm{grp}}(\mathcal{A})$ is the ordinal monoid obtained from $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathcal{A})$ by *always* adding an identity, denoted by ε.

Note that both $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ and $\mathrm{Sat}^{\omega}_{\mathrm{grp}}(\mathcal{A})$ are included in $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathcal{A})$. Moreover, those operators are monotonic under inclusion.

Proposition 2.34 is a generalisation of the identity $A^{\mathrm{ord}+} = A \cdot A^{\mathrm{ord}}$, which states that every non-empty word has a first letter. Of course, the dual statement is false since ordinals are not symmetric.

Proposition 2.34. $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathcal{A}) = \mathcal{A} \cdot \mathrm{Sat}^{\mathrm{ord}}_{\mathrm{grp}}(\mathcal{A})$.

Example 2.35: continuing ex. 2.32. The goal of this example is to compute $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(S_L)$. First, it contains ${S_L}^{\mathrm{sgl}}$. Then, since $\{\{a\}, \{aa\}\}$ is a group in $\mathcal{P}(S_L)$, we have $\{a, aa\} \in \mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(S_L)$. From the stability under product of the group saturation, we obtain that $\{ba, baa\}$, $\{a^{\omega}a, a^{\omega}\}$ and $\{ba^{\omega}a, ba^{\omega}\}$ all belong to $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(S_L)$. The egg-box diagram of $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(S_L)$ is represented in figure 9.

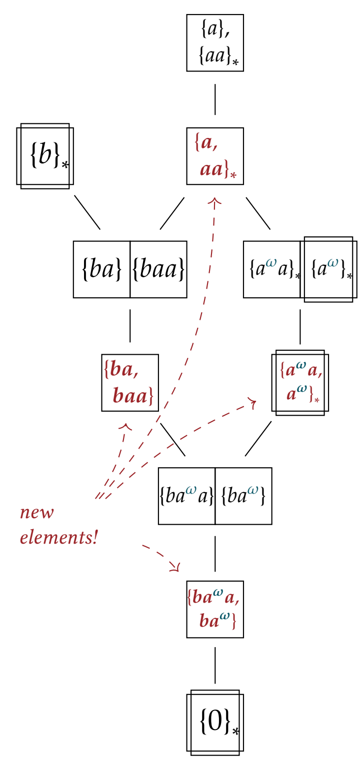


Figure 9: Egg-box diagram of the group saturation $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(S_L)$ of the syntactic ordinal semigroup of $L := b^{\mathrm{ord}+}(aa)^{\mathrm{ord}}$.

We give the counterpart of lemma 1.13 for transfinite words, which is the cornerstone of the induction used to prove the completeness of Henckell's theorem. It can be informally understood as: "either *(i)* we fall into a smaller structure by reading a single letter, or *(ii)* by reading any word of length ω, or *(iii)* the group saturation has a very simple structure".

Theorem 2.36: Induction principle for transfinite words. For every subset $\mathcal{A}$ of $\mathcal{P}(U)$, either:

i. there exists $a \in \mathcal{A}$ such that $a \cdot \mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathcal{A}) \subsetneq \mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathcal{A})$, or
ii. $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathrm{Sat}^{\omega}_{\mathrm{grp}}(\mathcal{A})) \subsetneq \mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathcal{A})$, or
iii. $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\mathcal{A})$ consists of a unique $\mathcal{L}$-trivial $\mathcal{R}$-class, and thus the generalised product $\pi : \mathcal{A}^{\mathrm{ord}+} \to \langle \mathcal{A} \rangle^{\cdot,\omega}$ is FO-definable.

For example, the group saturation $\mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(S_L)$, computed in ex. 2.35, falls in case *(i)* since $b \cdot \mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(S_L) \subsetneq \mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(S_L)$.

Proof of 2.36. See §B.5. Similar to the the proof of lem. 1.13 but we use properties specific to ordinals, and especially those that we established in §2.2. ☐

2.6. Generalisation of Henckell's theorem

We now have the necessary tools to state and prove a generalisation of Henckell's theorem for transfinite words.

Theorem 2.37. For every ordinal semigroup morphism $\varphi : A^{\mathrm{ord}+} \to U$ where U is a finite ordinal semigroup, $\mathrm{Pl}_{\mathrm{FO}}(\varphi) = {\downarrow}\, \mathrm{Sat}^{\mathrm{ord}+}_{\mathrm{grp}}(\varphi)$.

Corollary 2.38. FO-separability is decidable, and in ExpTime, for transfinite regular languages.

We assume that the input of the decision problem, i.e. the two transfinite regular languages, are specified by a finitary ordinal semigroup.

Proof. By theorem 2.37, since $\downarrow \mathrm{Sat}^{\mathrm{ord+}}_{\mathrm{grp}}(\varphi)$ is computable in exponential time. □

As for finite words, the proof of theorem 2.37 can be decomposed in two parts: a correctness result — lemma 2.39: every element of the group saturation is pointlike — and a completeness result — lemma 2.40: every pointlike set is included in an element of the group saturation.

Lemma 2.39: Correctness. $\downarrow \mathrm{Sat}^{\mathrm{ord+}}_{\mathrm{grp}}(\varphi) \subseteq \mathrm{Pl}_{\mathrm{FO}}(\varphi)$.

Proof. $\mathrm{Pl}_{\mathrm{FO}}(\varphi)$ contains every singleton $\{\varphi(w)\}$ with $w \in A^{\mathrm{ord+}}$ because "points are pointlike", it is an ordinal semigroup because, for every $k \in \mathbb{N}$, $\equiv_k$ is an ordinal semigroup congruence and finally, it is stable under group merging because of fact 2.29. □

Lemma 2.40: Completeness. $\mathrm{Pl}_{\mathrm{FO}}(\varphi) \subseteq \downarrow \mathrm{Sat}^{\mathrm{ord+}}_{\mathrm{grp}}(\varphi)$.

The proof of lemma 2.40 relies once again on a result stating that every morphism can be approximated by a FO-definable function.

Theorem 2.41: FO-approximation. For every morphism $\varphi : A^{\mathrm{ord+}} \to U$, where U is a finite ordinal semigroup, there exists an FO-definable function $\hat{\varphi} : A^{\mathrm{ord+}} \to \mathrm{Sat}^{\mathrm{ord+}}_{\mathrm{grp}}(U)$ such that $\varphi(w) \in \hat{\varphi}(w)$ for every $w \in A^{\mathrm{ord+}}$.

Of course, this can be extended to ordinal monoids: every morphism $A^{\mathrm{ord}} \to U$ can be approximated by an FO-definable function $A^{\mathrm{ord}} \to \mathrm{Sat}^{\mathrm{ord}}_{\mathrm{grp}}(U)$.

Example 2.42: continuing ex. 2.35. Consider the syntactic ordinal semigroup morphism of L, denoted by $\varphi : A^{\mathrm{ord+}} \to S_L$. It is not FO-definable: since $\varphi^{-1}[a]$, $\varphi^{-1}[aa]$, $\varphi^{-1}[ba]$, $\varphi^{-1}[baa]$, $\varphi^{-1}[a^\omega a]$, $\varphi^{-1}[a^\omega]$, $\varphi^{-1}[ba^\omega a]$ and $\varphi^{-1}[ba^\omega]$ are not FO-definable — always for the same reason: first-order logic cannot count modulo 2. However, by letting $\mu : S_L \to \mathrm{Sat}^{\mathrm{ord+}}_{\mathrm{grp}}(S_L)$ be defined as in table 1, we have that $\hat{\varphi} := \mu \circ \varphi : A^{\mathrm{ord+}} \to \mathrm{Sat}^{\mathrm{ord+}}_{\mathrm{grp}}(S_L)$ is FO-definable. For example, we now have

$$\hat{\varphi}^{-1}[\{a\}] = \hat{\varphi}^{-1}[\{aa\}] = \varnothing,$$

which is trivially FO-definable, and

$$\hat{\varphi}^{-1}[\{a, aa\}] = (aa)^+ + a(aa)^* = a^+,$$

which is also FO-definable. Likewise, the preimage $\hat{\varphi}^{-1}[\{a^\omega a, a^\omega\}]$ is the language of words whose letters are 'a' and containing infinitely many letters, i.e. $a^{\mathrm{ord+}} \setminus a^+$, which can be defined in FO by:

$$(\forall x.\, a(x)) \land (\exists x.\, \mathrm{lim}(x) \land \neg\, \mathrm{first}(x)).$$

x	$\mu(x)$
0	$\{0\}$
b	$\{b\}$
a	$\{a, aa\}$
aa	$\{a, aa\}$
ba	$\{ba, baa\}$
baa	$\{ba, baa\}$
$a^\omega a$	$\{a^\omega a, a^\omega\}$
a^ω	$\{a^\omega a, a^\omega\}$
$ba^\omega a$	$\{ba^\omega a, ba^\omega\}$
ba^ω	$\{ba^\omega a, ba^\omega\}$

Table 1: Recipe to make the syntactic morphism of L FO-definable.

Note that, in the proof of theorem 2.41, we first need to handle the case of ω-words (lemma B.4) before treating the general case (lemma B.5). This first step corresponds to Place & Zeitoun's proof of completeness of their generalisation of Henckell's theorem for ω-words [PZ16, §10.2].

Sketch of proof of 2.41. The full proof can be found in §B.6. First, we study morphism for ω-words (lemma B.4) — which corresponds to the completeness of Place & Zeitoun's generalisation of Henckell's theorem to ω-words [PZ16, §10.2]. We prove then proof a subcase of theorem 2.41 for the genralised product $\pi : \mathcal{A}^{\mathrm{ord+}} \to$

$\mathsf{Sat}^{\mathsf{ord}+}_{\mathsf{grp}}(\mathcal{A})$ with $\mathcal{A} \subseteq \mathcal{P}(U)$ (lemma B.5), by induction on $|\mathcal{A}|$ and $|\mathsf{Sat}^{\mathsf{ord}+}_{\mathsf{grp}}(\mathcal{A})|$. The base case $|\mathcal{A}| = 1$ is more difficult than for finite words: we need to prove some properties on the $\equiv_k$-classes. We use the results of §2.4 (more specifically lemma 2.30) and §2.3. Then, for the inductive case $|\mathcal{A}| \geq 2$, we study more precisely the group saturation of $\mathcal{A}$ and theorem 2.36 (induction principle) comes into play. Case *(iii)* (when the group saturation has a very simple structure) is easily handled. Case *(i)* (when one letter makes us fall into a smaller structure) is handled similarly to what Place & Zeitoun do for finite words (see [PZ16, §6.3] or §B.1). Finally, case *(ii)* (when ω-words makes us fall into a smaller structure) is handled using what have already been proven on ω-words (lemma B.4). □

Proposition 2.34 also plays a major role in the proof. The fact that the dual of this proposition is false is the reason why we do not single out the case $\mathsf{Sat}^{\mathsf{ord}+}_{\mathsf{grp}}(\mathcal{A}) \cdot a \subsetneq \mathsf{Sat}^{\mathsf{ord}+}_{\mathsf{grp}}(\mathcal{A})$ because this property does not give us any usable information.

Proof of 2.40. Exactly like the proof of 1.21: simply consider an FO-definable approximation $\hat{\varphi} : A^+ \to \mathsf{Sat}^{\mathsf{ord}+}_{\mathsf{grp}}(U)$ of φ. □

This concludes the proof of our generalisation of Henckell's theorem to transfinite languages.

Exercise 2.43. Deduce from theorem 2.37 the following propositions:

1. *Bedon's theorem:* see thm. 2.14.
2. *Place-Zeitoun's theorem*: For every ω-semigroup morphism $\varphi : A^\omega \to U$ where U is a finite ω-semigroup, $\mathrm{Pl}_{\mathrm{FO}}(\varphi) = {\downarrow}\,\mathsf{Sat}^{\omega}_{\mathsf{grp}}(\varphi)$.
3. *Perrin's theorem*: An ω-regular language is FO-definable if, and only if, its syntactic ω-semigroup is aperiodic.

For a formal definition of what an ω-semigroup is, see [PP04, §II].

A. More examples of (finitary) ordinal semigroups

A.1. Successor and limit ordinals

The equivalence relation on ω_1 defined by $x \sim y$ if, and only if, both x and y are successor ordinals or both are limit ordinals is a finitary ordinal semigroup congruence. The quotient $\omega_1/\sim$ has two elements, denoted by λ and σ, which are the class of limit ordinal and successor ordinals, respectively. Its egg-box diagram is represented in figure 10

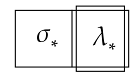


Figure 10: Egg-box diagram of $\omega_1/{\sim}$.

A.2. Banach-Picard & the semigroup of contractions

Let (E, d) be a non-empty complete metric space and let $\mathcal{C}(E)$ be the semigroup of contractions over E — recall that a contraction is a map $f : E \to E$ such that there exists some constant $k \in [0, 1[$ such that $d(f(x), f(y)) \leq kd(x, y)$ for all $x, y \in E$. By Banach-Picard theorem, every map $f \in \mathcal{C}(E)$ has a unique fixpoint, which is equal to $\lim_{n\infty} f^n(x)$ for all $x \in E$. By defining f^ω as the constant map $x \mapsto \lim_{n\infty} f^n(x)$, we obtain a finitary ordinal semigroup $(\mathcal{C}(E), \circ, -^\omega)$.

Indeed it satisfies (FOS_2) since $\lim_{n\to\infty} f^n(x) = \lim_{n\to\infty}(f^k)^n(x)$ for every $k \in \mathbb{N}$. Moreover, its satisfies (FOS_3) since, if λ is the fixpoint of $f \circ g$, then $f \circ g(\lambda) = \lambda$ and hence by postcomposing with g, it follows that $g(\lambda)$ is a fixpoint (and hence the unique fixpoint) of $g \circ f$. Therefore, $(g \circ f)^\omega = g \circ (f \circ g)^\omega$.

A.3. Real numbers

Equip the open interval $]0, 1[$ with the max operator and the omega power defined by $x^\omega := \frac{x+1}{2}$ for all $x \in]0, 1[$. Then $(]0, 1[, \max, -^\omega)$ is a finitary ordinal semigroup: indeed, it satisfies (FOS_3) since

$$\frac{\max(x, y) + 1}{2} = \max\left(x, \frac{\max(y, x) + 1}{2}\right).$$

Every $\mathcal{J}$-class of $]0, 1[$ is trivial: indeed, $x \leq_{\mathcal{J}} y$ iff $x \geq y$ (where $\geq$ refers to the usual ordering of the reals), so this ordinal semigroup has uncountably many $\mathcal{J}$-classes. All of them are regular, yet none are ω-stable.

B. Missing proofs

B.1. Proof of theorem 1.18

Before proving theorem 1.18, we start by proving the following lemma, which states that the product in a power semigroup is FO-approximable.

Lemma B.1. For every alphabet $\mathcal{A} \subseteq \mathcal{P}(U)$, there exists an FO-definable map $\hat{\pi} : \mathcal{A}^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ such that $\pi(w) \subseteq \hat{\pi}(w)$ for all $w \in \mathcal{A}^+$.

Proof of B.1. Fix a semigroup U. We prove the statement of this lemma by induction on $|\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})|$ and $|\mathcal{A}|$.

❧ **First case: $|\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})| = 1$.** The constant map $\hat{\pi} : \mathcal{A}^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ satisfies the property since $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ and $\langle \mathcal{A} \rangle^{\cdot}$ are trivial.

$\langle \mathcal{A} \rangle^{\cdot}$ is always a subsemigroup of $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$.

❧ **Second case: $|\mathcal{A}| = 1$.** Let $\mathcal{A} = \{a\}$ and observe that $\langle \mathcal{A} \rangle^{\cdot}$ is a cyclic semigroup. Let $n \leq |\langle \mathcal{A} \rangle^{\cdot}|$ be the least integer such that a^n belong to the maximal group $\mathcal{G}$ in $\langle \mathcal{A} \rangle^{\cdot}$. For $w = a^k \in \mathcal{A}^+$, let

$$\hat{\pi}(w) = \begin{cases} \{\pi(w)\} = \{\pi(a^k)\} & \text{if } k < n, \\ \bigcup \mathcal{G} & \text{otherwise.} \end{cases}$$

Then $\hat{\pi}$ is FO-definable — indeed, the preimage by $\hat{\pi}$ of $\{\{a^k\}\}$ with $k < n$ is the singleton $\{a^k\}$, and the preimage of $\{\bigcup \mathcal{G}\}$ is the language $\{a^k \mid k \geq n\}$, and we clearly have $\pi(w) \subseteq \hat{\pi}(w)$ for all $w \in \mathcal{A}^+$.

❧ **Third case: $|\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})| \geq 2$ and $|\mathcal{A}| \geq 2$.** By induction principle (lemma 1.13), either there exists $a \in \mathcal{A}$ such that $a \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A}) \subsetneq \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$, or there exists a such that $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A}) \cdot a \subsetneq \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$, or $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ has a maximum.

❧❧ *First subcase: $a \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A}) \subsetneq \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ for some $a \in \mathcal{A}$.* Let $\mathcal{B} := \mathcal{A} \setminus \{a\}$ and observe that $\mathcal{A}^* = \mathcal{B}^*(a^+\mathcal{B}^+)^*a^*$. Since $\{a\}$ and $\mathcal{B}$ are strictly smaller alphabets than $\mathcal{A}$, by induction hypothesis, there exists FO-definable maps $f_a : a^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(a)$ and $f_{\mathcal{B}} : \mathcal{B}^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{B})$ such that $\pi(w) \subseteq f_a(w)$ for every $w \in a^+$ and $\pi(w) \subseteq f_{\mathcal{B}}(w)$ for every $w \in \mathcal{B}^+$.

To prove this, given a word $w \in \mathcal{A}^*$, consider every position labelled by an 'a' that is not preceded by another 'a' — these positions are called *distinguished*.

The hypothesis $a \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A}) \subsetneq \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ together with proposition 1.12 yields

$$\mathrm{Sat}^+_{\mathrm{grp}}(\mathrm{Sat}^+_{\mathrm{grp}}(a) \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{B})) \subseteq a \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A}) \subsetneq \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A}),$$

so by induction hypothesis, there exists an FO-definable map

$$g : [\mathrm{Sat}^+_{\mathrm{grp}}(a) \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{B})]^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(\mathrm{Sat}^+_{\mathrm{grp}}(a) \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{B}))$$

such that $\pi(w) \subseteq g_{a\mathcal{B}}(w)$ for every word $w \in [\mathrm{Sat}^+_{\mathrm{grp}}(a) \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{B})]^+$. We define $\hat{\pi} : \mathcal{A}^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ by, for every $w = w_{\mathcal{B}}(w_{a,i}w_{\mathcal{B},i})_{i<k}w_a \in \mathcal{A}^* = \mathcal{B}^*(a^+ \cdot \mathcal{B}^+)^*a^*$:

$$\hat{\pi}(w) := f_{\mathcal{B}}(w_{\mathcal{B}}) \cdot g\left((f_a(w_{a,i}) \cdot f_{\mathcal{B}}(w_{\mathcal{B},i}))_{i<k}\right) \cdot f_a(w_a),$$

which is FO-definable since f_a, $f_{\mathcal{B}}$ and g are FO-definable, and since distinguished positions can be defined in first-order logic. Furthermore, by definition,

A way of formally proving that $\hat{\pi}$ is FO-definable would be to use an FO-interpretation (in the model-theoretic sense, see, e.g., [Grä07, def 3.5.7]).

Why $\mathrm{Sat}^*_{\mathrm{grp}}(-)$ and not $\mathrm{Sat}^+_{\mathrm{grp}}(-)$? Because $w_{\mathcal{B}}$, w_a and $(w_{a,i}w_{\mathcal{B},i})_{i<k}$ can be empty — but never all three at the same time!

$$\hat{\pi}(w) \in \mathrm{Sat}^*_{\mathrm{grp}}(\mathcal{B}) \cdot \mathrm{Sat}^*_{\mathrm{grp}}(\mathrm{Sat}^+_{\mathrm{grp}}(a) \cdot \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{B})) \cdot \mathrm{Sat}^*_{\mathrm{grp}}(a) \subseteq \mathrm{Sat}^*_{\mathrm{grp}}(\mathcal{A}),$$

and since w is not empty $\hat{\pi}(w) \in \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$. The inclusion $\pi(w) \subseteq \hat{\pi}(w)$ follows from the monotonicity of the product in a power semigroup.

❧❧ *Second subcase: $\mathrm{Sat}^+_{grp}(\mathcal{A}) \cdot a \subsetneq \mathrm{Sat}^+_{grp}(\mathcal{A})$ for some $a \in \mathcal{A}$.* This case is symmetric with the first subcase.

❧❧ *Third subcase: $\mathrm{Sat}^+_{grp}(\mathcal{A})$ has a maximum.* Define $\hat{\pi} : \mathcal{A}^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ to be the constant map, sending every word to the maximum of the group saturation: it is clearly FO-definable — its preimages are $\varnothing$ and $\mathcal{A}^+$ —, and over-approximate the product $\pi : \mathcal{A}^+ \to \langle A \rangle^{\cdot}$, which concludes the proof of lemma B.1. □

Observe that in the third case, we never used the hypothesis "$|\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})| \geq 2$", so we could have included the first case (when $\mathrm{Sat}^+_{\mathrm{grp}}(\mathcal{A})$ is trivial) in subcase 3 of case 3.

Proof of 1.18. The morphism $\varphi : A^+ \to U$ can be factorised as

$$\varphi = \underbrace{\bigcup}_{\substack{\text{projection}\\ \text{on } U}} \circ\, \pi{\restriction}_{U^{\mathrm{sgl}}} \circ \underbrace{-^{\mathrm{sgl}}}_{\substack{\text{lift to}\\ \mathcal{P}(U)}} \circ\, \varphi^+$$

where $\varphi^+ : A^+ \to U^+$ is the letter-to-letter map induced by φ and $\pi{\restriction}_{U^{\mathrm{sgl}}}$ is the restriction of the product $\pi : \mathcal{P}(U)^+ \to \mathcal{P}(U)$ on $\mathcal{P}(U)$ to the subsemigroup of singletons of $\mathcal{P}(U)$, and consider the alphabet U^{sgl} — without loss of generality, we assume that φ is surjective: otherwise, replace U by the image of φ.

By lemma B.1, there exists an FO-definable map $\hat{\pi} : U^{\mathrm{sgl}} \to \mathrm{Sat}^+_{\mathrm{grp}}(U^{\mathrm{sgl}})$ such that $\pi(w) \subseteq \hat{\pi}(w)$ for all $w \in (U^{\mathrm{sgl}})^+$. Since $\mathrm{Sat}^+_{\mathrm{grp}}(U^{\mathrm{sgl}}) = \mathrm{Sat}^+_{\mathrm{grp}}(\varphi)$ by definition of the latter object, we define the map $\hat{\varphi} : A^+ \to \mathrm{Sat}^+_{\mathrm{grp}}(\varphi)$ as $\bigcup \circ \hat{\pi} \circ -^{\mathrm{sgl}} \circ \varphi^+$: it is then routine to check that $\varphi(w) \in \hat{\varphi}(w)$ for all $w \in A^+$. The FO-definability of φ follows from the FO-definability of $\hat{\pi}$ and from φ^+ being a letter-to-letter map. □

The first step of this proof can be understood as "every deterministic morphism can be seen as a non-deterministic morphism". Observe that the induction of lemma B.1, even if one starts with deterministic objects (i.e. $\mathcal{A}$ only consists of singletons), the induction step will make the object non-deterministic, because of group saturation.

B.2. Elementary proof of theorem 2.27

Proof of 2.27 (existence of the ordinal idempotent power). Consider the finite directed graph whose vertices are the powers $\{x^\alpha \mid 0 < \alpha < \omega_1\}$ of x with an edge $y \to z$ if and only if $z = y^\omega$. Since every vertex has at least one outgoing edge, the graph has a cycle

$$y_0 \to y_1 \to \cdots \to y_{n-1} \to y_0$$

of size n. We want to show that this cycle is a loop, i.e. $n = 0$. For all $i \in \mathbb{Z}/n\mathbb{Z}$, we have:

$$y_i = y_{i-1}^\omega = y_{i-1} \cdot y_{i-1}^\omega = y_{i-1} \cdot y_i = y_{i-2}^\omega \cdot y_i = \ldots = y_{i-k}^{\omega^{k-1}} \cdot y_i = \ldots = y_i^{\omega^{n-1}} \cdot y_i = y_i^{\omega^{n-1}+1}$$

and hence

$$y_i^\omega = y_i^{(\omega^{n-1}+1)\omega} = y_i^{\omega^n},$$

i.e. $y_{i+1} = y_i$. Hence $y_0 = y_1 = \ldots = y_{n-1}$ and thus $n = 0$, i.e. our graph has a self-loop, from which it follows that x has an ordinal idempotent power. □

B.3. Proof of proposition 2.28

We start by generalising prop. 2.26 as follows.

Proposition B.2. In a finite ordinal semigroup an element x is ordinal idempotent if, and only if, $x^\lambda = x$ for some limit ordinal λ.

Proof of B.2. As usual, the implication from left to right is trivial. For the converse implication, assume that $x^\lambda = x$ where λ is a limit ordinal. First notice that x is idempotent — cf. proof of 2.26 —, and then that we can assume wlog. that $\lambda < \omega^\omega$ — see exo. 2.11. It follows that $x = x^\lambda \leq_{\mathcal{R}} x^\omega \leq_{\mathcal{R}} x$, so $(x^\omega)^\pi \mathrel{\mathcal{R}} x$, and thus by fact. 2.20, $x^{\omega^2} = x^\omega$, from which we get, by trivial induction on $n \in \mathbb{N}_{>0}$ that $x^{\omega^n} = x^\omega$, and hence by using Cantor's normal form on $\lambda < \omega^\omega$, we get $x^\lambda = x^{\omega \cdot p}$ for some $k, p \in \mathbb{N}$. Thus, $x = x^{\omega \cdot p}$, and hence $x \leq_{\mathcal{H}} x^\omega$, so by stability $x \mathrel{\mathcal{H}} x^\omega$, and thus $x = x^\omega$ by prop. 2.23. The conclusion follows from prop. 2.26. □

Note that there are some elements x such that $x^\alpha = x$ for every successor ordinal, yet x is not idempotent: see §A.1.

Proof of 2.28. Let $x \in S$ and $n \in \mathbb{N}$. We want to show that the semigroup generated by x^{ω^n} contains at most $|S| - n$ elements if x^{ω^n} is not ordinal idempotent. We do that by first showing that $x^{\omega^m} \notin \langle x^{\omega^n} \rangle^\cdot$ for all $m < n$: indeed, otherwise $x^{\omega^m} = x^{\omega^n \cdot k}$ for some $n \in \mathbb{N}$ and hence, by prop. B.2, x^{ω^m} would be ordinal idempotent, and thus so would x^{ω^n}. Then, observe that the elements $(x^{\omega^m})_{m<n}$ are pairwise distinct for the same reason. □

B.4. Proof of lemma 2.30

The proof relies on condensations — see, e.g., [Ros82, §4] for an introduction to the subject —, and more particularly on the finite condensation. A *condensation* of an ordinal α is an equivalence relation $\sim$ over α such that if $x \sim z$ and $x \leq y \leq z$ then $x \sim y \sim z$. Equivalently, it is an equivalence relation whose classes are convex. The quotient of an ordinal by a condensation is still an ordinal.

This has nothing to do with ordinals: we can define condensations on any linear order.

The finite condensation $\sim_{\mathsf{fin}}$ over α is the condensation defined by $x \sim_{\mathsf{fin}} y$ whenever $[x, y]$ is finite. For example, the ordinal $\omega \cdot 3$ — see fig. 11 — has 3 equivalence classes under the finite condensation $[0, \omega[$, $[\omega, \omega \cdot 2[$ and $[\omega \cdot 2, \omega \cdot 3[$, and hence $\omega \cdot 3/{\sim_{\mathsf{fin}}} = 3$. More generally, one can show that for $\alpha < \omega_1$ and $n < \omega$, we have $(\omega \cdot \alpha + n)/{\sim_{\mathsf{fin}}} = \alpha$ if $n = 0$ and $\alpha + 1$ otherwise. In particular, the three smallest ordinals β satisfying $\beta/{\sim_{\mathsf{fin}}} = \beta$ are 0, 1 and ω^ω.

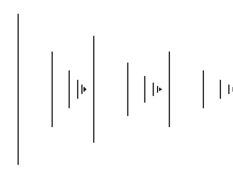


Figure 11: The ordinal $\omega \cdot 3$.

Interestingly, the finite condensation is definable in first-order logic, in the following sense.

Proposition B.3. For every first-order formula φ, there exists a first-order formula $\varphi^\dagger$ such that for every ordinal $\alpha < \omega_1$:

$$\alpha \models \varphi^\dagger \iff \alpha/{\sim_{\mathsf{fin}}} \models \varphi$$

and, moreover, $\mathrm{rk}(\varphi^\dagger) = \mathrm{rk}(\varphi) + 2$.

Proof. Trivial, by using an FO-interpretation — in the model-theoretic sense, see, e.g., [Grä07, def 3.5.7] — whose domain formula is $\mathrm{lim}(x)$, which is a formula of rank 2. □

As an immediate corollary of prop. B.3, for all α, β, for every $k \in \mathbb{N}$, if $\alpha \equiv_{k+2} \beta$ then $\alpha/{\sim_{\mathsf{fin}}} \equiv_k \beta/{\sim_{\mathsf{fin}}}$.

Proof of 2.30. We prove by induction on $n \in \mathbb{N}$ that for all $k \in \mathbb{N}_{>0}$, the language $\{\omega^n \cdot k\}$ is FO-definable. The base case $n = 0$ is trivial: it follows from exo. 2.10 and lem. 1.3.

Assume that the property holds for $n \in \mathbb{N}$, and let us build a formula defining $\{\omega^{n+1} \cdot k\}$. Observe that $(\omega^{n+1} \cdot k)/\sim_{\mathsf{fin}} = \omega^n \cdot k$. By induction hypothesis, there exists a formula $\varphi \in$ FO such that φ is exactly satisfied by $\{\omega^n \cdot k\}$. Then by prop. B.3, for every ordinal $\alpha \in]0, \omega_1[$, we have $\alpha \models \varphi^\dagger$ iff $\alpha/\sim_{\mathsf{fin}} = \omega^n \cdot k$ i.e. $\alpha = \omega^{n+1} \cdot k$. This concludes the induction.

Then one can deduce that $[\omega^n \cdot k, \omega_1[$ is FO-definable by observing that if φ defines exactly $\{\omega^n \cdot k\}$ then $\exists x. \varphi^{<x}$ defines $]\omega^n \cdot k, \omega_1[$. □

B.5. Proof of theorem 2.36

Recall that we want to show that either:

i. $a \cdot \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A}) \subsetneq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ for some $a \in \mathcal{A}$, or
ii. $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathsf{Sat}^{\omega}_{\mathsf{grp}}(\mathcal{A})) \subsetneq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$, or
iii. $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ consists of a unique $\mathcal{L}$-trivial $\mathcal{R}$-class, and thus the product $\pi : \mathcal{A}^{\mathsf{ord+}} \to \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ is FO-definable.

Proof of 2.36. Assume that *(i)* and *(ii)* do not hold. Then let J be a maximal $\mathcal{J}$-class in $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$. For $X \in J$, by $\neg$*(i)*, we have $X \leq_{\mathcal{R}} a$ for every $a \in \mathcal{A}$, and hence, by $\mathcal{J}$-maximality of J, $X \mathrel{\mathcal{R}} a$. Hence $\mathcal{A} \subseteq J$ — from which we deduce the uniqueness of the maximal $\mathcal{J}$-class — and J is an $\mathcal{R}$-class.

We consider Green's relations over $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$.

Moreover, for $X \in J$, by $\neg$*(ii)* we get $X = Y \cdot Z^\omega \leq_{\mathcal{J}} Z^\omega$ for some $Y, Z \in \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$, so $X \leq_{\mathcal{J}} Z$ and thus, by $\mathcal{J}$-maximality of X, $X \mathrel{\mathcal{J}} Z$, from which we get $Z \mathrel{\mathcal{J}} X \leq_{\mathcal{J}} Z^\omega \leq_{\mathcal{J}} Z$ so J is ω-stable.

Since J is ω-stable, it is $\mathcal{H}$-trivial by prop. 2.23, and thus $\mathcal{L}$-trivial since J is an $\mathcal{R}$-class. Furthermore, since J is ω-stable, it is regular, so every $\mathcal{L}$-class must contain an idempotent. By $\mathcal{L}$-triviality, it follows that J only contains idempotents.

For $E, F \in J$, since $E \mathrel{\mathcal{R}} F$ are idempotents, we have $E \cdot F = F$. Together with the ω-stability of J, it yields that any product of elements of J stays in J — more precisely, if κ is a limit ordinal, then $\pi((w_\iota)_{\iota<\kappa})$ is the unique element of J that can be written as an ω-power, and otherwise $\pi((w_\iota)_{\iota<\kappa}) = w_\theta$ where θ is the greatest position in κ. Hence, the restriction of the product of $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ indeed yields a map $\pi : J^{\mathsf{ord+}} \to J$ — said otherwise, J is an ordinal subsemigroup of $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$. The equality $J = \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(J)$ follows from J being an $\mathcal{H}$-trivial (and hence group-trivial) ordinal semigroup. But since $\mathcal{A} \subseteq J$ we get $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A}) \subseteq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(J) = J$ so $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A}) = J$ is indeed an $\mathcal{L}$-trivial $\mathcal{R}$-class.

Finally, the FO-definability of $\pi : \mathcal{A}^{\mathsf{ord+}} \to \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ is straighforward: for $X \in \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$, if X is not the unique ω-power of $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$, then the preimage of X is the set of words that have a last position, and this position is labelled by X ; if X is the unique ω-power of $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ — i.e. the unique element of $\mathcal{L}_\omega(J)$ —, then the preimage of X is the set of words that do not have a last position, or that have a last position and this position is labelled by X. □

In fact the FO-definability of π is also a corollary of Bedon's theorem since J is aperiodic — but this is overkill.

As for finite words, we prove that the product can be FO-approximated before showing the general result. First, we need to treat the case of words of length ω. We fix a finite ordinal semigroup U.

Lemma B.4. For every $\mathcal{A} \subseteq \mathcal{P}(U)$, there exists an FO-definable function $\hat{\pi} : \mathcal{A}^\omega \to \mathrm{Sat}^{\omega}_{\mathrm{grp}}(\mathcal{A})$ such that $\pi(w) \subseteq \hat{\pi}(w)$ for every $w \in \mathcal{A}^\omega$.

This lemma corresponds to [PZ16, prop 10.2]

Proof. Proof by induction on $|\mathcal{A}|$ and $|\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})|$.

This is not a typo.

❧ **First case: $|\mathcal{A}| = 1$.** Then $\mathcal{A}^\omega$ consists of a single word, so every map whose domain is $\mathcal{A}^\omega$ is FO-definable.

❧ **Second case: $|\mathcal{A}| \geq 2$.** By induction principle for finite words (lem. 1.13), either *(i)* there exists $a \in \mathcal{A}$ such that $a \cdot \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \subsetneq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$, or *(ii)* there exists $a \in \mathcal{A}$ such that $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \cdot a \subsetneq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$, or *(iii)* $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ has a maximum.

❧❧ *First subcase: $a \cdot \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \subsetneq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ for some $a \in \mathcal{A}$.* Let $\mathcal{B} = \mathcal{A} \setminus \{a\}$ and consider the decomposition $\mathcal{A}^\omega = L_a + L_{\mathcal{B}} + L_{a\mathcal{B}}$, with $L_a = \mathcal{B}^*(a^+\mathcal{B}^+)^* a^\omega$, $L_{\mathcal{B}} = \mathcal{B}^\omega + \mathcal{B}^*(a^+\mathcal{B}^+)^* a^+ \mathcal{B}^\omega$ and $L_{a\mathcal{B}} = \mathcal{B}^*(a^+\mathcal{B}^+)^\omega$. which can be done in first-order logic. We define $\hat{\pi} : \mathcal{A}^\omega \to \mathrm{Sat}^{\omega}_{\mathrm{grp}}(\mathcal{A})$ by defining its restrictions to L_a, $L_{\mathcal{B}}$ and $L_{a\mathcal{B}}$ — we focus on the last language, since the first two are easier to handle. By lemma B.1 (FO-approximation of the generalised product for finite words), there exists FO-definable functions

Note that a word of $\mathcal{A}^\omega$ belongs to L_a (resp. $L_{\mathcal{B}}$) iff its letters ultimately all belong to $\{a\}$ (resp. $\mathcal{B}$).

$$\begin{array}{rll} g : & \mathcal{A}^* \to \mathrm{Sat}^{*}_{\mathrm{grp}}(\mathcal{A}) & \qquad \pi(w) \subseteq g(w) \text{ for all } w \in \mathcal{A}^*, \\ g_a : & a^+ \to \mathrm{Sat}^{+}_{\mathrm{grp}}(a) \quad \text{s.t.} & \qquad \pi(w) \subseteq g_a(w) \text{ for all } w \in a^+, \\ g_{\mathcal{B}} : & \mathcal{B}^+ \to \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{B}) & \qquad \pi(w) \subseteq g_{\mathcal{B}}(w) \text{ for all } w \in \mathcal{B}^+. \end{array}$$

Moreover, since $a \cdot \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \subseteq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$, and hence $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathrm{Sat}^{+}_{\mathrm{grp}}(a) \cdot \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{B})) \subsetneq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ by prop. 1.12, the induction hypothesis yields the existence of an FO-definable function

$$f : (\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \cdot \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{B}))^\omega \to \mathrm{Sat}^{\omega}_{\mathrm{grp}}(\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \cdot \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{B}))$$

such that $\pi(w) \subseteq f(w)$ for every $w \in (\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \cdot \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{B}))^\omega$. Hence, one can define

$$\hat{\pi}{\restriction}_{L_{a\mathcal{B}}} : \begin{array}{ccc} L_{a\mathcal{B}} & \to & \mathrm{Sat}^{\omega}_{\mathrm{grp}}((\mathcal{A})) \\ w_{\mathcal{B}}(w_{a,i} w_{\mathcal{B},i})_{i<\omega} & \mapsto & g(w_{\mathcal{B}}) \cdot f([g_a(w_{a,i}) \cdot g_{\mathcal{B}}(w_{\mathcal{B},i})]_{i<\omega}). \end{array}$$

Moreover, one can define $\hat{\pi}{\restriction}_{L_a}$ and $\hat{\pi}{\restriction}_{L_{\mathcal{B}}}$ by using the induction hypothesis on the smaller alphabets $\{a\}$ and $\mathcal{B}$. Then $\pi(w) \subseteq \hat{\pi}(w)$ by monotonicity of the generalised product and $\hat{\pi}$ is FO-definable since every function and every decomposition used to define it are FO-definable.

❧❧ *Second subcase: $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A}) \cdot a \subsetneq \mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ for some $a \in \mathcal{A}$.* Symmetric of case the first subcase.

❧❧ *Third subcase: $\mathrm{Sat}^{+}_{\mathrm{grp}}(\mathcal{A})$ has a maximum.* Let X be this maximum. Then X^ω is the maximum of $\mathrm{Sat}^{\omega}_{\mathrm{grp}}(\mathcal{A})$, so take $\hat{\pi} : w \mapsto X^\omega$. This concludes the induction. ☐

Observe that the technical details and propositions used for the proof of B.4 are the same as what were used to prove lemma B.1 (lemma for finite words). Notably, the tool used to progress in the induction is the "induction principle" for finite words. The case of all transfinite words — see the following lemma — is trickier: even if the induction in itself is very similar to the induction for finite and omega words, it relies on stronger properties — those that were established in §2.3, 2.4 and 2.5. Let $\pi : \mathcal{P}(U)^{\mathsf{ord+}} \to \mathcal{P}(U)$ denote the generalised product of the finite power ordinal semigroup $\mathcal{P}(U)$.

Lemma B.5. For every $\mathcal{A} \subseteq \mathcal{P}(U)$, there exists an FO-definable function $\hat{\pi} : \mathcal{A}^{\mathsf{ord+}} \to \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ such that $\pi(w) \subseteq \hat{\pi}(w)$ for every $w \in \mathcal{A}^{\mathsf{ord+}}$.

Proof. Proof by induction on $|\mathcal{A}|$ and $|\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})|$.

☙ **First case: $|\mathcal{A}| = 1$.** Then $\mathcal{A}^{\mathsf{ord+}}$ is isomorphic to $\omega_1 \setminus \{0\}$, so we can see $\pi{\restriction}_{\mathcal{A}^{\mathsf{ord+}}}$ as a morphism $\omega_1 \setminus \{0\} \to \langle \mathcal{A} \rangle^{\pi} =: \mathcal{S}$. For $n \in \mathbb{N}$ and $k \in \mathbb{N}_{>0}$, if $\omega^n \cdot k$ belongs to the maximal group $\mathcal{G}$ in the semigroup generated by $\{\omega^n\}$, then define $\hat{\pi}(\omega^n \cdot k) := \bigcup \mathcal{G}$, and otherwise, let $\hat{\pi}(\omega^n \cdot k) := \pi(\omega^n \cdot k)$. Let $m \in \mathbb{N}$ be such that $\pi(\omega^m) = \pi(1)^{\rho}$. Defining

By convention, if $a_i = 0$, $\hat{\pi}(\omega^{m-1} a_i)$ designated the neutral element of $\mathsf{Sat}^{\mathsf{ord}}_{\mathsf{grp}}(\mathcal{A})$.

$$\hat{\pi}(\omega^m \cdot \alpha_m + \omega^{m-1} \cdot a_{m-1} + \ldots + \omega a_1 + a_0) := \hat{\pi}(\omega^m) \cdot \hat{\pi}(\omega^{m-1} a_{m-1}) \cdots \hat{\pi}(\omega a_1) \cdot \hat{\pi}(a_0)$$

for $\alpha_m < \omega_1$ and $a_{m-1}, \ldots, a_0 \in \mathbb{N}$ gives the desired property: we clearly have $\pi(w) \subseteq \hat{\pi}(w)$, and moreover, $\hat{\pi}$ is FO-definable — see lem. 2.30.

☙ **Second case: $|\mathcal{A}| \geq 2$.** By theorem 2.36, either *(i)* $a \cdot \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A}) \subsetneq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ for some $a \in \mathcal{A}$, or *(ii)* $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathsf{Sat}^{\omega}_{\mathsf{grp}}(\mathcal{A})) \subsetneq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$, or *(iii)* $\pi : \mathcal{A}^{\mathsf{ord+}} \to \langle \mathcal{A} \rangle^{\cdot,\omega}$ is FO-definable.

☙☙ *First subcase: $a \cdot \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A}) \subsetneq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$ for some $a \in \mathcal{A}$.* Let $\mathcal{B} = \mathcal{A} \setminus \{a\}$. Then $\mathcal{A}^{\mathsf{ord}} = \mathcal{B}^{\mathsf{ord}}(a^{\mathsf{ord+}} \mathcal{B}^{\mathsf{ord+}})^{\mathsf{ord}} a^{\mathsf{ord}}$ and proposition 2.34 yields

$$\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(a)\, \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{B})) \subsetneq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A}) :$$

thus we can construct $\hat{\pi}$ (nearly) exactly as what we did for finite words — see §B.1.

☙☙ *Second subcase: $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathsf{Sat}^{\omega}_{\mathsf{grp}}(\mathcal{A})) \subsetneq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$.* First, notice that $\mathcal{A}^{\mathsf{ord}} = (\mathcal{A}^{\omega})^{\mathsf{ord}} \mathcal{A}^{*}$. Moreover, by lem. B.1 (finite words) and B.4 (omega words), there exists two FO-definable functions

The equality $\mathcal{A}^{\mathsf{ord}} = (\mathcal{A}^{\omega})^{\mathsf{ord}} \mathcal{A}^{*}$ comes from the fact that every countable ordinal can be written as $\omega \cdot \alpha + n$ with $\alpha < \omega_1$ and $n \in \mathbb{N}$.

$$\begin{array}{ll} g_* : & \mathcal{A}^* \to \mathsf{Sat}^{*}_{\mathsf{grp}}(\mathcal{A}) \\ g_\omega : & \mathcal{A}^\omega \to \mathsf{Sat}^{\omega}_{\mathsf{grp}}(\mathcal{A}) \end{array} \quad \text{s.t.} \quad \begin{array}{l} \pi(w) \subseteq g_*(w) \text{ for all } w \in \mathcal{A}^*, \\ \pi(w) \subseteq g_\omega(w) \text{ for all } w \in \mathcal{A}^\omega. \end{array}$$

Moreover, since $\mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathsf{Sat}^{\omega}_{\mathsf{grp}}(\mathcal{A})) \subsetneq \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A})$, by induction hypothesis, there exists a map

$$f : \mathsf{Sat}^{\omega}_{\mathsf{grp}}(\mathcal{A})^{\mathsf{ord+}} \to \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathsf{Sat}^{\omega}_{\mathsf{grp}}(\mathcal{A}))$$

such that $\pi(w) \subseteq f(w)$ for all $w \in \mathsf{Sat}^{\omega}_{\mathsf{grp}}(\mathcal{A})^{\mathsf{ord+}}$. Then define $\hat{\pi}$ as follows:

$$\hat{\pi} : \begin{array}{ccc} \mathcal{A}^{\mathsf{ord+}} & \to & \mathsf{Sat}^{\mathsf{ord+}}_{\mathsf{grp}}(\mathcal{A}) \\ (w_\iota)_{\iota<\kappa} w_* & \mapsto & f([g_\omega(w_\iota)]_{\iota<\kappa}) g_*(w_*). \end{array}$$

Then $\pi(w) \subseteq \hat{\pi}(w)$ by monotonicity of the generalised product and $\hat{\pi}$ is FO-definable since f, g_* and g_ω are FOdefinable, and since the first letter of each block of size ω in the non-ambiguous decomposition $\mathcal{A}^{\mathsf{ord}} = (\mathcal{A}^{\omega})^{\mathsf{ord}}\mathcal{A}^*$ can be recognised in first-order logic by the formula $\mathrm{lim}(x)$.

❧❧ *Third subcase: π is FO-definable.* Then take $\hat{\pi} := \pi$. This concludes the induction. □

Finally, theorem 2.41 can be immediately deduced from lemma B.5 — the proof is the same as what was done for finite words.

C. Solutions of some exercises

C.1. Exercise 1.11

1. Let $V := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and consider the semigroup morphism $\varphi : A^+ \to V$ that sends w to $(|w|_a \mod 2, |w|_b \mod 2)$. Since V is finite and $L = \varphi^{-1}[(\bar{0},\bar{0})]$, it follows that L is regular. Moreover V is indeed the syntactic semigroup of L since the only semigroups dividing V are (isomorphic to) the trivial group and $\mathbb{Z}/2\mathbb{Z}$, which trivially cannot recognise L.
2. Notice that V is abelian, so $\mathcal{J}=\mathcal{H}$. The groups $\mathbb{Z}/2\mathbb{Z} \times \{0\}$, $\{0\} \times \mathbb{Z}/2\mathbb{Z}$ and $\{(\bar{0},\bar{0}),(\bar{1},\bar{1})\}$ all belong to $\mathrm{Sat}^+_{\mathrm{grp}}(V)$, and since it is closed under product, it follows that $\mathrm{Sat}^+_{\mathrm{grp}}(V)$ contains every subset of V of cardinality 2. Moreover, since V is a group, $V \in \mathrm{Sat}^+_{\mathrm{grp}}(V)$. Then, one can check that by product and by group merging, we cannot obtain a set of cardinality 3.
   Hence, the $\mathrm{Sat}^+_{\mathrm{grp}}(V)$ has three $\mathcal{H}$-classes, that are linearly ordered: the maximal $\mathcal{H}$-class contains every singleton, the intermediate class contains every subset of cardinality 2, and the minimal $\mathcal{H}$-class contains only V.

C.2. Exercise 1.20

The syntactic semigroup S_L of $a(aa)^+$ is represented in figure 12. Then $\mathrm{Sat}^+_{\mathrm{grp}}(S_L)$ has four elements: $\{a\}$, $\{a^2\}$, $\{a^3\}$ and $\{a^2,a^3\}$. There is a unique map $\hat{\varphi}$ that is FO-definable and such that $\varphi(w) \in \hat{\varphi}(w)$ for all w: it is the map sending a to $\{a\}$ and every other word to $\{a^2,a^3\}$. But it is not a semigroup morphism: $\varphi(a)^2 = \{a^2\} \neq \{a^2,a^3\}$.

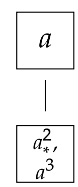


Figure 12: Egg-box diagram of the syntactic semigroup of $a(aa)^+$.

C.3. Exercise 2.11

1. This amounts to showing that for every ordinals $\alpha, \beta \in \omega_1$, if $\alpha, \beta < \omega^\omega$ then $\alpha + \beta < \omega^\omega$ and $\alpha \cdot \omega < \omega^\omega$. Both inequalities follow from the fact that $\alpha < \omega^\omega$ implies $\alpha < \omega^n$ for some $n \in \mathbb{N}$ — see, e.g., [Deh17, prop. II.3.3.3].
2. If $L_1 = L_2$, then they coincide on words of length strictly less than ω^ω. Conversely, if $L_1 \cap A^{[0,\omega^\omega[} = L_2 \cap A^{[0,\omega^\omega[}$, let $\varphi : A^{\mathsf{ord}+} \to S$ be a surjective morphism recognising both L_1 and L_2. The previous question and thm. 2.8 yields

   $$\varphi\,[A^{[0,\omega^\omega[}] \subseteq S = \langle \varphi[A] \rangle^{\pi} = \langle \varphi[A] \rangle^{\cdot,\omega} = \varphi[\langle A \rangle^{\cdot,\omega}] \subseteq \varphi\,[A^{[0,\omega^\omega[}]$$

   from which the conclusion follows.

C.4. Exercise 2.16

Let $L_1 := (ab)^{\mathsf{ord}+}$ and $L_2 := A^{\mathsf{ord}+} \setminus (A^{\mathsf{ord}} aa A^{\mathsf{ord}} + A^{\mathsf{ord}} bb A^{\mathsf{ord}})$.

First, notice that $L_2 \supsetneq L_1$ since L_2 contains words like $(ba)^\omega$ or even $(ab)^\omega (ba)^\omega$. Then the syntactic ordinal semigroup of L_2, whose egg-box diagram is represented in figure 13, contains seven elements:

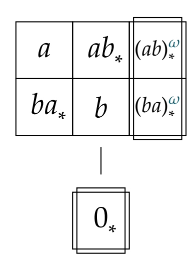


Figure 13: Egg-box diagram of the syntactic ordinal semigroup of L_2.

– 0, recognising words that do not belong in L_2 ;

- a, recognising words that must be followed by a 'b' and preceded by either an 'b' or a limit ordinal — in this context, by "limit ordinal", we mean "a word of L_2 whose domain is a limit ordinal, i.e. either $(ab)^\omega$ or $(ba)^\omega$." ;
- b, recognising words that must be followed by an 'a' and preceded by an 'a' or a limit ordinal ;
- ab, recognising words that must be followed by an 'a' and preceded by a 'b' or a limit ordinal ;
- ba, recognising words that must be followed by an 'b' and preceded by a 'a' or a limit ordinal ;
- $(ab)^\omega$, recognising words that can be followed by anything, and must be preceded by a 'b' or by a limit ordinal ;
- $(ba)^\omega$, recognising words that can be followed by anything, and must be preceded by an 'a' or by a limit ordinal.

References

[Alm99] Jorge Almeida. Some algorithmic problems for pseudovarieties. *Publ. Math. Debrecen*, 54(1):531–552, 1999.

[BC11] Alexis Bès and Olivier Carton. Algebraic Characterization of FO for Scattered Linear Orderings. In Marc Bezem, editor, *Computer Science Logic (CSL'11) - 25th International Workshop/20th Annual Conference of the EACSL*, volume 12 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 67–81, Dagstuhl, Germany, 2011. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.CSL.2011.67.

[Bed98] Nicolas Bedon. *Langages reconnaissables de mots indexés par des ordinaux*. Theses, Université de Marne la Vallée, January 1998. URL: https://tel.archives-ouvertes.fr/tel-00003586.

[Bed01] Nicolas Bedon. Logic over words on denumerable ordinals. *Journal of Computer and System Sciences*, 63(3):394–431, 2001. doi:10.1006/jcss.2001.1782.

[Boj15] Mikołaj Bojańczyk. Recognisable languages over monads. In Igor Potapov, editor, *Developments in Language Theory*, pages 1–13, Cham, 2015. Springer International Publishing. URL: https://arxiv.org/abs/1502.04898v1.

[Boj20] Mikołaj Bojańczyk. *Languages recognised by finite semigroups, and their generalisations to objects such as trees and graphs, with an emphasis on definability in monadic second-order logic.* 2020. Unpublished book. arXiv:2008.11635v1.

[BR12] Nicolas Bedon and Chloé Rispal. Schützenberger and Eilenberg theorems for words on linear orderings. *Journal of Computer and System Sciences*, 78(2):517–536, March 2012. doi:10.1016/j.jcss.2011.06.003.

[Büc73] J. Richard Büchi. *The monadic second order theory of ω_1*, pages 1–127. Springer Berlin Heidelberg, Berlin, Heidelberg, 1973. doi:10.1007/BFb0082721.

[CCP18] Olivier Carton, Thomas Colcombet, and Gabriele Puppis. An algebraic approach to MSO-definability on countable linear orderings. May 2018. doi:10.1017/jsl.2018.7.

[CH91] Sang Cho and Dung T. Huynh. Finite-automaton aperiodicity is pspace-complete. *Theoretical Computer Science*, 88(1):99–116, 1991. doi:10.1016/0304-3975(91)90075-D.

[CS15] Thomas Colcombet and A. V. Sreejith. Limited set quantifiers over countable linear orderings. In *Proceedings, Part II, of the 42nd International Colloquium on Automata, Languages, and Programming - Volume 9135*, ICALP 2015, page 146–158, Berlin, Heidelberg, 2015. Springer-Verlag. doi:10.1007/978-3-662-47666-6_12.

[Deh17] Patrick Dehornoy. *La théorie des ensembles.* Calvage et Mounet, 2017.

[Grä07] Erich Grädel. *Finite Model Theory and Descriptive Complexity*, pages 125–230. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007. doi:10.1007/3-540-68804-8_3.

[GS82] Yuri Gurevich and Saharon Shelah. Monadic theory of order and topology in ZFC. *Annals of Mathematical Logic*, 23(2):179–198, 1982. doi:10.1016/0003-4843(82)90004-3.

[GS19] S.J.v. Gool and B. Steinberg. Pointlike sets for varieties determined by groups. *Advances in Mathematics*, 348:18–50, 2019. doi:10.1016/j.aim.2019.03.020.

[Hen88] Karsten Henckell. Pointlike sets: the finest aperiodic cover of a finite semigroup. *Journal of Pure and Applied Algebra*, 55(1):85–126, 1988. doi:10.1016/0022-4049(88)90042-4.

[Lit72] Ami Litman. On the decidability of the monadic theory of ω_1. Master's thesis, The Hebrew University, 1972.

[Mak04] Johann A Makowsky. Algorithmic uses of the Feferman–Vaught theorem. *Annals of Pure and Applied Logic*, 126(1-3):159–213, 2004. doi:10.1016/j.apal.2003.11.002.

[MP71] Robert McNaughton and Seymour A. Papert. *Counter-Free Automata.* The MIT Press, 1971.

[Per84] Dominique Perrin. Recent results on automata and infinite words. In *International Symposium on Mathematical Foundations of Computer Science*, pages 134–148. Springer, 1984. doi:10.1007/BFb0030294.

[Pin20] Jean-Éric Pin. Mathematical foundations of automata theory. MPRI lecture notes, 2020. URL: https://www.irif.fr/~jep/PDF/MPRI/MPRI.pdf.

[PP04] Jean-Eric Pin and Dominique Perrin. *Infinite Words: Automata, Semigroups, Logic and Games.* Elsevier, 2004. URL: https://hal.archives-ouvertes.fr/hal-00112831.

[PZ16] Thomas Place and Marc Zeitoun. Separating regular languages with first-order logic. *Logical Methods in Computer Science*, 12, 2016. doi:10.2168/LMCS-12(1:5)2016.

[PZ18] Thomas Place and Marc Zeitoun. The complexity of separation for levels in concatenation hierarchies. In Sumit Ganguly and Paritosh Pandya, editors, *38th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2018)*, volume 122 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 47:1–47:17, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.FSTTCS.2018.47.

[Rab69] Michael O. Rabin. Decidability of second-order theories and automata on infinite trees. *Transactions of the American Mathematical Society*, 141:1–35, 1969. URL: http://www.jstor.org/stable/1995086.

[RC05] Chloé Rispal and Olivier Carton. Complementation of Rational Sets on Countable Scattered Linear Orderings. *International Journal of Foundations of Computer Science*, 16(4):767–786, 2005. URL: https://hal.archives-ouvertes.fr/hal-00160985.

[Ris04] Chloé Rispal. *Automates sur les ordres linéaires : Complémentation*. Theses, Université de Marne la Vallée, December 2004. URL: https://tel.archives-ouvertes.fr/tel-00720658.

[Ros82] Joseph G Rosenstein. *Linear orderings*. Academic press, 1982.

[Sch65] M.P. Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8(2):190–194, 1965. doi:10.1016/S0019-9958(65)90108-7.

[She75] Saharon Shelah. The monadic theory of order. *Annals of Mathematics*, 102(3):379–419, 1975. URL: http://www.jstor.org/stable/1971037.

[vGS19] Samuel J. van Gool and Benjamin Steinberg. Merge decompositions, two-sided Krohn–Rhodes, and aperiodic pointlikes. *Canadian Mathematical Bulletin*, 62(1):199–208, 2019. doi:10.4153/CMB-2018-014-8.

[Wil93] Thomas Wilke. An algebraic theory for regular languages of finite and infinite words. *International Journal of Algebra and Computation*, 03(04):447–489, 1993. doi:10.1142/S0218196793000287.