



HAL
open science

An Application of the Feferman-Vaught Theorem to Automata and Logics for Words over an Infinite Alphabet

Alexis Bès

► **To cite this version:**

Alexis Bès. An Application of the Feferman-Vaught Theorem to Automata and Logics for Words over an Infinite Alphabet. 2007. hal-00155280

HAL Id: hal-00155280

<https://hal.science/hal-00155280>

Preprint submitted on 17 Jun 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

An Application of the Feferman-Vaught Theorem to Automata and Logics for Words over an Infinite Alphabet

Alexis Bès

LACL, Université Paris XII-Val de Marne,

Email: `bes@univ-paris12.fr`

June 17, 2007

LACL Technical Report 2007-06

Abstract

We show that a special case of the Feferman-Vaught composition theorem gives rise to a natural notion of automata for finite words over an infinite alphabet, with good closure and decidability properties, as well as several logical characterizations.

We also consider a slight extension of the Feferman-Vaught formalism which allows to express more relations between component values (such as equality), and prove related decidability results. From this result we get an interesting class of decidable logics for words over an infinite alphabet.

The problem of finding suitable notions of automata for words over an infinite alphabet has been addressed in several papers [1, 13, 2, 3, 9, 18]. The motivations are e.g. modelization of temporized systems, distributed systems, or representation of semi-structured data. A common goal is to find a simple and expressive model which preserves as much as possible the good properties of the classical model. Kaminski and Francez [13] introduce *finite-memory automata*: these are finite automata equipped with a finite number of registers which allow to store symbols during the run, and compare them with the current symbol. The paper [3] extends somehow this idea by allowing transitions which involve an equivalence relation of finite index defined on the set of (vector) values of the registers. The paper [18] continues the study of finite-memory automata, and also introduce pebble automata, which are automata equipped with a finite set of pebbles whose use is restricted by a stack discipline. The automaton can test equality by comparing the pebbled symbols. The work [2] does not consider directly automata, but addresses decidability issues for logics which allow to express properties of words over an infinite alphabet. More recently, Choffrut

and Grigorieff [9] define automata whose transitions are expressed as first-order formulas (see below).

The aim of this paper is to show that a special case of the Feferman-Vaught composition theorem gives rise to a natural notion of automata for finite words over an infinite alphabet, with good closure and decidability properties, as well as several logical characterizations. Building on Mostowski's work [17], Feferman and Vaught consider in [11] several kinds of products of logical structures, and prove that the first-order (shortly:FO) theory of a (generalized) product of structures reduces to the FO theory of the factor structures and the monadic second-order (shortly:MSO) theory of the index structure. We refer the interested reader to the survey papers [15, 23] which present several applications of these results, as well as extensions of the technique; for recent related results see e.g. [20, 24].

An interesting special case of the Feferman-Vaught (shortly: FV) theorem is when one considers the generalized weak power of a single structure M , and the index structure is $(\omega; <)$. In this case the domain of the resulting structure roughly consists in the set of finite words over the domain of M (seen as an alphabet), and the definable relations can be characterized in terms of automata thanks to Büchi's result on the equivalence between definability in the MSO theory of $(\omega; <)$ and automata [6]. The automata model and related logics we consider can be seen as direct reformulations of this special case.

In Section 2 we define the automata model. Given a structure M with domain Σ (finite or not), we define M -automata as classical finite automata which read finite words over Σ and such that the transition between two states is allowed if the current symbol s read by the automaton satisfies some first-order formula $\varphi(x)$ in M . That is, M -automata are simply finite automata equipped with FO constraints. We show that the class of languages recognizable by such automata (which are called M -recognizable languages) are closed under rational operations as well as complementation, and that the emptiness problem is decidable whenever the FO theory of M is. These results are straightforward generalizations of the classical case of a finite alphabet.

In Section 3 we provide several logical characterizations of M -recognizable languages. The first one uses MSO logic and is an easy adaptation of Büchi's classical result [6]. The second one extends the Eilenberg-Elgot-Shepherdson FO formalism [10] for synchronous relations and relies heavily on the Feferman-Vaught technique. This result, and actually the automaton model itself, are a natural generalization of Choffrut and Grigorieff results mentioned above [9]. We finally provide a third logical characterization of M -recognizable relations for the special case where $M = (\omega; +)$.

Several results of Section 2 and 3 are rather easy generalizations or reformulations of well-known results; therefore many proofs in these sections are only sketched.

In terms of expressive power, M -automata are incomparable with automata and logics considered in [2, 13, 18], since on one hand they allow to express FO constraints, but on the other hand they can't test whether two positions in a word carry the same symbol (for instance, the language $\{aa \mid a \in \Sigma\}$ is not

M -recognizable whenever Σ is infinite). As shown e.g. in [2, 18] these kinds of tests have to be limited if one wants to keep good decidability properties. In Section 4 we propose a slight extension of the Feferman-Vaught formalism which allows to test whether a n -tuple s_1, \dots, s_n of symbols appearing in distinct positions in a word w , satisfies a formula $\varphi(x_1, \dots, x_n)$ in M . We isolate a syntactic fragment of this logic, which we denote by $MSO_R^+(\mathcal{L})$, for which the satisfiability problem (or in other words, the emptiness problem for related languages) still reduces to the decidability of the FO theory of M . We also discuss easy generalizations of the result.

We wish to thank Lev Beklemishev, Christian Hoffrut, Serge Grigorieff, Anca Muscholl, Peter Revesz, Luc Ségoufin and Wolfgang Thomas for interesting discussions and comments.

1 Definitions and notations

In the sequel we shall deal with finite words over some alphabet, finite or not. Given a word $w = w_0 \dots w_n$ over the alphabet Σ , a *position* in w is an element of $\{0, \dots, n\}$, and we say that a position i carries the symbol w_i . We shall sometimes use the notation $w[i]$ for w_i .

We shall consider several logical formalisms. By FO we mean first-order logic with equality. We shall also consider Monadic Second-Order Logic (shortly: MSO). We denote by $FO(M)$ (respectively $MSO(M)$) the first-order (respectively monadic second-order) theory of the structure M . We consider only relational structures. Given a language \mathcal{L} and a \mathcal{L} -structure M , for every relational symbol R of \mathcal{L} we denote by R^M the interpretation of R in M . However, we will often confuse logical symbols with their interpretation. Moreover we will use freely abbreviations such as $\exists x \in X \varphi$.

We shall deal with multitape automata. As usual, given n finite words (w_1, \dots, w_n) over Σ we complete (if necessary) each w_i with a sufficient number of occurrences of some special symbol $\#$ in order to have words of the same length. Doing this, we obtain n words over $\Sigma \cup \{\#\}$ with the same length, which can be seen as a single word over the alphabet $(\Sigma \cup \{\#\})^n$ (i.e. the alphabet of n -tuples of elements of $\Sigma \cup \{\#\}$). This word will be denoted by $H(w_1, \dots, w_n)$.

Consider a relational language \mathcal{L} and a \mathcal{L} -structure M with domain Σ . Since we have to deal with the symbol $\#$ we shall associate to M the structure $M_\#$ in the language $\mathcal{L}_\# = \mathcal{L} \cup \{P_\#\}$, such that:

- the domain of $M_\#$ is $\Sigma \cup \{\#\}$;
- for every relational symbol R of \mathcal{L} , we have $R^{M_\#} = R^M$;
- $P_\#$ denotes a unary predicate not in \mathcal{L} , interpreted as follows: $P_\#(x)$ holds in $M_\#$ iff $x = \#$.

2 Automata

We define a notion of synchronous multi-tape finite automata that read finite words over any (in)finite alphabet Σ .

A M -automaton is a finite n -tape synchronous non-deterministic automaton which reads finite words over the alphabet Σ . Transition rules are triplets of the form (q, φ, q') , where q, q' are states of the automaton, and $\varphi(x_1, \dots, x_n)$ is a first-order formula in the language $\mathcal{L}_\#$ of $M_\#$. The interpretation of such a triplet is “we can pass from the state q to the state q' if the n -tuple (a_1, \dots, a_n) of symbols read (simultaneously) by the n heads satisfies the formula φ in $M_\#$ ”.

Formally, given a first-order language \mathcal{L} and a \mathcal{L} -structure M , a M -automaton is defined by $\mathcal{A} = (Q, n, \Sigma, M, E, I, T)$ where

- Q is a finite set (of states);
- $n \geq 1$ is the number of heads;
- Σ is an alphabet (finite or not);
- $E \subseteq Q \times \mathcal{F}_n \times Q$ denotes the set of transitions, where \mathcal{F}_n is the set of $\mathcal{L}_\#$ -formulas with n free variables;
- $I \subseteq Q$ is the set of initial states;
- $T \subseteq Q$ is the set of terminal states.

Given a n -tuple $w = (w_1, \dots, w_n)$ of words over Σ , a *path γ in \mathcal{A} labeled by w* is a sequence of states $\gamma = q_0 \dots q_m$, where $m = |H(w)|$ such that $q_0 \in I$, and for every $i \leq m$ there exists a $\mathcal{L}_\#$ -formula $\varphi(x_1, \dots, x_n)$ such that $(q_i, \varphi, q_{i+1}) \in E$ and

$$M_\# \models \varphi(\pi_1(H(w))(i), \dots, \pi_n(H(w))(i))$$

where $\pi_j(H(w))$ denotes the j -th component of $H(w)$. The path γ is *successful* if $q_m \in T$. The word w is accepted by \mathcal{A} if it is the label of a successful path.

A language $X \subseteq (\Sigma^*)^n$ is said to be M -recognizable iff there exists some M -automaton whose set of accepted words equals $H(X)$.

Examples:

1. Let $M = (\omega; +)$ where $+$ denotes the graph of addition. Then the following languages are M -recognizable:
 - the set of words over ω (seen as as an infinite alphabet) of the form $(1, 0, \dots, 0)$ (we allow the case where there is no 0). Consider indeed the automaton with two states q_0, q_1 , where q_0 is initial and q_1 is terminal, and whose set of transitions is $\{(q_0, \varphi_1, q_1), (q_1, \varphi_0, q_1)\}$ where $\varphi_0(x)$ is the formula $x + x = x$, and $\varphi_1(x)$ expresses that $x = 1$. The automaton is pictured in Figure 1.

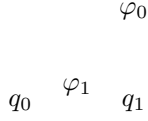


Figure 1: A simple M -automaton

- the set of words whose symbols are alternatively even and odd. Consider indeed the automaton with two states q_0, q_1 , where q_0, q_1 both are initial and terminal states, and whose set of transitions is $\{(q_0, \varphi_e, q_1), (q_1, \varphi_o, q_0)\}$ where $\varphi_e(x)$ is the formula $\exists z z + z = x$, and $\varphi_o(x) = \neg\varphi_e(x)$.
 - the language $L \subseteq \omega^* \times \omega^* \times \omega^*$ of words (u, v, w) such that u, v, w have the same length, and for each i the i -th symbol of w equals the sum of the corresponding symbols of u and v . Consider indeed the automaton with a single state q (which is initial and terminal) and a single transition (q, φ, q) where $\varphi(x, y, z)$ is the formula $x + y = z$. Observe that if u, v, w do not have the same length then the first letter of $H(u, v, w)$, say (u_0, v_0, w_0) , has at least one component which is equal to $\#$, which by the very definition of $M_\#$ implies $M_\# \not\models \varphi(u_0, v_0, w_0)$, which implies in turn that there is no (successful) run of \mathcal{A} labelled by (u, v, w) .
2. Let $M = (\Sigma; (P_a)_{a \in \Sigma})$, where $P_a(x)$ holds iff $x = a$. Then one can show that for Σ finite, M -recognizable relations coincide with synchronized relations (as defined in [10]).
 3. One can show that for every \mathcal{L} -structure $M = (\Sigma; \dots)$ where Σ is infinite, the language $\{aa : a \in \Sigma\}$ is not M -recognizable.

There is an equivalent way of defining M -recognizability: a subset X of Σ^* is M -recognizable iff there exist a partition of Σ into definable subsets X_1, \dots, X_n , and a finite (classical) automata over the alphabet $\Sigma_n = \{1, \dots, n\}$, such that the image of X by the mapping $f : \Sigma^* \rightarrow \Sigma_n^*$ is recognizable, where f is defined as the morphism induced by the letter-to-letter substitution which maps every $a \in \Sigma$ to the symbol i such that $a \in X_i$.

This alternative definition of M -recognizability allows to transfer easily classical results of automata theory to the case of words over any alphabet. In particular the following result holds.

Proposition 1 *The class of M -recognizable languages is closed under boolean and rational operations.*

Regarding the emptiness problem for M -recognizable languages, the main difference with the classical case is that given a M -automaton \mathcal{A} there can exist transitions $(q, \varphi, q') \in E$ such that no n -tuple of elements of $M_\#$ satisfies

φ ; such transitions will never appear in any run of \mathcal{A} . Thus one has to remove such transitions from E in order to apply the usual reachability algorithm for the emptiness problem; this can be done effectively if and only if $FO(M)$ is decidable. This leads to the following result.

Proposition 2 *The emptiness problem for M -recognizable languages is equivalent to the decidability of $FO(M)$.*

3 Logic and M -automata

There are three main equivalent formalisms that relate logic and automata:

- Büchi's MSO logic [6] (the weak monadic second order theory of $(\omega, <)$);
- the Eilenberg-Elgot-Shepherdson (shortly:EES) formalism [10], i.e. the FO theory of $S = (\Sigma^*; EqLength, <_{pref}, \{L_a\}_{a \in \Sigma})$ where
 - $EqLength(x, y)$ holds iff x and y have the same length
 - $x <_{pref} y$ holds iff x is a prefix of y
 - $L_a(x)$ holds iff a is the last letter of x .
- the so-called Büchi Arithmetic of base k , i.e. the FO theory of the structure $(\omega; +, V_k)$ where $V_k(x)$ denotes the greatest power of k which divides x , see [5].

In this section we extend these formalisms to the case of words over any alphabet (finite or not). For the first one, MSO logic, the extension is very natural and easy to obtain. The extension of the EES formalism relies heavily on the Feferman-Vaught technique. Finally we show that for $M = (\omega; +)$, M -recognizable relations coincide with relations definable in $(\omega^\omega; +)$. The latter structure can therefore be seen as “Büchi Arithmetic of base ω ”.

3.1 A first logical characterization with MSO

Let $M = (\Sigma; \dots)$ be a \mathcal{L} -structure. We associate to every $\mathcal{L}_\#$ -formula F some unary relational symbol α_F . We define then $MSO(\mathcal{L})$ as MSO over the language $\{<, (\alpha_F)_{F \in \mathcal{F}}\}$ where \mathcal{F} denotes the set of $\mathcal{L}_\#$ -formulas with at least one free variable.

We say that $A \subseteq (\Sigma^*)^n$ is $MSO(M)$ -definable if there exists a $MSO(\mathcal{L})$ -sentence ψ such that $w = (w_1, \dots, w_n) \in A$ iff $(D, <_D) \models \psi$ where

- $D = \{0, 1, \dots, |H(w)| - 1\}$, and $<_D$ is the natural ordering relation restricted to D ;
- For every $\mathcal{L}_\#$ -formula F with n free variables, and every position x in w , the interpretation of $\alpha_F(x)$ in $(D, <_D)$ is TRUE iff

$$M_\# \models F(\pi_1(H(w))(x), \dots, \pi_n(H(w))(x)),$$

where $\pi_i(H(w))$ denotes the i -th component of $H(w)$.

Let us give a few examples:

- Let $M = (\omega; +)$.
 - the set $A \subseteq \omega^*$ of words that contain no odd symbol is $MSO(M)$ -definable by the sentence $\forall y \alpha_F(y)$, where $F(x) : \exists z(z + z = x)$
 - the set of words whose symbols are alternatively even and odd is $MSO(M)$ -definable by the formula

$$\forall x \forall y ((x < y \wedge \neg \exists z x < z < y) \rightarrow ((\alpha_F(x) \leftrightarrow \neg \alpha_F(y))))$$

where F is the formula defined above.

- Let $M = (\Sigma; (P_a)_{a \in \Sigma})$. One can prove that if Σ is finite, then $MSO(M)$ -definable relations coincide with relations definable in the classical MSO theory of successor, i.e. these are precisely the synchronous relations.

Proposition 3 *Let M be a relational structure with domain Σ . For every $n \geq 1$ and every $L \subseteq (\Sigma^*)^n$, the language L is $MSO(M)$ -definable iff it is M -recognizable.*

Proof Simple adaptation from Büchi's equivalence between WMSO definability and recognizability [6]. For the direction recognizable \rightarrow definable one uses the classical encoding of an accepting run of an automaton by a formula. For the converse one uses the fact that the formulas $\alpha_{F_1}, \dots, \alpha_{F_m}$ appearing in a $MSO(\mathcal{L})$ -sentence ψ can be chosen such that every n -tuple of elements of the domain of $M_{\#}$ satisfies exactly one formula among the F_i 's in M , which allows then to see words over Σ as words over the finite alphabet $\{1, \dots, m\}$ and then use Büchi's technique. \square

3.2 A special case of the Feferman-Vaught composition method

We now recall the Feferman-Vaught composition method [11]. More precisely we shall focus on the notion of generalized weak power introduced in [11], which generalizes the notion of weak power of structures studied by Mostowski [17].

Let $A = (D; (R_i)_{i \in I}, e)$, be a relational structure in the language $\mathcal{L}_A = \{(R_i)_{i \in I}, e\}$ where e denotes a constant symbol and $(R_i)_{i \in I}$ is a set of relational symbols.

Let $B = (S_{Fin}(\omega); \subseteq, (R'_j)_{j \in J})$ be a \mathcal{L}_B -structure with domain the set $S_{Fin}(\omega)$ of finite subsets of ω , and where \subseteq is interpreted as the inclusion relation, and $(R'_j)_{j \in J}$ denotes a set of relations over $S_{Fin}(\omega)$.

Let us denote by $A_e^{(\omega)}$ the set of ω -sequences of elements of D which are ultimately equal to e .

Definition 4 Let R be a k -ary relation over $A_e^{(\omega)}$; we say that R is describable in $(\mathcal{A}, \mathcal{B})$ if and only if there exist

- \mathcal{L}_A -formulas with k free variables F_1, \dots, F_l
- a \mathcal{L}_B -formula $G(X_1, \dots, X_l)$

such that for every k -tuple (f_1, \dots, f_k) of elements of $A_e^{(\omega)}$, we have $(f_1, \dots, f_k) \in R$ if and only if

$$\mathcal{B} \models G(T_1, \dots, T_l)$$

where

$$T_i = \{x \in \omega \mid \mathcal{A} \models F_i(f_1(x), \dots, f_k(x))\} \quad \text{for every } i \in \{1, \dots, l\}.$$

Definition 5 With the above notations, we say that the structure $(A_e^{(\omega)}; \mathcal{R})$, where \mathcal{R} denotes the set of relations describable in $(\mathcal{A}, \mathcal{B})$, is the generalized weak power of \mathcal{A} relative to \mathcal{B} .

Theorem 6 ([11]) Let \mathcal{C} is a generalized weak power of \mathcal{A} relative to \mathcal{B} . Then every relation which is FO-definable in \mathcal{C} is describable in $(\mathcal{A}, \mathcal{B})$.

Moreover if $\text{Th}(\mathcal{A})$ and $\text{Th}(\mathcal{B})$ are decidable then $\text{Th}(\mathcal{C})$ is decidable.

Remark 7 Our definition of generalized weak power is a slight modification of the one given by Feferman and Vaught in [11]. Let us precise the differences. First of all, we consider only sequences indexed by ω while sequences indexed by any infinite set I are considered in [11]. Moreover our definition of describable relations uses definability in some algebra of finite subsets of ω , while [11] considers the algebra of finite or cofinite subsets of ω . However Theorem 9.6 of [11] shows that we can restrict ourselves to finite subsets of ω only.

The previous definitions are clearly related to the notion of $\text{MSO}(M)$ -definability which we defined in the previous subsection. Let us be more specific.

First of all, we set $B = (S_{Fin}(\omega); \subseteq, \prec)$ where $x \prec y$ iff x and y are two singleton sets, say $x = \{m\}$ and $y = \{n\}$, such that $m < n$. This structure can be seen as a FO counterpart of the MSO theory of $(\omega; <)$; more precisely it is easy to prove that given any n -ary relation R over finite subsets of ω , the relation R is MSO-definable in $(\omega; <)$ iff it is FO-definable in B .

For every finite word w over Σ^* , let us define $f(w)$ as the word over $(\Sigma \cup \{\#\})^\omega$ obtained by appending to w infinitely many symbols $\#$. Obviously $f(w)$ can be seen as an element of $(\Sigma \cup \{\#\})^{(\omega)}$.

The following is easy to check.

Proposition 8 Let $M = (\Sigma; \dots)$ be a \mathcal{L} -structure, $\mathcal{A} = M_\#$ and $\mathcal{B} = (S_{Fin}(\omega); \subseteq, \prec)$. For every n -ary relation R over Σ^* , R is $\text{MSO}(M)$ -definable iff $f(R)$ is describable in $(\mathcal{A}, \mathcal{B})$.

The previous proposition together with Theorem 6 yield the following corollary.

Corollary 9 *Let C be a relational \mathcal{L} -structure with domain Σ^* , such that the interpretation of every relational symbol of \mathcal{L} is a M -recognizable relation. Then every relation which is FO-definable in C is M -recognizable. Moreover if $FO(M)$ is decidable then the same holds for $FO(C)$.*

This corollary can be seen as a natural generalization of Hodgson's results on automatic structures [12].

3.3 Extending the EES formalism

Let us focus now on the EES formalism. Eilenberg, Elgot and Shepherdson prove [10] that for Σ finite, $|\Sigma| \geq 2$, a relation over Σ^n is synchronous iff it is definable in the structure $S = (\Sigma^*; EqLength, <_{pref}, \{L_a\}_{a \in \Sigma})$ where

- $EqLength(x, y)$ holds iff x and y have the same length;
- $x <_{pref} y$ holds iff x is a prefix of y ;
- $L_a(x)$ holds iff a is the last letter of x .

They also asked whether there is an appropriate notion of automata that captures this logic when Σ is infinite. Choffrut and Grigorieff [9] recently solved this problem (and also other questions raised in [10]) by introducing a notion of automata with constraints expressed as FO formulas. It appears that the automata notion they consider captures exactly M -recognizable relations for the special case $M = (\Sigma; (P_a)_{a \in \Sigma})$.

We can extend Choffrut-Grigorieff results in the following way.

Proposition 10 *Let Σ be a set with at least two elements, and $M = (\Sigma; \dots)$ be a \mathcal{L} -structure. Let*

$$S_M = (\Sigma^*; EqLength, <_{pref}, (A_R)_{R \in \mathcal{L}})$$

where

- $EqLength(x, y)$ holds iff x and y have the same length;
- $x <_{pref} y$ holds iff x is a prefix of y ;
- for every n -ary relation symbol R of \mathcal{L} , the symbol A_R denotes a n -ary relation symbol such that $A_R(u_1, \dots, u_n)$ holds iff there exist $w_1, \dots, w_n \in \Sigma^*$ and $a_1, \dots, a_n \in \Sigma$ such that:
 - $u_i = w_i a_i$ for every i ;
 - all w_i 's have the same length;
 - $(a_1, \dots, a_n) \in R^M$.

Then the following holds:

1. For every $n \geq 1$ and every $L \subseteq \Sigma^n$, the language L is M -recognizable iff it is (FO) definable in S_M .
2. If $FO(M)$ is decidable then the same holds for $FO(S_M)$.

Proof

1. It is easy to check that all base relations of S_M are M -recognizable, which implies by Corollary 9 that every FO-definable relation in S_M is M -recognizable.

For the converse one uses as in Proposition 3 the classical encoding of an accepting run *à la* Büchi.

2. Consequence of Corollary 9.

□

Note that if we take $M = (\Sigma; (P_a)_{a \in \Sigma})$ in the above proposition (which corresponds to the Choffrut-Grigorieff setting), then we get a structure S_M which is not equal to S but has the same expressive power.

3.4 A special case

We shall concentrate now on the case where $M = (\omega; +)$ (where $+$ denotes the graph of addition). In this case we've got another logical characterization of M -recognizable relations, this time in terms of ordinal theories. This is essentially a reformulation of known results.

In the sequel we consider structures of the form $(\alpha; +)$ where α is an ordinal. The domain of this structure is the set of ordinals less than α , and $+$ is interpreted as the graph of ordinal addition restricted to the domain.

Feferman and Vaught prove in [11] that for every ordinal γ the structure $(\omega^\gamma; +)$ is isomorphic to the generalized weak power of $(\omega; +)$ relative to $(S_{Fin}(\gamma); \subseteq, <)$, where $S_{Fin}(\gamma)$ denotes the set of finite subsets of γ and $X < Y$ iff $X = \{\alpha\}$ and $Y = \{\beta\}$ with $\alpha < \beta$.¹

In particular for $\gamma = \omega$ their result, combined with Büchi's result, implies that via some encoding all relations definable in $(\omega^\omega; +)$ are $(\omega; +)$ -recognizable, and that the theory of $(\omega^\omega; +)$ is decidable.

Let us be more specific. We first recall some useful results on ordinal arithmetic; all of them can be found e.g. in Sierpinski's book [22, chap.XIV]

¹As a corollary, the FO theory of $(\omega^\gamma; +)$ reduces to the FO theory of $(\omega; +)$ (Presburger Arithmetic, which is decidable [19]) and the WMSO theory of $(\gamma, <)$. The latter was proved to be decidable by Büchi [7] a few years after Feferman-Vaught' work, which implies the decidability of the FO theory of $(\omega^\gamma; +)$.

Proposition 11 (Cantor’s normal form for ordinals) *Every ordinal $\alpha > 0$ can be written uniquely as*

$$\alpha = \omega^{\alpha_1} a_1 + \cdots + \omega^{\alpha_k} a_k$$

where $\alpha_1, \alpha_2, \dots, \alpha_k$ is a decreasing sequence of ordinals, and $0 < a_i < \omega$.

We will use the abbreviation “CNF” for “in Cantor’s normal form”.

The following proposition relates the CNF of the ordinal $\alpha + \beta$ from the CNF of α and β .

Proposition 12 *Let $\alpha = \omega^{\alpha_1} a_1 + \cdots + \omega^{\alpha_k} a_k$ and $\beta = \omega^{\beta_1} b_1 + \cdots + \omega^{\beta_l} b_l$ be two ordinals > 0 (CNF).*

- *If $\alpha_1 < \beta_1$ then $\alpha + \beta = \beta$*
- *If $\alpha_1 \geq \beta_1$ and if $\alpha_j = \beta_1$ for some j , then*

$$\alpha + \beta = (\omega^{\alpha_1} a_1 + \cdots + \omega^{\alpha_{j-1}} a_{j-1}) + \omega^{\alpha_j} (a_j + b_1) + (\omega^{\beta_2} b_2 + \cdots + \omega^{\beta_l} b_l)$$

- *If $\alpha_1 \geq \beta_1$ and if $\alpha_j \neq \beta_1$ for every j , then*

$$\alpha + \beta = (\omega^{\alpha_1} a_1 + \cdots + \omega^{\alpha_m} a_m) + (\omega^{\beta_1} b_1 + \cdots + \omega^{\beta_l} b_l)$$

where m is the greatest index for which $\alpha_m > \beta_1$.

Consider now the function $f : \omega^\omega \rightarrow \omega^*$ which maps every ordinal $\alpha < \omega^\omega$ written in CNF as $\alpha = \sum_{i=0}^{\infty} \omega^i a_i$ with $a_i < \omega$ and $a_m \neq 0$, to the word $c(\alpha) = a_m \dots a_0$ over the alphabet ω . Given n ordinals $\alpha_1, \dots, \alpha_n$, we define $c(\alpha_1, \dots, \alpha_n)$ as $H(c(\alpha_1), \dots, c(\alpha_n))$, where we choose 0 as the padding symbol #.

Example 13 Consider the ordinals $\alpha = \omega^6 \cdot 5 + \omega^4 \cdot 4 + \omega^3 \cdot 3 + \omega^1 \cdot 2 + \omega^0 \cdot 11$, and $\beta = \omega^3 \cdot 17 + \omega^2 \cdot 6 + \omega^1 \cdot 2$. Then by Proposition 12 (second case), the ordinal $\gamma = \alpha + \beta$ equals $\gamma = (\omega^6 \cdot 5 + \omega^4 \cdot 4) + \omega^3 \cdot (3 + 17) + (\omega^2 \cdot 6 + \omega^1 \cdot 2)$. We have

$$c(\alpha, \beta, \gamma) = \begin{pmatrix} 5 \\ 0 \\ 5 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 4 \\ 0 \\ 4 \end{pmatrix} \begin{pmatrix} 3 \\ 17 \\ 20 \end{pmatrix} \begin{pmatrix} 0 \\ 6 \\ 6 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} \begin{pmatrix} 11 \\ 0 \\ 0 \end{pmatrix}.$$

Proposition 12 is the key argument in Feferman-Vaught’ proof that $(\omega^\gamma; +)$ is isomorphic to the generalized weak power of $(\omega; +)$ relative to $(S_{Fin}(\gamma); \subseteq, \prec)$. Let us reformulate their ideas in terms of $(\omega; +)$ –automata.

Proposition 14 *The graph of addition for ordinals $< \omega^\omega$, seen as a relation over $\omega^* \times \omega^* \times \omega^*$, is $(\omega^\omega; +)$ –recognizable.*

Proof[sketch] A convenient $(\omega^\omega; +)$ –automaton which recognizes the language $X = \{c(\alpha, \beta, \gamma) \mid \alpha, \beta, \gamma < \omega^\omega, \alpha + \beta = \gamma\}$ is pictured in Figure 2, where

- $\varphi_1(x, y, z) : x \neq 0 \wedge y = 0 \wedge z = x$
- $\varphi_2(x, y, z) : y \neq 0 \wedge z = x + y$
- $\varphi_3(x, y, z) : z = y$

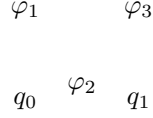


Figure 2: A $(\omega; +)$ -automaton for ordinal addition

Let us illustrate the construction with the ordinals α, β, γ of Example 13. We have $c(\alpha, \beta, \gamma) \in X$. A successful run of the automaton for $c(\alpha, \beta, \gamma)$ can be obtained by following the transition labelled by φ_1 for the first three symbols of $c(\alpha, \beta, \gamma)$, then the transition labelled by φ_2 for the symbol $\begin{pmatrix} 3 \\ 17 \\ 20 \end{pmatrix}$, and the transition labelled by φ_3 for the remaining symbols of $c(\alpha, \beta, \gamma)$.

This example illustrates the second case of Proposition 12, but it is rather easy to check that the automaton is actually convenient for all cases. \square

We can provide now a characterization of M -recognizable relations for the case $M = (\omega; +)$.

Proposition 15 *For every $n \geq 1$, and every n -ary relation R over ω^ω , the relation R is (FO) definable in $(\omega^\omega; +)$ iff $c(R)$ is $(\omega; +)$ -recognizable.*

Proof (sketch) The “only if” part comes from the fact that the range of c , and the graph of ordinal addition, are M -recognizable. The proof of the converse comes from the fact that one can encode the run of a M -automaton in $(\omega^\omega; +)$. Indeed one defines successively the following relations:

- powers of ω less than ω^ω
- the graph of $x \mapsto x\omega$
- the relation $R(\alpha, \beta)$ “ α is a power of ω which appears in the decomposition of β in base ω ”
- the relation $S(\alpha, \beta)$ “ α is an ordinal of the form $\omega^k a_k$ with $0 < a_k < \omega$, and a_k is the coefficient of ω^k when one writes β in base ω ”.

Then one encodes the run of the automaton in a similar way as in $(\omega; +, V_k)$ (see [5]): a successful run $(q_{i_0}, \dots, q_{i_n})$ of the automaton is encoded here by the

$$\text{ordinal } \sum_{j=n}^{j=0} \omega^j i_j.$$

□

A few remarks:

- One can prove that the graph of $x \mapsto \omega x$ is not M -recognizable, either in a direct way, or using the fact that by [8] the theory of $(\omega^\omega; +, x \mapsto \omega x)$ is undecidable, while the theory of $(\omega^\omega; +, x \mapsto x\omega)$ is decidable since the function $x \mapsto x\omega$ is definable in $(\omega^\omega; +)$ which has a decidable theory.
- We could reformulate the above results by replacing $(\omega^\omega; +)$ by the structure $(\omega; \times, <_P)$ where $x <_P y$ holds iff $x < y$ and x, y are prime numbers. In this case we encode every word $u = a_0 \dots a_n$ over the alphabet ω by the integer $c'(u) = 2^{a_0+1} 3^{a_1+1} \dots p_n^{a_n+1}$ where p_n denotes the n -th prime number. We refer to [16] for details about the link between $(\omega^\omega; +)$ and $(\omega; \times, <_P)$.

4 An extension of the Feferman-Vaught formalism

The automata and logic that we introduced in the previous sections do not allow comparisons between symbols from different positions. For instance, for every structure M with infinite domain, the language $\{ss \mid s \in |M|\}$ is not $MSO(M)$ -definable. More generally, given any formula $\varphi(x, y)$ in the language of M , the language $\{s_1 s_2 \mid M_\# \models \varphi(s_1, s_2)\}$ is not in general $MSO(M)$ -definable.

A natural way to add expressive power is to extend MSO with predicates such as $P(x, y)$ interpreted as “ x, y are two positions in w such that $w(x) = w(y)$ ”, or more generally predicates interpreted as “ x, y are two positions in w such that $M_\# \models \varphi(w(x), w(y))$ ” (where φ is a $\mathcal{L}_\#$ -formula).

However these extensions do not add expressive power when M is finite, and lead to undecidable theories in case M has an infinite domain (we refer the reader e.g. to [2] where it is shown that much weaker related formalisms have undecidable FO theories).

Thus in order to get decidability results we have to restrict the use of these new predicates. Below we describe a syntactic fragment for which the satisfiability problem still reduces to decidability of the first-order theory of M .

Given a \mathcal{L} -structure M , we associate to every $\mathcal{L}_\#$ -formula F with m free variables some m -ary relational symbol θ_F . We define then $MSO^+(\mathcal{L})$ as MSO over the language $\{<, (\theta_F)_{F \in \mathcal{F}}\}$ where \mathcal{F} denotes the set of $\mathcal{L}_\#$ -formulas with at least one free variable.

The interpretation of $MSO^+(\mathcal{L})$ sentences is similar to $MSO(\mathcal{L})$, but for every $\mathcal{L}_\#$ -formula F with m free variables the interpretation of $\theta_F(x_1, \dots, x_m)$

is “the positions x_1, \dots, x_m in the word w satisfy $M_{\#} \models F(w(x_1), \dots, w(x_m))$ ”. We say that $X \subseteq \Sigma^*$ is $MSO^+(M)$ –definable if there exists a $MSO^+(\mathcal{L})$ –sentence φ which defines X . The definition can be extended easily to the case of subsets $X \subseteq (\Sigma^*)^n$. Note that if one allows only $MSO^+(\mathcal{L})$ sentences where the predicates θ_F are unary, we get nothing but $MSO(\mathcal{L})$.

Example 16

- let $M = (\omega; +)$. The language $X \subseteq \omega^*$ of words over ω of the form $w = s_1 \dots s_k s'_1 \dots s'_l$ such that $s'_j \geq 2s_k$ for every $j \in \{1, \dots, l\}$, is $MSO^+(M)$ –definable by the $MSO^+(\mathcal{L})$ –sentence

$$\exists x(\exists x'(x < x') \wedge \forall y(x < y \rightarrow \theta_F(x, y)))$$

where

$$F(x_1, x_2) : \exists z(x_2 = x_1 + x_1 + z)$$

denotes the formula which expresses that $x_2 \geq 2x_1$.

- Let $M = (\Sigma^*; EqLength, <_{pref}, \{L_a\}_{a \in \Sigma})$ be the structure S used in Section 3.3. The set of words $w = s_0 s_1 \dots s_n$ over the infinite alphabet $\Gamma = \Sigma^*$ such that all even positions carry the same symbol, and all odd positions carry a symbol which is a prefix of s_0 , is $MSO^+(M)$ –definable. Indeed a convenient $MSO^+(\mathcal{L})$ –sentence is

$$\exists X[EvenPositions(X) \wedge \exists x \in X \forall y \in X \theta_{F_1}(x, y) \wedge \exists z(\forall t < z \wedge \forall y \notin X \theta_{F_2}(y, x))]$$

where $EvenPositions(X)$ is a MSO-formula which expresses that X consists of the set of even positions of w , and

$$F_1(v_1, v_2) : v_1 = v_2 ;$$

$$F_2(v_1, v_2) : v_1 <_{pref} v_2.$$

The formalism $MSO^+(\mathcal{L})$ is in general too expressive with respect to decidability, thus we have to consider a syntactic fragment of it.

We define $MSO^+_R(\mathcal{L})$ as the syntactic fragment of $MSO^+(\mathcal{L})$ consisting in formulas of the form

$$\exists x_1 \dots \exists x_n \varphi(x_1, \dots, x_n)$$

where φ is a $MSO^+(\mathcal{L})$ –formula which satisfies the following constraint, which we denote by (*): *all predicates of the form θ_F in φ have the form $\theta_F(x_1, \dots, x_n, y)$, i.e. contain at most one free variable distinct from the x_i s.*

Note that the two examples above are $MSO^+_R(\mathcal{L})$ –formulas.

Theorem 17 *The emptiness problem for $MSO^+_R(M)$ –definable languages reduces to the decidability of the FO theory of M .*

Proof To each $MSO_R^+(\mathcal{L})$ -formula ψ of the form

$$\exists x_1 \dots \exists x_n \varphi(x_1, \dots, x_n)$$

where φ satisfies (*) we associate in an effective way a $MSO(\mathcal{L}')$ -formula ψ' where \mathcal{L}' is obtained by adding to \mathcal{L} new constant symbols c_1, \dots, c_n , such that for every \mathcal{L} -structure M , φ is satisfiable by some word over Σ iff there exists some \mathcal{L}' -expansion M' of M such that the set of words over $|M'|$ defined by φ' is not empty.

The transformation proceeds as follows. First, we can assume that all formulas of the form $\theta_F(x_1, \dots, x_n, y)$ which appear in φ are such that y appears freely in θ_F : indeed if y does not appear in θ_F then $\theta_F(x_1, \dots, x_n)$ is equivalent to $\exists y(y = x_n \wedge \theta_{F'}(x_1, \dots, x_{n-1}, y))$ where F' is obtained from F by substituting y for x_n .

We define the $MSO(\mathcal{L}')$ -formula ψ' as

$$\exists x_1 \dots \exists x_n \left(\bigwedge_{i=1}^n \alpha_{F_i}(x_i) \wedge \varphi'(x_1, \dots, x_n) \right)$$

where $F_i(y)$ denotes the formula $y = c_i$ and φ' is obtained from φ by replacing every formula $\theta_F(x_1, \dots, x_n, y)$ by the formula $\alpha_{F'}(y)$ where F' is obtained from F by replacing every occurrence of x_i by the constant symbol c_i .

It is easy to check that for every \mathcal{L} -structure M , φ is satisfiable by some word model over Σ iff there exists some \mathcal{L}' -expansion M' of M such that $L(\varphi') \neq \emptyset$.

Assume that the formula φ' involves the $\mathcal{L}_\#$ -formulas F_1, \dots, F_p . Given M' , the question of whether the language defined by φ' is empty reduces to compute the set $E_{M'}$ of subsets $I \subseteq \{1, \dots, p\}$ such that there exists $a \in M'$ such that $(M' \models F_i(a) \text{ iff } i \in I)$. Thus it suffices to compute all possible sets $E_{M'}$ for all \mathcal{L}' -expansions M' of M . This can be computed effectively since for every subset E of subsets of $\{1, \dots, p\}$, one can find a \mathcal{L} -sentence H_E such that $M \models H_E$ iff there exists some \mathcal{L}' -expansion M' of M such that $E_{M'} = E$. The decidability of the FO theory of M allows then to conclude. \square

5 Discussion and conclusion

The proof of Theorem 17 makes uses of Büchi's decidability result for the WMSO theory of $(\omega; <)$. However the arguments are sufficiently general to apply to any decidable extension of WMSO. An interesting example is the WMSO theory T_{card} of ω , without $<$, but with the predicate $X \sim Y$ interpreted as “ X and Y have the same cardinality”. This theory was proven to be decidable by Feferman and Vaught in [11] by reduction to Presburger Arithmetic (by elimination of quantifiers, and without using the composition technique). The result was re-discovered and specified recently in the papers [14, 21], which show nice connections with issues in verification as well as constraint databases.

One can show that Theorem 17 holds with T_{card} , which provides a class of theories which are both decidable and quite expressive. As an example, if we set $M = (\Sigma^*; EqLength, <_{pref}, \{L_a\}_{a \in \Sigma})$ (the EES structure, whose FO theory is decidable [10]), then the corresponding syntactic fragment allows to express properties related to finite words w over the alphabet $\Sigma' = \Sigma^*$ (that is, finite sequences of words over Σ) such as “there exist two distinct symbols s, s' appearing in w such that at least one third of the symbols in w are prefix of s , or have the same length as s' ”. Another interesting example is the case $M = (\omega; +)$. In this case we obtain a decidable fragment for words over the alphabet ω , i.e. lists of natural numbers. This fragment could be an interesting formalism for the verification of programs which manipulate pointers and linked data structures.

By Proposition 3, M -automata capture the logic $MSO(\mathcal{L})$. Thus a natural issue is to get an automata counterpart for the logic $MSO_R^+(\mathcal{L})$. An idea is to consider M -automata equipped with a finite number of “write once” registers. In addition to the usual transitions of M -automata, these automata are allowed to write the current symbol in some empty register, and test whether the symbols currently stored in the registers and the current symbol satisfy some $\mathcal{L}_\#$ -sentence in $M_\#$. Once a symbol is stored in some register, the automaton cannot store any other symbol in this register. In order to capture the fragment $MSO_R^+(\mathcal{L})$, it seems that one should also allow non-deterministic “epsilon-transitions” where the automaton chooses to store some symbol from the input alphabet in some (empty) register.

Another interesting issue would be to find (more natural) extensions of the Feferman-Vaught formalism in the spirit of Theorem 17. The formalism $MSO^+(\mathcal{L})$ allows the use of predicates θ_F for all $\mathcal{L}_\#$ -formulas F , which makes necessary to consider the fragment $MSO_R^+(\mathcal{L})$ in order to get decidability results. It would be interesting to find other fragments of $MSO^+(\mathcal{L})$ obtained by imposing conditions on the $\mathcal{L}_\#$ -formulas F . One can consider e.g the case where we allow only the use of formulas F which define equivalence relations in M . Note that similar results are already proven in the papers [2, 4].

Finally, it seems that all results in this paper can be extended rather easily to the case of infinite words as well as (in)finite binary trees, by relying on classical decidability results for MSO theories.

References

- [1] J.M. Autebert, J.Beauquier, and L. Boasson. Langages sur des alphabets infinis. *Discrete Applied Mathematics*, 2:1–20, 1980.
- [2] M. Bojanczyk, C. David, A.Muscholl, T. Schwentick, and L. Segoufin. Two-variable logic on words with data. preprint, 2005.
- [3] P. Bouyer, A. Petit, and D. Thérien. An algebraic approach to data languages and timed languages. *Inf. Comput*, 182(2), 2003.

- [4] Patricia Bouyer. A logical characterization of data languages. *IPL*, 84(2):75–85, 2002.
- [5] V. Bruyère, G. Hansel, C. Michaux, and R. Villemaire. Logic and p -recognizable sets of integers. *Bull. Belg. Math. Soc. - Simon Stevin*, 1(2):191–238, 1994.
- [6] J. R. Büchi. Weak second-order arithmetic and finite automata. *Z. Math. Logik und grundl. Math.*, 6:66–92, 1960.
- [7] J. R. Büchi. Transfinite automata recursions and weak second order theory of ordinals. In *Proc. Int. Congress Logic, Methodology, and Philosophy of Science, Jerusalem 1964*, pages 2–23. North Holland, 1965.
- [8] C. Choffrut and S. Grigorieff. The elementary theories of ω^ω with addition and left resp. right translations. preprint, 2005.
- [9] C. Choffrut and S. Grigorieff. Logic for finite words over infinite alphabets. preprint, 2005.
- [10] S. Eilenberg, C. Elgot, and J. Shepherdson. Sets recognized by n -tape automata. *J. Alg.*, 13(4):447–464, 1969.
- [11] S. Feferman and R.L. Vaught. The first order properties of products of algebraic systems. *Fundam. Math.*, 47:57–103, 1959.
- [12] B.R. Hodgson. Decidabilité par automate fini. *Ann. Sci. Math. Quebec*, 7:39–57, 1983.
- [13] Michael Kaminski and Nissim Francez. Finite-memory automata. *Theoretical Computer Science*, 134(2):329–363, 1994.
- [14] V. Kuncak, H. H. Nguyen, and M. Rinard. An algorithm for deciding bapa: Boolean algebra with presburger arithmetic. In *Proc. CADE-20*, volume 3632 of *Lect. Notes in Comput. Sci.*, pages 260–277, 2005.
- [15] J. A. Makowsky. Algorithmic uses of the Feferman-Vaught theorem. *Annals of Pure and Applied Logic*, 126(1–3):159–213, 2004.
- [16] F. Maurin. The theory of integer multiplication with order restricted to primes is decidable. *J. Symb. Log.*, 62(1):123–130, 1997.
- [17] Andrzej Mostowski. On direct products of theories. *J. Symb. Log.*, 17(1):1–31, 1952.
- [18] F. Neven, T. Schwentick, and V. Vianu. Finite state machines for strings over infinite alphabets. *ACM Trans. Comput. Log.*, 5(3):403–435, 2004.
- [19] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Comptes Rendus du Premier Congrès des Mathématiciens des Pays Slaves*, pages 92–101, 395, Warsaw, 1927.

- [20] A. Rabinovich. Selection and uniformization in generalized product. *Logic J. of IGPL*, pages 125–134, 2004.
- [21] P. Revesz. The expressivity of constraint query languages with boolean algebra linear cardinality constraints. In *Proc. ADBIS'04*, volume 3631 of *Lect. Notes in Comput. Sci.*, pages 167–182, 2005.
- [22] W. Sierpinski. *Cardinal and Ordinal Numbers*. PSW Warsaw, 2nd edition, 1965.
- [23] W. Thomas. Ehrenfeucht games, the composition method, and the monadic theory of ordinal words. In *Structures in Logic and Computer Science, A Selection of Essays in Honor of A. Ehrenfeucht*, number 1261 in *Lect. Notes in Comput. Sci.*, pages 118–143. Springer-Verlag, 1997.
- [24] S. Wohrle and W. Thomas. Model checking synchronized products of infinite transition systems. In *Proceedings of the 19th Annual Symposium on Logic in Computer Science (LICS)*, pages 2–11. IEEE Computer Society, 2004.