Long Words: the theory of concatenation and ω-power

Stephen L. Bloom*
Stevens Institute of Technology
Department of Computer Science
Hoboken, NJ 07030
bloom@cs.stevens-tech.edu

Christian Choffrut
LIAFA, University of Paris 7
2 Place Jussieu
75251 Paris Cedex 05
cc@liafa.jussieu.fr

March 26, 1999

1 Introduction

In his study of regular omega-languages, Wilke [Wil91, Wil93] introduced "binoids", or "Wilke algebras" in the terminology of [PP95], which are two-sorted structures (M_f, M_ω) equipped with an associative product $M_f \times M_f \to M_f$, an "ω-power operation", $x \in M_f \mapsto x^\omega \in M_\omega$, and a mixed product $M_f \times M_\omega \to M_\omega$ satisfying

$$\begin{aligned} (x \cdot y)^\omega &= x \cdot (y \cdot x)^\omega, \quad x \in M_f \\ (x^n)^\omega &= x^\omega, \quad x \in M_f,\ n \geq 1. \end{aligned}$$

One of the authors had already been engaged in the study of two-sorted labeled posets equipped with the operations of serial product $P \cdot Q$ and omega-power P^ω, defined below [BÉ98]. Here, we remove the two sorted structure and keep the two operations. In the present context, the labeled posets form a one-sorted structure equipped with the two operations. In this paper, we axiomatize the variety these posets generate. It turns out that the answer involves certain words of infinite ordinal length, explaining the title.

*Supported in part by the U.S.-Hungarian Joint Fund, grant 351 and by LIAFA, Université Paris 7.

2 Labeled Posets

An A-**labeled poset** $(P, \leq, \ell)$ consists of a poset $(P, \leq_P)$, and an assignment $\ell : P \to A$ of a letter $v\ell$ in A to each vertex v in P. Sometimes we write P for the labeled poset as well as the unlabeled underlying poset.

A **morphism** $f : P \to Q$ of A-labeled posets is a function $P \to Q$ which preserves the ordering and the labeling. We agree to identify isomorphic labeled posets, without further mention.

Suppose that A is a set and P, Q are A-labeled posets with disjoint underlying sets. The **series product** of P and Q is defined by

$$P \cdot Q \quad := \quad (P \cup Q, \leq_{P \cdot Q})$$

where

$$x \leq_{P \cdot Q} y \quad \Leftrightarrow \quad x \leq_P y \text{ or } x \leq_Q y \text{ or } (x \in P \text{ and } y \in Q).$$

so that every element of P is less than each element of Q. Define the ω-**power** P^ω as the countable series product of P with itself:

$$P^\omega \quad := \quad P \cdot P \cdot P \cdot \ldots .$$

(More formally, we define $P^\omega = (P \times \{1, 2, \ldots\}, \leq)$, where $(p, i) \leq (p', j)$ if $i < j$ or $(i = j$ and $p \leq_P p')$. The label of (p, i) is the label of p.)

Since we identify isomorphic A-labeled posets, it follows that there is a small set of all finite (or countably infinite) A-labeled posets. Thus, the collection of all finite or countable A-labeled posets, $(Pos(A), \cdot, {}^\omega)$ equipped with the binary operation of series product and the unary operation of ω-power forms an algebra. We want to axiomatize the variety generated by these algebras.

We list some equations clearly satisfied by the labeled posets.

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \tag{1}$$

$$(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega \tag{2}$$

$$(x^n)^\omega = x^\omega, \quad n \geq 1. \tag{3}$$

Let Ax denote the collection of these identities and let V denote the variety of all models of Ax, so that, in particular, for any set A, $(Pos(A), \cdot, {}^\omega)$ belongs to V. In fact, any subcollection of $Pos(A)$ closed under series product and ω-power forms a model, such as $W_k(A)$, the collection of all A-labeled posets of width at most k, for any fixed $k \geq 1$.

Note the following consequences of the axioms.

Proposition 2.1 *The following identities hold in any model of Ax.*

$$\begin{aligned} x^\omega &= x^k \cdot x^\omega, \quad k \geq 1 && (4) \\ ((x^\omega y)^n x^p)^\omega &= (x^\omega y)^\omega, \quad n \geq 1, p \geq 0. && (5) \end{aligned}$$

Proof. For (4), it is sufficient to prove the case $k = 1$. By the axiom (3) with $n = 2$,

$$(x^2)^\omega = x^\omega,$$

and by the axiom (2) with $x = y$,

$$(x^2)^\omega = x \cdot (x^2)^\omega.$$

As for (5), we notice first that if $n, p \geq 1$,

$$x^p (x^\omega y)^n = (x^\omega y)^n, \qquad (6)$$

since if $n = 1$, $x^p(x^\omega y) = (x^p x^\omega)y = x^\omega y$, by (4). If $n > 1$, $x^p(x^\omega y)^n = x^p(x^\omega y)(x^\omega y)^{n-1}$, and $x^p(x^\omega y) = x^\omega y$. Now we calculate using the axioms (2) and (3):

$$\begin{aligned} ((x^\omega y)^n x^p)^\omega &= (x^\omega y)^n (x^p (x^\omega y)^n)^\omega \quad \text{by (6)}, \\ &= ((x^\omega y)^n)^\omega \\ &= (x^\omega y)^\omega. \quad \square \end{aligned}$$

We will be concerned with the following labeled posets.

Definition 2.2 *We let* $\mathbf{W(A)}$ *denote the least collection of A-labeled posets containing the singletons labeled a, $a \in A$, closed under the two operations of series product and ω-power.*

When the underlying poset of an A-labeled poset P is an ordinal, or more generally, a well-ordered set, P is called **an ordinal word** on the alphabet A. (When A is understood, we say just "ordinal word".) Note that if $P \in W(A)$, P is an ordinal word. When $(P, \leq_P, \ell)$ is an ordinal word and the domain of ℓ is the ordinal α, we write $|P|$ for α, called the **length** of P. When $\beta < \alpha$, $\{x : \beta \leq x < \alpha\}$ is also well-ordered, and the restriction of the labeling function of P to this set is also an ordinal word, called the **tail of P at β**, written $\mathsf{tail}[P, \beta]$.

Note that if $\beta + \gamma < \alpha$, then

$$\mathsf{tail}[\mathsf{tail}[P, \beta], \gamma] = \mathsf{tail}[P, \beta + \gamma].$$

Definition 2.3 *An ordinal word is* **tail-finite** *if it has at most finitely many nonisomorphic tails.*

Example 2.4 The word $abab\ldots$ of length ω has two nonisomorphic tails; the word $abab^2ab^3\ldots ab^n\ldots$ of length ω has infinitely many nonisomorphic tails.

We will use the following fact.

Proposition 2.5 *Let u, v be ordinal words. Then uv is a tail-finite word iff both u and v are tail-finite; similary, u^ω is tail-finite iff u is.*

Proof. Any tail of uv is either a tail of v or of the form $t \cdot v$, for a tail t of u. Thus, if u has n tails, up to isomorphism, and v has m, then uv has at most $n + m$ tails, up to isomorphism. Any tail of u^ω is isomorphic to one of the form $t \cdot u^\omega$, for a tail t in P. Thus, u^ω has at most the number of tails that u has. $\square$

3 Other Models

If $\mathcal{W}_k(A)$ is the collection of all subsets of A-labeled posets of width at most k, then $\mathcal{W}_k(A)$ equipped with these operations is a model of Ax.

Suppose that L, L' are **sets** of nonempty A-labeled posets (of width at most k). Define

$$\begin{aligned} L \cdot L' &:= \{P \cdot Q : P \in L,\ Q \in L'\} \\ L^\omega &:= \{P_1 \cdot P_2 \cdot \ldots : P_i \in L\}. \end{aligned}$$

Then the operations $L, L' \mapsto L \cdot L'$ and $L \mapsto L^\omega$ satisfy Ax. In particular, if $k = 1$, the collection of all sets of words on A of length $< \omega^\omega$ is a model of Ax.

4 Terms

Fix the set A. The set of A-**terms** T_A is the least set of expressions built from the letters in the alphabet A, using the binary function symbol $\cdot$ and the unary function symbol ω in the usual way. (When $A = \emptyset$, $T_A = \emptyset$.) We write $t \cdot t'$ instead of $\cdot(t, t')$ and t^ω instead of $\omega(t)$. For later use, a term not of the form $t \cdot t'$ is called **primitive**. A primitive term is either a letter in A or an ω-**term** t^ω, for some term t. Since the operation symbol $\cdot$ will always be interpreted as an associative operation, we will neglect to parenthesize product terms, and write, for example

$$t = t_1 \cdot t_2 \cdot \ldots \cdot t_k.$$

Definition 4.1 *Each term t denotes an A-ordinal word $[\![t]\!]$ on the alphbet A.*

$$\begin{aligned} [\![a]\!] &:= a, \quad a \in A \\ [\![t \cdot t']\!] &:= [\![t]\!] \cdot [\![t']\!] \\ [\![t^\omega]\!] &:= [\![t]\!]^\omega. \end{aligned}$$

The **length** *of the word $[\![t]\!]$ denoted by the term t will be written $|t|$ instead of $\|[\![t]\!]\|$, for obvious reasons.*

$$\begin{aligned} |a| &:= 1, \quad a \in A \\ |t \cdot t'| &:= |t| + |t'| \\ |t^\omega| &:= |t| \times \omega. \end{aligned}$$

Note that the operations $+, \times$ of ordinal arithmetic are being used here. (See [Sier58] for all you want to know about ordinal arithmetic.)

We omit the easy proof of the following Proposition.

Proposition 4.2 *For each term t, $|t|$ is the length of $[\![t]\!]$.* $\square$

Proposition 4.3 *Suppose that t, t' are terms such that $|t \cdot t'| = \omega^n$, for some $n \geq 1$. Then $|t| < \omega^n$ and $|t'| = \omega^n$. If $|t^\omega| = \omega^n \times m$ then $m = 1$ and $\omega^{n-1} \leq |t| < \omega^n$.*

Proof. Indeed, for any ordinals α, β, if $\alpha \geq \omega^n$, and $\beta > 0$, $\alpha + \beta > \omega^n$, so when $\alpha + \beta = \omega^n$, $\alpha < \omega^n$; if also α and $\beta < \omega^n$, $\alpha + \beta < \omega^n$. Similarly, if $\alpha \times \omega = \omega^n \times m$, then necessarily $m = 1$ and $\omega^{n-1} \leq \alpha < \omega^n$, since, for any $k \geq 1$,

$$(\omega^{k-1} \times m_1 + \omega^{k-2} \times m_2 + \ldots + \omega \times m_{k-1} + m_k) \times \omega = \omega^k.$$

□

The next fact follows from the previous Proposition.

Proposition 4.4 *Suppose that $n \geq 1$, $m \geq 0$ and t is a term such that*

$$\omega^n \times m \leq |t| < \omega^n \times (m+1).$$

Then, (temporarily letting the empty word denote a term of length 0), there are terms u_i, $i \in [m+1]$, some of which may be empty, and nonempty terms v_i, $i \in [m]$, such that t is the term

$$u_1 \cdot v_1^\omega \cdot \ldots \cdot u_m \cdot v_m^\omega \cdot u_{m+1},$$

and

$$\begin{array}{rcl} |u_i| & < & \omega^n, \quad i \in [m+1], \\ \omega^{n-1} & \leq & |v_i| \; < \; \omega^n, \quad i \in [m]. \end{array}$$

Proof. We use induction on m. The case $m = 0$ is trivial. Now, write t as a product $t_1 \cdot \ldots \cdot t_k$ of primitive terms t_i. If $|t_i| < \omega^n$, for all $i \in [k]$, then $|t| < \omega^n$ also. So there is a first term, say t_{j_1} with $|t_{j_1}| \geq \omega^n$. By Proposition 4.3, necessarily t_{j_1} has the form $(v_1)^\omega$, for some term v_1, and $|t_{j_1}| = |v_1^\omega| = \omega^n$. Thus, if $1 < j_1$, let u_1 be the product of the terms t_i, for $i < j_1$. If $j_1 = 1$, u_1 is empty. Now $\omega^n \times (m-1) \leq |t_{j_1+1} \cdot \ldots \cdot t_k| < \omega^n \times m$, and hence by the induction assumption, we are done. □

5 Characterizing $W(A)$

We give a structural characterization of the ordinal words in $W(A)$, defined above in Definition 2.2.

Theorem 5.1 *The following conditions are equivalent for an ordinal word u on the alphabet A.*

1. *u belongs to $W(A)$.*
2. *$|u| < \omega^\omega$ and u is tail-finite.*
3. *There is a term $t \in T_A$ with $u = [\![t]\!]$.*

The proof is divided into a number of propositions.

Proposition 5.2 *If u is an ordinal word that belongs to $W(A)$, then the length of u is $< \omega^\omega$, and u is tail-finite. Thus, condition (1) of Theorem 5.1 implies condition (2)*

Proof. Each singleton word in $W(A)$ has length $< \omega^\omega$ and is tail-finite, and these two properties are preserved by the two operations $u, v \mapsto uv$ and $u \mapsto u^\omega$. Indeed, if α, β are any two ordinals $< \omega^\omega$, then $\alpha + \beta < \omega^\omega$ and $\alpha^\omega < \omega^\omega$.

As for being tail-finite, any tail of uv is either a tail of v or of the form wv, for a tail w of u. Thus, if u has n tails, up to isomorphism, and v has m, then uv has at most $n + m$ tails, up to isomorphism. Any tail of u^ω is isomorphic to one of the form $w \cdot u^\omega$, for a tail w of u. Thus, u^ω has at most the number of tails that u has. Thus, every ordinal word in $W(A)$ is tail-finite and has length less than ω^ω. □

Proposition 5.3 *If $u = [\![t]\!]$, then $u \in W(A)$. Thus, condition (3) of Theorem 5.1 implies condition (1).*

Proof. By induction on the structure of the term t. If t is a, then $a \in W(A)$. If $t = t_1 \cdot t_2$, then since $[\![t_i]\!] \in W(A)$, so is $[\![t_1 \cdot t_2]\!]$; lastly, if $t = t_1^\omega$, then since $[\![t_1]\!] \in W(A)$, so is $[\![t_1]\!]^\omega = [\![t]\!]$. □

Proposition 5.4 *If u is a tail-finite word of length $|u| < \omega^\omega$, then $u = [\![t]\!]$ for some term t. Thus, condition (2) implies condition (3).*

Proof. Since the length of u may be written as

$$|u| \quad = \quad \omega^n \times m_n + \omega^{n-1} \times m_{n-1} + \ldots + m_0,$$

for some nonnegative integers m_i, $i = 0, \ldots, n$, the proof follows from the Lemma:

Lemma 5.5 *Suppose that u is a tail-finite word. For each $n \geq 0$, if $\omega^n \leq |u|$, then there is a term t of length ω^n such that*

$$u = [\![t]\!] \cdot \mathsf{tail}[u, \omega^n].$$

If $n > 0$, t has the form $t_1(t_2)^\omega$ (or just t_2^ω) where $|t_1| < \omega^n$ and $\omega^{n-1} \leq |t_2| < \omega^n$.

Proof of Lemma 5.5. Since the case $n = 0$ is obvious, assume $n > 0$, so that $\omega^n = \sup_k \omega^{n-1} \times k$. Then, by the induction hypothesis, there is a term of length ω^{n-1}, say s_1 such that

$$u = [\![s_1]\!] \cdot \mathsf{tail}[u, \omega^{n-1}].$$

Since $\mathsf{tail}[u, \omega^{n-1}]$ has length at least as long as ω^n, there is a term s_2 of length ω^{n-1}, such that

$$\mathsf{tail}[u, \omega^{n-1}] = [\![s_2]\!] \cdot \mathsf{tail}[\mathsf{tail}[u, \omega^{n-1}], \omega^{n-1}],$$

so that

$$u = [\![s_1 \cdot s_2]\!] \cdot \mathsf{tail}[u, \omega^{n-1} \times 2].$$

In the same way, for each $k > 0$, we can find terms of length ω^{n-1}, $s_1, \ldots, s_k$ so that

$$u = [\![s_1 \cdot \ldots \cdot s_k]\!] \cdot \mathsf{tail}[u, \omega^{n-1} \times k].$$

Since u is tail-finite, there is a least m, k such that

$$\mathsf{tail}[u, \omega^{n-1} \times m] = \mathsf{tail}[u, \omega^{n-1} \times (m + k + 1)],$$

showing that

$$u = [\![s_1 \cdot \ldots \cdot s_{m-1} \cdot (s_m \cdot \ldots \cdot s_{m+k})^\omega]\!] \cdot \mathsf{tail}[u, \omega^n].$$

Thus, we let $t = s_1 \cdot \ldots \cdot s_{m-1} \cdot (s_m \cdot \ldots \cdot s_{m+k})^\omega$. Since each s_i is a term of length ω^{n-1}, t has length ω^n. □

The following Corollaries are consequences of Theorem 5.1 and Proposition 2.5.

Corollary 5.6 *If u is a tail-finite word with $|u| = \omega^{n_1} + \ldots + \omega^{n_k}$ with $n_1 \geq \ldots \geq n_k$, then there are terms t_i of length ω^{n_i}, $i \in [k]$, such that*

$$u = [\![t_1 \cdot \ldots \cdot t_k]\!].$$

□

Corollary 5.7 *If u, v are ordinal words such that $uv = [\![t]\!]$, for some term $t \in T_A$, then there are terms r, s with $u = [\![r]\!]$ and $v = [\![s]\!]$; if u is an ordinal word such that for some term $t \in T_A$, $u^\omega = [\![t]\!]$, then $u = [\![r]\!]$, for some term r.*

Corollary 5.8 *If u_i, v_i, $i = 1, 2$ are terms such that $[\![u_1 \cdot v_1]\!] = [\![u_2 \cdot v_2]\!]$ and $[\![u_1]\!] \geq [\![u_2]\!]$, then there is a term w such that $[\![u_1]\!] = [\![u_2 \cdot w]\!]$ and $[\![v_2]\!] = [\![w \cdot v_1]\!]$.* □

6 The Main Theorem

We need some preliminary facts on ordinal words whose length is $< \omega^\omega$. From now on, "ordinal word" means one whose length is $< \omega^\omega$.

If the length of the word x is $\alpha = \omega^n \times m_n + \ldots + \omega \times m_1 + m_0$, we say that the **degree of** x is n and write $\partial_x = n$, following [CH98].

Proposition 6.1 *For words x, y of length $< \omega^\omega$,*

$$\begin{aligned} \partial_{xy} &= \max\{\partial_x, \partial_y\} \\ \partial_{x^\omega} &= \partial_x + 1 \\ \partial_{x^k} &= \partial_x, \quad k \geq 1. \quad \square \end{aligned}$$

We will rely on the following theorem.

Theorem 6.2 [CH98]. *Suppose that x, y are ordinal words of length $< \omega^\omega$. Then $x^\omega = y^\omega$ iff $\partial_x = \partial_y$ and there are words u, v and nonnegative integers n, m, p, q such that*

$$\begin{aligned} x &= (u^\omega v)^n u^p \\ y &= (u^\omega v)^m u^q. \end{aligned}$$

Corollary 6.3 *Suppose that x, y, z are ordinal words of length $< \omega^\omega$. Then if $xy^\omega = z^\omega$ and $|x| < |z|$, then $z = xu$, for some ordinal word u and $y^\omega = (ux)^\omega$. Thus, there are words v, w such that y and ux are in $(v^\omega w)^* v^*$ and $\partial_y = \partial_{ux}$.* $\square$

The crucial fact is proved next.

Theorem 6.4 *Let s, t be terms such that $[\![s]\!] = [\![t]\!]$. Then $s = t$ is true in all models of* Ax*, i.e., the identity $s = t$ is provable from* Ax.

Proof. Suppose that n is the least integer such that $|s| = |t| < \omega^{n+1}$. We use induction on n to show $s = t$ is provable. If $n = 0$, the two terms differ at most in the parenthesizing of the common letters in each, and hence by the axiom (1), $s = t$ is provable. Now assume that if $|s| = |t| < \omega^{n+1}$ and $[\![s]\!] = [\![t]\!]$, then $s = t$ is provable from Ax. We will prove that if $\omega^{n+1} \leq |s| = |t| < \omega^{n+2}$ and $[\![s]\!] = [\![t]\!]$, then $s = t$ is provable from Ax.

We prove first that if $|s| = |t| = \omega^{n+1}$, then $s = t$ is provable. In this case, by Proposition 4.4, we have $s = u_1 \cdot v_1^\omega$ and $t = u_2 \cdot v_2^\omega$, where where $|u_i| < \omega^{n+1}$ and $\omega^n \leq |v_i| < \omega^{n+1}$. Assume without loss of generality that $|u_1| \leq |u_2|$. Then, by Corollary 5.7, we have $[\![u_2]\!] = [\![u_1 \cdot u]\!]$ and

$$[\![v_1^\omega]\!] = [\![u \cdot v_2^\omega]\!],$$

for some term u. Further, the identity

$$u_2 = u_1 \cdot u$$

is provable, by the induction hypothesis.

If $|v_1| \leq |u|$, then $k|v_1| \leq |u| < (k+1)|v_1|$ for some $0 < k < \omega$. By Corollary 5.8 applied to the equality $[\![v_1^\omega]\!] = [\![v_1^k \cdot v_1^\omega]\!] = [\![u \cdot v_2^\omega]\!]$, there exists a term $w \in T_A$ with $|w| < |v_1|$ such that $[\![v_1^k \cdot w]\!] = [\![u]\!]$ and $[\![v_1^\omega]\!] = [\![w \cdot v_2^\omega]\!]$. The identity $v_1^\omega = v_1^k \cdot v_1^\omega$ is provable, by (4), and the identity $v_1^k \cdot w = u$ is provable by the induction assumption. We need show only that

$$v_1^\omega = w \cdot v_2^\omega \tag{7}$$

is also provable. But in this case, Corollary 5.8 applied to $[\![v_1^\omega]\!] = [\![v_1 \cdot v_1^\omega]\!] = [\![w \cdot v_2^\omega]\!]$ implies there exists a term $w_1 \in T_A$ for which $[\![v_1]\!] = [\![w \cdot w_1]\!]$ and $[\![w_1 \cdot v_1^\omega]\!] = [\![v_2^\omega]\!]$ holds. The identity $v_1 = w \cdot w_1$ is provable, by the induction assumption and $w_1 \cdot v_1^\omega = w_1 \cdot (w \cdot w_1)^\omega = (w_1 \cdot w)^\omega$ is provable by axiom 1.

We show $(w_1 \cdot w)^\omega = v_2^\omega$ is provable also. Indeed, by Theorem 6.2, there exist ordinal words α_1, α_2 and integers n, p, m, q such that $[\![w_1 \cdot w]\!] = (\alpha_1^\omega \alpha_2)^n \alpha_1^p$ and $[\![v_2]\!] = (\alpha_1^\omega \alpha_2)^m \alpha_1^q$. By Corollary 5.7 there are two terms $z_1, z_2 \in T_A$ such that $[\![z_1]\!] = \alpha_1$ and $[\![z_2]\!] = \alpha_2$. Thus equalities $w_1 \cdot w = (z_1^\omega z_2)^n z_1^p$ and $v_2 = (z_1^\omega z_2)^m z_1^q$ are provable, by the induction hypothesis, and $(w_1 \cdot w)^\omega = v_2^\omega$ holds by identity (5).

If $|v_1| > |u|$ holds, then $|u| + k|v_2| \leq |v_1| < (k+1)|v_2|$ for some $0 < k < \omega$. Then Corollary 5.8 applied to equality $[\![v_1 \cdot v_1^\omega]\!] = [\![(u \cdot v_2^k) \cdot v_2^\omega]\!]$ implies there exists a term $w \in T_A$ with $|w| < |v_2|$ such that $[\![v_1]\!] = [\![(u \cdot v_2^k) \cdot w]\!]$ and $[\![v_2^\omega]\!] = [\![w \cdot v_1^\omega]\!]$. The identities $v_1^\omega = v_1 \cdot v_1^\omega$ and $u \cdot v_2^\omega = (u \cdot v_2^k) \cdot v_2^\omega$ are provable from the axioms. The identity $v_1 = (u \cdot v_2^k) \cdot w$ is provable, by induction, and the identity $v_2^\omega = w \cdot v_1^\omega$ is of the same form as equation (7), and can be treated in the same way.

It remains to show that if s, t are terms with $[\![s]\!] = [\![t]\!]$ and $\omega^{n+1} < |s| = |t| < \omega^{n+2}$, then $s = t$ is provable. By Proposition 4.4, we may write

$$\begin{aligned} s &= u_0 v_0^\omega \cdot \ldots \cdot u_{m-1} v_{m-1}^\omega \cdot u_m \\ t &= u_0'(v_0')^\omega \cdot \ldots \cdot u_{m-1}(v_{m-1}')^\omega \cdot u_m', \end{aligned}$$

where $m \geq 1$ and $|u_i|, |u_i'| < \omega^{n+1}$ and $\omega^n \leq |v_i|, |v_i'| < \omega^{n+1}$. But then, since the segments of length ω^{n+1} must be identical, for $i < m$,

$$[\![u_i \cdot v_i^\omega]\!] \quad = \quad [\![u_i' \cdot (v_i')^\omega]\!],$$

and $[\![u_m]\!] = [\![u_m']\!]$. But $u_m = u_m'$ is provable by the induction hypothesis, and we have just shown that the the other identities are provable also. Thus $s = t$ is provable. □

As an immediate corollary of the preceding result, we may prove the main theorem.

Theorem 6.5 *$W(A)$ is freely generated by A in V.*

Proof. Suppose that $f : A \to M$ is a function from the set A to the underlying set of a model in V. Since the term algebra T_A is freely generated by A in the class of all algebras with one binary and one unary function, there is a unique extension of f to $f^\flat : T_A \to M$ which preserves all the operations. We define a morphism $\varphi : W(A) \to M$ as follows. If u is a word in $W(A)$, u is denoted by a term t, by Corollary 5.6. We map u to the image of t under $f^\flat$. The definition of this map is forced, and it is well-defined by Theorem 6.4. The map clearly preserves the operations. The proof is complete. □

Corollary 6.6 *The variety V is generated by the structures $(Pos(A), \cdot, ^\omega)$, as well as the collections $W_k(A)$ of A-labeled posets of width at most k, for any fixed $k \geq 1$ and the algebras $\mathcal{W}_k(A)$ of sets of A-labeled posets of width at most k.*

Remark 6.7 Since any ordinal below ω^ω is writable as a sum of nonincreasing powers of ω, in any model of Ax, the operation $x \mapsto x^\alpha$ has a natural definition, for any ordinal $\alpha < \omega^\omega$:

$$\begin{aligned} x^{\omega^{n+1}} &:= (x^{\omega^n})^\omega, \quad n \geq 1 \\ x^{\alpha+\beta} &:= x^\alpha \cdot x^\beta. \end{aligned}$$

7 No finite axiomatization

Z. Ésik has pointed out that a modification of a construction in [ÉB95] will show that there is no finite axiomatization of the variety V. We present this modification below.

Note that if there is any finite axiomatization, then a finite subset of the axioms 1, 2 and 3 will axiomatize V, by the compactness theorem.

Proposition 7.1 *For any finite subset E of the power identities (3), there is a model M_p of E and the identities (1), (2) which fails to satisfy*

$$(x^p)^\omega = x^\omega,$$

for some prime p. Thus, V is not finitely axiomatizable.

Proof. For any integer n, and any prime p, let $\theta_p(n)$ be the largest quotient of n which is not divisible by any prime $< p$. (For example, $\theta_5(2^3 3^2 5^2 7^2) = 5^2 7^2$.) Now let F denote all nonnegative integers, and let I_p denote all positive integers whose prime factorization contains only primes $\geq p$ (including 1), together with another element $\top$. Now assume that F and I_p are disjoint, say by replacing F by $F \times \{0\}$. Let $A_p = F \cup I_p$. Define the operations of $\cdot$ and $^\omega$ on A_p as follows.

$$x \cdot y \;:=\; \begin{cases} x + y & \text{if } x, y \in F \\ y & \text{if } x \in F \text{ and } y \in I_p \\ \top & \text{otherwise.} \end{cases}$$

$$x^\omega \;:=\; \begin{cases} \theta_p(x) \in I_p & \text{if } x \in F \\ \top & \text{otherwise.} \end{cases}$$

We show first that $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, for all $x, y, z \in A_p$. Indeed, if the left side is not $\top$, then $x, y \in F$ and the value is $x + (y + z)$, if $z \in F$, the same as the value of the right side, or is z, again, the value of the right hand side. Otherwise, at least one of x, y is in I_p and the value is $\top$, again the value of the right.

Now we show $(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega$. If $(x \cdot y)^\omega \neq \top$, then $x, y \in F$, and $(y \cdot x)^\omega = (x \cdot y)^\omega = x \cdot (y \cdot x)^\omega$. If $(x \cdot y)^\omega = \top$, then $(y \cdot x)^\omega = \top$ and $(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega = \top$.

Last, we show for all $2 \leq n < p$, $(x^n)^\omega = x^\omega$. Indeed, if $x \in I_p$, $x^n = \top$, and $x^\omega = \top$. If $x \in F$ and $n < p$, then $x^n = nx = \overbrace{x + x \ldots + x}^{n}$, and $(x^n)^\omega = \theta_p(nx) = \theta_p(x) = x^\omega$.

However, $x^p = px$ and $(x^p)^\omega = \theta_p(px) \neq \theta_p(x) = x^\omega$ for any $x \in F$. Thus, if p is a prime larger than all of the integers appearing in the identities in E, A_p is a model satisfying the claims of the proposition. □

8 Complexity

In this section, we show that there is a polynomial time algorithm to decide whether $[\![s]\!] = [\![t]\!]$, for any two terms $s, t \in T_A$. In brief, the method is to associate a "simple"

Choueka automaton $\mathcal{A}_t$ [Chou78] with each term $t \in T_A$; the size of $\mathcal{A}_t$ is $O(n)$ where n is the number of symbols in t. We then show that the subautomaton $\mathcal{B}$ of the product automaton $\mathcal{A}_s \times \mathcal{A}_t$ consisting of the states which are accessible from the initial state has a size which is bounded by the product of the sizes of $\mathcal{A}_s$ and $\mathcal{A}_t$ and show that it is possible to determine in time polynomial in the size of $\mathcal{B}$ whether $\mathcal{B}$ recognizes any word at all. It does if and only if $[\![s]\!] = [\![t]\!]$.

We use the following notation. For any set Q, we define the sets $[Q]_k$ by induction on $k \geq 0$.

$$\begin{aligned} [Q]_0 &:= Q \\ [Q]_{k+1} &:= \mathcal{P}([Q]_k), \end{aligned}$$

where $\mathcal{P}(X)$ denotes the powerset of X.

Definition 8.1 *A* ***Choueka automaton*** $\mathcal{A} = (h, Q, S, q_0, E, F)$ ***of height*** h ***on the alphabet*** A, *"CA" for short, consists of*

1. *An integer* $h \geq 0$*;*
2. *A finite subset* Q*, of "states";*
3. *An "initial state"* $q_0 \in Q$*;*
4. *A subset* $S_k \subseteq [Q]_k$*, for each* $k, 1 \leq k \leq h$*, the "states of height* k*". We let* $S_0 = Q$*, and let* S *denote the union* $\bigcup_{k=0}^{h} S_k$*.*
5. *A set of "transitions", or "arrows":*

$$E \subseteq S \times A \times S_0$$

6. *A subset* $F \subseteq S$ *of "final states".*

The **size** of the automaton $\mathcal{A}$ is the cardinality of the set S.

Suppose that $\alpha < \omega^{h+1}$ and that $u : \alpha \to A$ is a word of length α and let $\mathcal{A} = (h, Q, S, q_0, E, F)$ be a CA. A **run of** $\mathcal{A}$ **on** u is a sequence of states (q_β), indexed by the ordinals $\beta \leq \alpha$, such that if $\beta < \alpha$,

$$(q_\beta, u_\beta, q_{\beta+1}) \in E,$$

and, when $\beta = \lambda + \omega^k$, for $1 \leq k \leq h$, the state $q_{\lambda+\omega^k}$ is the subset of $[Q]_{k-1}$ defined by

$$q_{\lambda+\omega^k} \quad := \quad \{q : \exists^\infty i < \omega(q = q_{\lambda+\omega^{k-1}\times i})\}.$$

It is easy to see that if $\beta = \lambda + \omega^k$, for some $k \geq 0$, then $q_\beta \in [Q]_k$, and it is required that when $k > 0$, this set must belong to S_k.

A run $(q_\beta)_{\beta\leq\alpha}$ of $\mathcal{A}$ on u is **successful** if $q_\alpha \in F$; u is **recognized by** $\mathcal{A}$ if there is some successful run of $\mathcal{A}$ on u.

We are not dealing with automata in full generality. Rather, we are interested in those that recognize at most a single word. This justifies the following properties that we impose on a CA $\mathcal{A}$:

1) There is no arrow (q, a, q_0) whose target is the initial state;

2) There is no arrow (f, a, q) whose source is a final state $f \in F$;

3) For each state $q \in S$ there is at most one arrow whose source is q.

The first condition does not restrict the class of sets of words recognized by the automaton. The next two imply that the automaton recognizes at most one word. We call a Choueka automaton satisfying the above properties a **simple** Choueka automaton.

By removing all the final states which are not accessible from the inital state any automaton satisfying the 3 above conditions is equivalent to some automaton satisfying the additional condition

4) There is a unique final state f, i. e., $F = \{f\}$

Since the automaton satisfies condition 3), if the length of the recognized word has degree h, then for every $0 < k \leq h$:

5) Distinct states in $[Q]_k$ are disjoint subsets of $[Q]_{k-1}$.

Let Q_k for $0 \leq k \leq h$ be the set of states in S_k which are accessible from some state in Q. In particular $Q_0 = Q$. Condition 5) implies $|Q_0| \geq |Q_1| \ldots \geq |Q_h|$. In particular if n is the number of accessible states in the automaton, then we have

$$|Q| + h \leq n \leq (h+1)|Q| \tag{8}$$

Now we show how to construct a Choueka automaton $\mathcal{A}_t$ for each term t, by induction on the structure of t such that $\mathcal{A}_t$ recognizes precisely one word, namely $[\![t]\!]$.

1. If $t = a$, then $\mathcal{A}_a$ has height 0, and there are two states q_0, q_1 in S_0, and one arrow $(q_0, a, q_1) \in E$; the final state is q_1.

2. Assume that s, t are terms with $[\![s]\!] = u : \alpha \to A$ and $[\![t]\!] = v : \beta \to A$. Assume further that the automata for s, t are:

$$\mathcal{A}_s = (h_s, Q^s, S^s, q_0^s, E^s, f^s)$$
$$\mathcal{A}_t = (h_t, Q^t, S^t, q_0^t, E^t, f^t).$$

   where Q^s and Q^t are disjoint. Let $h = \max h_s, h_t$. Define $\mathcal{A}_{s\cdot t}$ as follows.

$$\mathcal{A}_{s\cdot t} \quad := \quad (h, Q^s \cup Q^t, S^s \cup S^t, q_0^s, E^s \cup E^t \cup \{(f^s, v_0, q_1^t)\}, f^t),$$

   where $(q_0^t, v_0, q_1^t) \in E^t$.

3. Lastly, assume that

$$\mathcal{A}_s = (h_s, Q^s, S^s, q_0^s, E^s, f^s)$$

   recognizes $u = [\![s]\!]$ and suppose that that $|u| = \omega^{h_s} \times m + \gamma$ where de degre of γ is less than h_s. Let $r_1, \ldots, r_m$ be the states of $\mathcal{A}_s$ visited by the prefixes of u of length $\omega^{h_s}, \omega^{h_s} \times 2, \ldots, \omega^{h_s} \times m$, in the successful run $(q_\beta)_{\beta \leq |u|}$ of $\mathcal{A}_s$ on u. Then define

$$\mathcal{A}_{s^\omega} \quad := \quad (h_s + 1, Q^s, S^s \cup \{r_1, \ldots, r_m\}, q_0^s, E^s \cup (f^s, u_0, q_1^s), f^{s^\omega}\})$$

   where where $(q_0^s, u_0, q_1^s) \in E^s$ and $f^{s^\omega} = \{r_1, \ldots, r_m\}$. Then $\mathcal{A}_{s^\omega}$ recognizes precisely u^ω.

Corollary 8.2 *For each term s in T_A there is a simple Choueka automaton $\mathcal{A}_s$ with at most $n + 1$ states and n arrows, where n is the number of symbols in s such that $\mathcal{A}_s$ recognizes the word $[\![s]\!]$.* □

We now describe an algorithm to determine, given terms s, t in T_A, whether $[\![s]\!] = [\![t]\!]$. First, it can be tested in time linear in the sum of the sizes of the terms s and t whether the degrees of the lengths of the associated words are equal. We assume from now on that they have the same degree, say h, since otherwise we may conclude $[\![s]\!] \neq [\![t]\!]$. We consider the product automaton $\mathcal{A}_s \times \mathcal{A}_t = (Q^s \times Q^t, A, E, (q_0^s, q_0^t), F)$ as defined in [Chou78], p. 83. We recall that in order to specify the set of transitions E we need the projection

$$\pi_{\mathcal{A}_s} : \bigcup_{0 \le k \le h} [Q^s \times Q^t]_k \to \bigcup_{0 \le k \le h} [Q^s]_k$$

defined recursively as follows. If $(q,p) \in [Q^s \times Q^t]_0$, then $\pi_{\mathcal{A}_s}(q,p) = q$. If $r \in [Q^s \times Q^t]_k$ with $k > 0$, then $\pi_{\mathcal{A}_s}(r) = \{\pi_{\mathcal{A}_s}(r') \mid r' \in r\}$. The projection $\pi_{\mathcal{A}_t} : \bigcup_{0 \le k \le h} [Q^s \times Q^t]_k \to \bigcup_{0 \le k \le h} [Q^t]_k$, $k > 0$, is defined similarly. Then E consists of the transitions $(r, a, (q,p))$ for which $(\pi_{\mathcal{A}_s}(r), a, q) \in E_{\mathcal{A}_s}$ and $(\pi_{\mathcal{A}_t}(r), a, p) \in E_{\mathcal{A}_t}$ holds. Finally, F consists of those subsets $r \in \bigcup_{0 \le k \le h} [Q^s \times Q^t]_k$ for which $f_s \in \pi_{\mathcal{A}_s}(r)$ and $f_t \in \pi_{\mathcal{A}_t}(r)$.

We note that the product of two simple Choueka automata is also a simple automaton.

Now, to determine whether two terms s, t denote the same word, we form the two automata $\mathcal{A}_s$ and $\mathcal{A}_t$ of size bounded by $h \times |Q^s|$ and $h \times |Q^t|$ respectively. Next consider the subautomaton $\mathcal{B}$ of the product automaton consisting of all the states which are accessible from the initial state. Because of the definition of the product automaton and because of equation (8), the size of $\mathcal{B}$ is bounded by $h \times |Q^s| \times |Q^t|$, i.e., it is bounded by the product of the sizes of the two automata. We need only check now whether $\mathcal{B}$ recognizes *any* word.

Proposition 8.3 *Given a simple Choueka automaton*

$$\mathcal{B} \quad = \quad (h, Q, S, q_0, E, f),$$

one can determine in $O(|S|^2)$ steps whether $\mathcal{B}$ recognizes any word.

Proof. We explain intuitively how we proceed. In the case of standard automata (i.e., on finite words), accessibility reduces to accessibility in the underlying graph, i.e., that graph whose vertices are the states and whose edges are obtained by forgetting the labels of the transitions. Similarly, the underlying graph of the Choueka automaton has edges which connect two states of height 0 together or a limit state and an ordinary state via the transition function. The "jumps" to limit states are not realized by edges. If we enrich the underlying graph with these additional edges then the accessibility problem in the automaton reduces to the accessibility problem in the enriched graph. We show that this enriched graph has a number of edges which is quadratic in the number of accessible states and that the construction of each additional edge requires constant time. The conclusion follows from the fact that the complexity of the graph reachability problem from a given vertex in a directed graph is linear in the number of edges of the graph.

In order to be more specific, consider a run of length $\alpha = \omega^h a_h + \omega^{h-1} a_{h-1} + \ldots \omega a_1 + a_0$ in the automaton, where the a_i's are nonnegative integers and $a_h > 0$. The run can be factored into a_h factors of length ω^h followed by a_{h-1} factors of length ω^{h-1}, ... Symbolically we represent the situation as follows where the p_j's belong to Q and the $q_k^{(i)}$'s belong to S_i and are the states visited by the different prefixes of the word (the arrows are labeled by the lengths of the factors, not the factors themselves; also we noted the type of the edges, as explained below).

$$\begin{aligned} & p_0 \xrightarrow[3]{\omega^h} q_1^{(h)} \ldots \xrightarrow[2]{\omega^h} q_{a_h}^{(h)} \xrightarrow[1]{1} p_1 \xrightarrow[3]{\omega^{h-1}} q_1^{(h-1)} \ldots \xrightarrow[2]{\omega^{h-1}} q_{a_{h-1}}^{(h-1)} \xrightarrow[1]{1} p_2 \\ & \xrightarrow[3]{\omega^{h-2}} \ldots \xrightarrow[2]{\omega^2} q_{a_2}^{(2)} \xrightarrow[1]{1} p_{h-1} \xrightarrow[3]{\omega} q_1^{(1)} \ldots \xrightarrow{\omega(2)} q_{a_1}^{(1)} \xrightarrow[1]{a_0} p_h \end{aligned} \tag{9}$$

(if α is not a successor ordinal, i.e., $a_0 = 0$, then the above run is modified accordingly by truncation). The arrows labeled by integers correspond to transitions in E.

The aim of the construction is to build a graph whose transitive closure connects all pairs of states p_0 and p_n as in (9). It should be clear that if this run is to be simulated by a path in a graph, then this graph requires three types of edges.

Type 1 edges:

$q \xrightarrow[1]{} q'$ if $q \in S, q' \in Q$ and there exists $a \in A$ with $(q, a, q') \in E$.

Type 2 edges:

$q \xrightarrow[2]{} q'$ if $q, q' \in S_k$ for some $0 < k \leq h$ and there exists a run of length ω^k that connects q and q'.

Type 3 edges:

$q \xrightarrow[3]{} q'$ if $q \in Q, q' \in S_k$ for some $0 < k \leq h$ and there exists a run of length ω^k that connects q and q'.

Actually, in order to more easily compute the edges of type 2 we will introduce the last type.

Type 4 edges:

$q \xrightarrow[4]{} q'$ if $q \in S_{k-1}, q' \in S_k$ for some $0 < k \leq h$ and there exists a run of length ω^k that connects q and q'.

The type 1 edges correspond to the transitions of the automaton and the construction is initialized with them.

Now the graph is constructed by induction on k, i.e., we assume that at stage k the four types of edges as above are constructed with $k-1$ in place of h and we show how to construct the graph involving the states up to height k. (The base of the induction with $k = 0$ is clear). At stage k we construct in that order, the type 4 then the type 3 finally the type 2 edges. These constructions require respectively, $|S_{k-1}|$, $|S_k|$ and $|S_0|$ edges. Each additional edge requires a constant number of operations. Indeed constructing the type 4 edges amounts to the following problem: given a mapping of a finite set X into itself, consider its graph and associate with every element $x \in X$ the set of all the vertices of the strongly connected component which is accesible from x. This can be done in time proportional to the number of elements. Now, computing a new edge of type 3, $q \to q'$, requires the traversal of the edge of type 3 (constructed at stage $k-1$) $q \to q''$ (of length ω^{k-1}) followed by the edge of type 4, $q'' \to q'$ (constructed at stage k). A new edge of type 2 requires the traversal of the type 1 edge $q \to q''$ (of length 1) followed by the edge of type 3 (of length ω^{k-1} constructed at stage at stage $k-1$) $q'' \to q'''$, followed by the edge of type 4 $q''' \to q'$ (constructed at stage k).

Summing up from $k = 0$ to $k = h$, the costs of all these operations, we find that the total cost is less than or equal to $h|S_0| + 2\sum_{0<k\leq h} |S_k|$. Because of equation (8) this quantity is in $O(S^2)$.

Once the graph is constructed, we are left with the accessibility problem from a given vertex which can be solved in linear time in the number of edges. This completes the proof.

$\square$

9 Acknowledgements

We thank Zoltán Ésik for the observation discussed in Section 7. Ralph Tindell made several very useful comments .

References

[BÉ95] S.L. Bloom and Z. Ésik. Nonfinite axiomatizability of shuffle inequalities. In *Proceedings of TAPSOFT '95*, volume 915 of *Lecture Notes in Computer Science*, pages 318–333, 1995.

[BÉ96] S.L. Bloom and Z. Ésik. Free shuffle algebras in language varieties. *Theoretical Computer Science*, 163:55–98, 1996.

[BÉ98] S.L. Bloom and Z. Ésik. Shuffle binoids. *Theoretical Informatics and Applications*, 32:175–198, 1998.

[ÉB95] Z. Ésik and L. Bernátsky. Scott induction and equational proofs, in: *Mathematical Foundations of Programming Semantics '95.* ENTCS, vol. 1, 1995.

[Chou78] S.C. Choueka. Finite automata, definable sets and regular expressions over ω^n-tapes. J. Comp. Sys. Sci., 17:81–97, 1978.

[CH98] C. Choffrut and S. Horvath. Equations in transfinite strings. in *Proceedings of Mathematical Foundations of Computer Science 1998.* L. Brim, J. Gruska, J. Zlatuška, eds. volume 1450 of *Lecture Notes in Computer Science*, pages 656–664, 1998.

[PP95] D. Perrin and J-E. Pin. Semigroups and automata on infinite words. in J. Fountain (ed.), Semigroups, Formal Languages and Groups, pages 49–72, Kluwer Academic Pub., 1995.

[Sier58] W. Sierpinski. *Cardinal and Ordinal Numbers.* Warsaw: PWN, 1958.

[Wil91] T. Wilke. An Eilenberg Theorem for ∞-languages. In "Automata, Languages and Programming", Proc. of 18th ICALP Conference, 510:588–599, 1991.

[Wil93] T. Wilke. An algebraic theory for regular languages of finite and infinite words. *International Journal of Algebra and Computation*, 3:447–489, 1993.