Theoretical Informatics and Applications
RAIRO: Theoret. Informatics Appl. **38** (2004) 3–17
DOI: 10.1051/ita:2004005

AXIOMATIZING OMEGA AND OMEGA-OP POWERS OF WORDS

Stephen L. Bloom[1,*] and Zoltán Ésik[2,†]

Abstract. In 1978, Courcelle asked for a complete set of axioms and rules for the equational theory of (discrete regular) words equipped with the operations of product, omega power and omega-op power. In this paper we find a simple set of equations and prove they are complete. Moreover, we show that the equational theory is decidable in polynomial time.

Mathematics Subject Classification. 06F99, 03B25.

1. Introduction

The theory of finite automata and regular languages on finite words has been generalized to various linear and nonlinear structures. In many cases, the study of such extensions was motivated by questions from formal logic. The linear structures studied include omega words [8], (countable) ordinal words [1,9,10,17], and, more recently, all (countable) words on scattered linear orders, in the terminology of [6,7,14], *cf.* [6,7], where there is a unified treatment.

Countable words[3], *i.e.*, finite or countably infinite labeled linear orders, were already studied by Courcelle in the 1970's. He singled out a subclass of countable words that we call regular words. These words arise as initial solutions of finite systems of recursion equations. Since each finite system of recursion equations unfolds to a system of regular trees, it follows that the regular words are exactly the frontiers of regular trees. This observation was made explicit by Thomas in [15]. He also gave a characterization of regular words in terms of formal logic.

---

[1] Department of Computer Science Stevens Institute of Technology Hoboken, NJ 07030; e-mail: bloom@cs.stevens-tech.edu
[*] *Partially supported by NSF grant 0119916.*
[2] Institute for Informatics University of Szeged 6720 Szeged, Hungary
[†] *Partially supported by BRICS, Aalborg, Denmark, NSF grant 0119916, and by grant No. T35163 of the National Foundation of Hungary for Scientific Research.*
[3] "Arrangements" in the terminology of [11].

He showed that a nonempty countable word, viewed as the isomorphism class of a labeled linear order, is regular iff it is a model of an $\aleph_0$-categorical sentence of a certain monadic second-order logic. In [5], the authors have shown that a countable word is regular iff it can be defined on an ordinary regular language (which can be chosen to be a prefix code) equipped with the lexicographical order such that the labeling function satisfies a regularity condition.

Courcelle defined the operations of product, omega power and omega-op power, and characterized the least class of words that can be generated from the letters of an alphabet by a property of (regular) trees. It was shown by Heilbrunner in [13] that a word belongs to this class iff it is a nonempty scattered regular word. An infinite collection of operations generating all regular nonempty words from single letters, including those having dense suborderings, was also described in [13].

In this paper, our concern is the equational theory of words equipped with the operations of product, omega power and omega-op power. Courcelle [11] asked for a complete set of axioms and rules for this theory. In this paper, we find such a system. The axioms are the identities given in Definition 3.6, and the rules are those of standard equational logic. Our methods also give a polynomial time decision algorithm. (That the equational theory is decidable follows from the result of Thomas [15] to the effect that the equality of the frontiers of regular trees is decidable. However, no elementary upper bound seems to be known for this more general problem.) Moreover, it follows that for any alphabet A, the algebra of discrete regular A-labeled nonempty words is freely generated by A in the variety axiomatized by the equations in Definition 3.6.

Our results extend those in [3] concerning the equational theory of just the operations of product and omega power. However, the arguments and methods used here are quite different. In particular, we have not used automata to achieve the polynomial complexity bound.

We use what might be called a "bottom up" method to prove the completeness theorem. Given a scattered word u, we show how to partition its underlying linear order L_u into blocks of an equivalence relation: two points $p < q$ are in the same block iff the interval $\{x \in L_u : p \leq x \leq q\}$ is finite. The blocks of L_u are also linearly ordered in the obvious way, and we denote this linearly ordered set by $\widehat{L}_u$. The blocks of scattered regular words are denoted by what we call the "primitive terms" below. It turns out that if two primitive terms s, t denote isomorphic words, then our axioms Ax are strong enough so that $\mathsf{Ax} \vdash s = t$. We then may choose a normal form for primitive terms. Now, we let $\widehat{u}$ denote the word on $\widehat{L}_u$, where a block is labeled by a new letter corresponding to the normal form for any primitive term denoting the block. In order to show that $\widehat{u}$ is also regular, we make use of "proper terms". Any scattered regular word on A is denoted by a term on A, built from letters in A using the operations of product, omega and omega-op power. We prove that every term is provably equal to a proper term. If t is a proper term, we show how to obtain a term $\widehat{t}$ and a substitution σ such that the word denoted by $\widehat{t}$ is $\widehat{u}$ and $\sigma(\widehat{t}) = t$. These preliminary results allow a quick proof of the completeness theorem, as seen below.

1.1. Notation

ω is the linearly ordered set of the nonnegative integers; ω^{op} is the linearly ordered set $\{\dots,-2,-1,0\}$.

2. Linear words

If $(L,\leq)$ is a linearly ordered set, and $p<q$ in L, we say q is **the successor** of p, and p is the predecessor of q, if there is no $r\in L$ with $p<r<q$.

A **linear word**, $(L_u,\leq,u,A)$ consists of a linearly ordered set $(L_u,\leq)$, an "alphabet" A and a "labeling function" $u: L_u\to A$. When the alphabet A is fixed, we say for short that u is a word *on* A, or (an "A-labeled word") *over* the linear order $(L_u,\leq)$. The linear order $(L_u,\leq)$ is the *underlying linear order* of u. When L_u is empty, we have the **empty word**, written $\mathbf{1}$, on A (for any set A). An **interval** of the linear order $(L,\leq)$ is a subset I of L such that if $p<q<r$ in L, and if $p,r\in I$, then $q\in I$. If u,v are words on A, we say v is a **subword** of u if L_v is an interval of L_u, and if, for any $p\in L_v$, $v(p)=u(p)$.

If u and v are words over A with underlying linear orders $(L_u,\leq)$ and $(L_v,\leq)$, respectively, a **morphism** $h: u\to v$ is an order preserving function $h: L_u\to L_v$ which preserves the labeling:

$$u(x)=v(h(x)),\quad x\in L_u.$$

Thus, for any set A, the collection of words on A forms a category. Two words u,v on A are **isomorphic** when they are isomorphic in this category, *i.e.*, when there are morphisms $h: u\to v,\ g: v\to u$ such that $u\xrightarrow{h}v\xrightarrow{g}u$ and $v\xrightarrow{g}u\xrightarrow{h}v$ are the respective identities. We write $u\cong v$ when u and v are isomorphic. We usually identify isomorphic words.

We equip the collection of all words on A with several operations. Suppose that $u=(L_u,\leq,u)$ and $v=(L_v,\leq,v)$ are words. The **product** $u\cdot v$ is the word over the sum L_u+L_v, *i.e.*, over the disjoint union of L_u and L_v ordered so that $x<y$, for every $x\in L_u,\ y\in L_v$; for pairs in L_u or L_v, the order is the original one. For $x\in L_u+L_v$,

$$(u\cdot v)(x)=\begin{cases}u(x) & \text{if } x\in L_u\\ v(x) & \text{if } x\in L_v.\end{cases}$$

The **omega power** of u, denoted u^ω, is the word whose underlying order is $L_u\times\omega$, ordered and labeled as follows:

$$\begin{aligned}(x,i)\leq(y,j) &\iff i<j \text{ or } (i=j \text{ and } x\leq y)\\ u^\omega(x,i) &= u(x).\end{aligned}$$

Similarly, the **omega-op power** $u^{\omega^{op}}$ of u is the word whose underlying order is $L_u \times \omega^{op}$, ordered and labeled as for u^ω, but now i, j range over the nonpositive integers.

In the latter sections, we will also be considering the **reverse** operation $u \mapsto u^r$. The underlying order of u^r is $(L_u, \geq)$, *i.e.*, the reverse of $(L_u, \leq)$. The labeling function of the reverse is the same as that of u.

Remark 2.1. The operations just defined make sense also for "partial words", *i.e.*, labeled partially ordered sets. For example, the underlying partial order of the product $u \cdot v$ is, as a set of pairs, $\leq_u \cup \leq_v \cup (L_u \times L_v)$, where $\leq_u$ is the set of ordered pairs $(x, y) \in L_u$ such that $x \leq y$; similarly for $\leq_v$.

Note. The subcollection of all words on A whose underlying linear order is finite or countably infinite is closed under the operations of product, omega and omega-op power. As mentioned in the introduction, in [13], the least collection of words on A which contains the singletons labeled $a \in A$, closed under product, omega and omega-op powers was shown to be the nonempty scattered regular words, *i.e.*, those nonempty scattered words isomorphic to the frontier of a binary regular tree. (A word is scattered [14] if there is no order embedding of the rationals into its underlying linear order.)

3. Terms

All of our algebras $(X, \cdot, ^\omega, ^{\omega^{op}})$ are enrichments of a semigroup $(X, \cdot)$ by two unary operations $x \mapsto x^\omega$, and $x \mapsto x^{\omega^{op}}$. The **basic models** are the algebras $(AW, \cdot, ^\omega, ^{\omega^{op}})$ of all finite and countable words on the alphabet A, enriched with the three indicated operations. For each such algebra, we let $(AR_s, \cdot, ^\omega, ^{\omega^{op}})$ denote the least subalgebra of AW containing the singletons, *i.e.*, the subalgebra of AW consisting of the scattered nonempty regular words.

Proposition 3.1. *Suppose that A and B are sets and* $\mathbf{B}$ *is any algebra of words on B equipped with the operations $\cdot, ^\omega, ^{\omega^{op}}$. Then any function $A \to B$ can be extended to a homomorphism $AW \to \mathbf{B}$.*

Proof. Given $h : A \to B$, for each word u in AW define $h^\sharp(u)$ as the word obtained by substituting a disjoint copy of $h(a)$ for each $x \in L_u$, where $u(x) = a$. It is a routine matter to show that $h^\sharp$ is a homomorphism. □

Definition 3.2. Let A be a fixed set.

(1) A **term on the alphabet** A is either a letter $a \in A$, or $t \cdot t'$, t^ω or $t^{\omega^{op}}$, where t, t' are terms on A.
(2) When t is a term on the alphabet A, we let $|t|$ denote the linear word on A denoted by t. More precisely, $|a|$ is a singleton set, labeled a. Using induction, we define

$$|t \cdot t'| := |t| \cdot |t'|$$
$$|t^\omega| := |t|^\omega$$
$$|t^{\omega^{op}}| := |t|^{\omega^{op}}.$$

(3) An equation $t = t'$ is **valid** if $|t| \cong |t'|$.
(4) The **height** of a term t, denoted $\mathsf{ht}(t)$, is the maximum number of nested $^\omega$ and $^{\omega^{op}}$ operations. Terms of height zero are called "finite terms". Those of positive height are "infinite terms".

We sometimes add a term **1** of height 0 denoting the empty word. When t is a term, $\mathbf{1} \cdot t$ and $t \cdot \mathbf{1}$ mean t; $\mathbf{1} \cdot \mathbf{1}$ means **1**.

As usual, each term on A induces a term function $X^A \to X$ over any algebra X equipped with the operations $\cdot, ^\omega, ^{\omega^{op}}$. For a term t, the word $|t|$ is just the value of the function induced by t over the algebra AW when each letter a is evaluated as the singleton word labeled a.

From Proposition 3.1 we immediately infer the following fact.

Proposition 3.3. *For any terms t, t' on A, $t = t'$ is valid iff $t = t'$ holds in all algebras of words under any evaluation of the letters in A, i.e., when $t = t'$ holds in the variety generated by all word algebras.*

Because we will always interpret the operation sign $\cdot$ as an associative operation, we allow ourselves to write terms such as $t_1 \cdot t_2 \cdots t_k$, for $k \geq 3$, with no parentheses.

Definition 3.4. We assume a nonempty "alphabet" A. A **primitive term** (on A) is either

(1) $a_1 \cdots a_k$, $a_i \in A$, $k \geq 1$ (a "finite" primitive term), or
(2) $a_1 \cdots a_k (b_1 \cdots b_m)^\omega$, $a_i, b_j \in A$, $k \geq 0, m \geq 1$ (a "right infinite" primitive term), or
(3) $(c_m \cdots c_1)^{\omega^{op}} a_k \cdots a_1$, $a_i, c_j \in A$, $k \geq 0, m \geq 1$ (a "left infinite" primitive term), or
(4) $(c_m \cdots c_1)^{\omega^{op}} a_k \cdots a_1 (b_1 \cdots b_n)^\omega$, $a_i, b_j, c_l \in A$, $k \geq 0$, $m, n \geq 1$ (a "bi-infinite" primitive term).

A **proper term** is either

- a primitive term, or
- a term of the form $t \cdot t'$ where t, t' are proper terms and $|t|$ has no greatest element or $|t'|$ has no least element, or
- a term of the form t^ω, or $t^{\omega^{op}}$, where t is a proper term and $|t|$ either has no least or no greatest element.

An **extended primitive term** is either **1** or a primitive term; an **extended proper term** is either **1** or a proper term.

Remark 3.5. If r, l are primitive terms such that $|r|$ has a greatest and $|l|$ has a least element, then $r \cdot l$ is primitive. Indeed, r must have the form 3.4.1 or 3.4.3, and l must have the form 3.4.1 or 3.4.2.

Definition 3.6 (The axioms)**.** Let Ax denote the following infinite set of equations between terms on the three-element set x, y, z.

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad (1)$$
$$(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega \quad (2)$$
$$(x \cdot y)^{\omega^{op}} = (y \cdot x)^{\omega^{op}} \cdot y \quad (3)$$
$$(x^n)^\omega = x^\omega, \quad n \geq 2 \quad (4)$$
$$(x^n)^{\omega^{op}} = x^{\omega^{op}}, \quad n \geq 2. \quad (5)$$

Remark 3.7. In [2], Bedon and Carton define semigroups equipped with an omega power operation satisfying (2) and (4). These semigroups are a one-sorted version of Wilke algebras[4] [16].

Proposition 3.8. *Each equation in* Ax *is valid.*

For terms t and t' on A, let us write $\mathsf{Ax} \vdash t = t'$ iff $t = t'$ is derivable from the equations in Ax by the rules of equational logic. (Note that in a derivation, axioms may be instantiated by terms on A.) It follows from Propositions 3.8 and 3.3 that any such equation is valid.

The following theorem is one of the main tools used to prove the completeness of the axioms.

Theorem 3.9. *For each finite term t on A there is a unique finite primitive term $a_1 \cdots a_k$ on A such that* $\mathsf{Ax} \vdash t = a_1 \cdots a_k$.

For each infinite term t on A there are extended primitive terms l, r and an extended proper term m on A such that:

- $\mathsf{Ax} \vdash t = l \cdot m \cdot r$;
- $|t|$ *has a least element iff* $l \neq \mathbf{1}$;
- $|t|$ *has a greatest element iff* $r \neq \mathbf{1}$;
- *if* $m \neq \mathbf{1}$, *either $|l|$ does not have a greatest element or $|m|$ has no least, and either $|m|$ has no greatest element or $|r|$ has no least; if $m = \mathbf{1}$, then either $|l|$ has no greatest or $|r|$ has no least;*
- $\mathsf{ht}(l \cdot m \cdot r) = \mathsf{ht}(t)$.

Thus, since $l \cdot m \cdot r$ is proper, for each term t there is a proper term t' with $\mathsf{ht}(t') = \mathsf{ht}(t)$ *and* $\mathsf{Ax} \vdash t = t'$.

Proof. The claim for finite terms is clear, using the associativity axiom.

Suppose now that t is an infinite term.

If $t = (a_1 \cdots a_k)^\omega$, we let $l = t$ and let $m = r = \mathbf{1}$; if $t = (a_k \cdots a_1)^{\omega^{op}}$, we let $l = m = \mathbf{1}$ and let $r = t$.

We continue by induction on the structure of t.

Suppose that $t = t_1 \cdot t_2$. If t_1 is finite, so that t_2 is infinite, let $l = a_1 \cdots a_k l_2$, $m = m_2$ and $r = r_2$, where $\mathsf{Ax} \vdash t_1 = a_1 \cdots a_k$ and $\mathsf{Ax} \vdash t_2 = l_2 \cdot m_2 \cdot r_2$, by the induction hypothesis. Similarly when t_2 is finite and t_1 is infinite.

[4]Wilke algebras are called "binoids" in [16].

Now assume $t = t_1 \cdot t_2$ and both t_1, t_2 are infinite terms. Then, let

$$\begin{aligned} l &= l_1 \\ m &= m_1 \cdot (r_1 l_2) \cdot m_2 \\ r &= r_2, \end{aligned}$$

where $\mathsf{Ax} \vdash t_i = l_i \cdot m_i \cdot r_i$, $i = 1, 2$, by the induction hypothesis. Note that we need not worry about the case when r_1 has a greatest and l_2 has a least element, by Remark 3.5. Also, $\mathsf{Ax} \vdash t = l \cdot m \cdot r$, by the associativity axiom (1).

If $t = (t_1)^\omega$, and t_1 is infinite with $\mathsf{Ax} \vdash t_1 = l_1 \cdot m_1 \cdot r_1$, we let

$$\begin{aligned} l &= l_1 \\ m &= (m_1 \cdot r_1 l_1)^\omega \\ r &= \mathbf{1}. \end{aligned}$$

$\mathsf{Ax} \vdash t = l \cdot m \cdot r$, by axiom (2).

If $t = (t_1)^{\omega^{op}}$ where t_1 is infinite with $\mathsf{Ax} \vdash t_1 = l_1 \cdot m_1 \cdot r_1$, we let

$$\begin{aligned} l &= \mathbf{1} \\ m &= (r_1 l_1 \cdot m_1)^{\omega^{op}} \\ r &= r_1. \end{aligned}$$

$\mathsf{Ax} \vdash t = l \cdot m \cdot r$ by axiom (3). This completes the proof. □

Proposition 3.10. *Suppose that t_1, t_2 are **primitive** terms on A. Then*

$$|t_1| \cong |t_2| \iff \mathsf{Ax} \vdash t_1 = t_2.$$

Proof. In fact, for each primitive term there is a normal form. The normal form of a finite term is itself. For a term of the form $a_1 \cdots a_k (b_1 \cdots b_m)^\omega$, we find the shortest word $b_1 \cdots b_i$ such that $b_1 \cdots b_m$ is a power of $b_1 \cdots b_i$, and then apply the rewriting rule $x(yx)^\omega \rightsquigarrow (xy)^\omega$ to $a_1 \cdots a_k (b_1 \cdots b_i)^\omega$ as many times as possible. Then $|t_1| \cong |t_2|$ iff t_1 and t_2 have the same normal form. The normal form of a left infinite primitive term is obtained in the same way. Note that the normal form of a finite, or left or right infinite primitive term is unique modulo associativity. As for bi-infinite primitive terms, a normal form is a term $(b_k \cdots b_1)^{\omega^{op}} a_1 \cdots a_m (c_1 \cdots c_n)^\omega$, where neither $b_k \cdots b_1$ nor $c_1 \ldots c_n$ is a nontrivial power of a word, moreover, if $m \neq 0$, then a_1 is different from b_k and a_m is different from c_n. However, the normal form may not be unique. In that case, $m = 0$ holds for all normal forms, and the normal forms are equivalent modulo the equation

$$(xy)^{\omega^{op}} (zy)^\omega = (yx)^{\omega^{op}} (yz)^\omega,$$

which is easily derivable from the axioms. □

Now fix the alphabet A. A **primitive word**[5] is either a finite word on A or a word on A whose underlying linear order is isomorphic to ω, ω^{op} or $\omega^{op} + \omega$, which is ultimately periodic (in both directions in the later case). Thus, the nonempty primitive words are those denoted by primitive terms. Thus, for a finite or countable alphabet A, there are only countably many primitive words on A.

Suppose that u is a linear word on A, with underlying order $(L_u, \leq)$, and suppose v is a subword of u, with underlying linear order $(L_v, \leq)$. We say v is **closed with respect to the successor relation** if whenever $x, y \in L$ and y is the successor in L_u of x, then $x \in L_v \iff y \in L_v$.

A *minimal successor closed subword* of a word u is a nonempty subword of u which is closed with respect to the successor relation and which does not contain any proper nonempty subword with the same property.

The minimal successor closed subwords of u are the blocks of the equivalence relation $\equiv$ on L_u:

$$\begin{aligned} p \equiv q \iff & \ p \leq q \text{ and } [p, q] \text{ is finite, or} \\ & \ q \leq p \text{ and } [q, p] \text{ is finite.} \end{aligned}$$

Here, $[p, q] = \{x : p \leq x \leq q\}$.

Proposition 3.11. *Any minimal successor closed subword of a word is either finite, or its underlying linear order is isomorphic to ω, ω^{op}, or $\omega^{op} + \omega$.*

Proposition 3.12. *For any term t on A, each minimal successor closed subword of $|t|$ is a primitive word.*

Proof. Clear, either from Theorem 3.9, or by a straightforward induction. □

Example 3.13. The word $abaaba^3b \ldots a^nb \ldots$ is a minimal successor closed word, but it is not primitive.

Definition 3.14 (The new alphabet B)**.** For each nonempty primitive word u on A, let b_u be a new letter in an alphabet B disjoint from the set of all terms on A.

Now, given a linear word u on A whose minimal successor closed subwords are primitive, let $\widehat{u}$ denote the linear word on B whose points are the minimal successor closed subwords of u, each labeled by the corresponding letter in B. The order in $\widehat{u}$ is inherited from u.

Proposition 3.15. *Suppose that u, v are A-labeled words whose minimal successor closed subwords are primitive. Then, $u \cong v$ iff $\widehat{u} \cong \widehat{v}$.*

Proof. If $\widehat{u} \cong \widehat{v}$, then clearly $u \cong v$.

Now let $\varphi : u \to v$ be an isomorphism. We define an isomorphism $\widehat{\varphi} : \widehat{u} \to \widehat{v}$, as follows. When M is a minimal successor closed subword of u, and $x \in M$, let $\widehat{\varphi}(M)$ denote the minimal successor closed subword of v containing $\varphi(x)$. □

[5]In the field of Combinatorics on Words, a "primitive word" is a finite nonempty word which is not a proper power. This is *not* the way we are using the term.

Lemma 3.16. *Let u_1 and u_2 be words whose minimal successor closed subwords are primitive.*

- *Suppose that u_1 has no greatest element or that u_2 has no least. Then*

$$\widehat{u_1 \cdot u_2} = \widehat{u}_1 \cdot \widehat{u}_2.$$

- *Suppose that $u \neq \mathbf{1}$ and u has no least or no greatest element. Then*

$$\widehat{u^\omega} = (\widehat{u})^\omega$$

and

$$\widehat{u^{\omega^{op}}} = (\widehat{u})^{\omega^{op}}.$$

Proof. For $u_1 \cdot u_2$: there exist no $x \in L_{u_1}$ and $y \in L_{u_2}$ such that in $u_1 \cdot u_2$, y is the successor of x. □

Let t_u be a primitive term on A such that $|t_u| = u$. Since by Proposition 3.10 all such primitive terms are equivalent with respect to the axioms, in the subsequent arguments we can fix the term t_u for each nonempty primitive word u. For example, we can take the lexicographically least. Let σ denote the unique term homomorphism mapping terms on B to terms on A such that

$$\sigma(b_u) = t_u$$

for each letter $b_u \in B$. Let σ also denote the substitution that maps a linear word on B to the corresponding word on A, so that for every term t on B,

$$|\sigma(t)| = \sigma(|t|).$$

Proposition 3.17. *For each proper term t on the alphabet A there is a term $\widehat{t}$ on the alphabet B such that $\sigma(\widehat{t}) = t$ and $\mathsf{ht}(\widehat{t}) < \mathsf{ht}(t)$ when t is infinite. Moreover, if $|t| = u$, then $|\widehat{t}| = \widehat{u}$.*

Proof. If t is primitive, then $\widehat{t}$ is a single letter, and $\sigma(\widehat{t}) = t$, by definition of σ. If $t = t_1 \cdot t_2$ is proper, then $\widehat{t} = \widehat{t}_1 \cdot \widehat{t}_2$, by the lemma. Since σ is a homomorphism, using induction, $\sigma(\widehat{t}) = t$. If $t = (t_1)^\omega$ or $(t_1)^{\omega^{op}}$, then $\widehat{t}$ is $(\widehat{t}_1)^\omega$ or $(\widehat{t}_1)^{\omega^{op}}$, respectively. Again $\sigma(\widehat{t}) = t$. □

As mentioned earlier, if $\mathsf{Ax} \vdash t = t'$, for terms t and t', then the equation $t = t'$ is valid. We now prove the converse.

Theorem 3.18. *The axioms are complete: any valid equation is derivable from* Ax.

Proof. Suppose that t_1, t_2 are terms on A such that $|t_1| \cong |t_2|$. We use induction on

$$h := \max\{\mathsf{ht}(t_1), \mathsf{ht}(t_2)\}$$

to show that $\mathsf{Ax} \vdash t_1 = t_2$. When $h = 0$, the only axiom needed is the associativity axiom. Now suppose that $h > 0$, so that both t_1, t_2 must be infinite terms. By Theorem 3.9, there are proper terms s_1, s_2 such that $\mathsf{Ax} \vdash t_i = s_i$, and $\mathsf{ht}(s_i) = \mathsf{ht}(t_i) \leq h$, $i = 1, 2$. Since $|s_1| \cong |s_2|$, also $|\widehat{s}_1| \cong |\widehat{s}_2|$, by Propositions 3.15 and 3.17. Now $\mathsf{ht}(\widehat{s}_i) < h$, $i = 1, 2$. By induction,

$$\mathsf{Ax} \vdash \widehat{s}_1 = \widehat{s}_2.$$

But, by Proposition 3.3, for any terms t, t', and any term morphism φ, if $\mathsf{Ax} \vdash t = t'$, then $\mathsf{Ax} \vdash \varphi(t) = \varphi(t')$. Thus, in particular,

$$\mathsf{Ax} \vdash \sigma(\widehat{s}_1) = \sigma(\widehat{s}_2),$$

i.e.,

$$\mathsf{Ax} \vdash s_1 = s_2,$$

and thus,

$$\mathsf{Ax} \vdash t_1 = t_2.$$ □

Corollary 3.19. *There is an $O(n^3)$ algorithm to decide if an equation $t = t'$ is valid, where n is the total number of symbols in the terms t, t'.*

Proof. Our recursive algorithm first converts the terms t and t' into proper terms, using the constructive proof of Theorem 3.9. During the conversion, the primitive subterms are brought into normal form and an ordered list of the encountered normal forms is maintained. (We assume a lexicographic order on the normal forms and that in case of ambiguity the lexicographically least normal form is selected.) This can be done in $O(n^2)$ time. If t and thus t' are finite, we just compare the two sides for syntactic equality. If $\mathsf{ht}(t), \mathsf{ht}(t') > 0$, then, in linear time, we compute the terms $\widehat{t}$ and $\widehat{t}'$ and repeat the procedure. Since h is at most n, and since the heights are reduced by one at each step, the algorithm terminates in $O(n^3)$ time. □

Corollary 3.20. *If $t = t'$ is valid, then $\mathsf{ht}(t) = \mathsf{ht}(t')$.*

Proof. The algorithm given in the proof of Corollary 3.19 reduces the heights of the terms by one in each step. Moreover, when $t = t'$ is valid, the algorithm terminates with height 0 terms. □

3.1. Adding reverse

In a more or less routine manner, we may now obtain an axiomatization of the equational theory of linear words enriched with the operations of product, omega and omega-op power and the reversal operation $t \mapsto t^r$. The axioms are (1, 2, 4) together with

$$(x^r)^r = x \tag{6}$$
$$(x \cdot y)^r = y^r \cdot x^r \tag{7}$$
$$(x^\omega)^r = (x^r)^{\omega^{op}}. \tag{8}$$

The axioms (3), and (5) are now redundant.

3.2. Adding **1**

We may add a constant term **1** to denote the empty word (on any alphabet), and then add the following axioms to those in Definition 3.6.

$$\begin{aligned} \mathbf{1} \cdot x = x &= x \cdot \mathbf{1} \\ (\mathbf{1})^\omega = (\mathbf{1})^{\omega^{op}} &= \mathbf{1} \\ \mathbf{1}^r &= \mathbf{1}. \end{aligned}$$

4. All axioms

For the reader's convenience, we list the totality of the axioms.

$$\begin{aligned} (x \cdot y) \cdot z &= x \cdot (y \cdot z) \\ (x \cdot y)^\omega &= x \cdot (y \cdot x)^\omega \\ (x \cdot y)^{\omega^{op}} &= (y \cdot x)^{\omega^{op}} \cdot y \\ (x^n)^\omega &= x^\omega, \quad n \geq 2 \\ (x^n)^{\omega^{op}} &= x^{\omega^{op}}, \quad n \geq 2 \\ (x^r)^r &= x \\ (x \cdot y)^r &= y^r \cdot x^r \\ (x^\omega)^r &= (x^r)^{\omega^{op}} \\ \mathbf{1} \cdot x = x &= x \cdot \mathbf{1} \\ (\mathbf{1})^\omega = (\mathbf{1})^{\omega^{op}} &= \mathbf{1} \\ \mathbf{1}^r &= \mathbf{1}. \end{aligned}$$

5. Free algebras

The first theorem follows immediately from the proof of the Completeness Theorem, Theorem 3.18.

Recall the definitions of the word algebras $(AW, \cdot, ^\omega, ^{\omega^{op}})$ and $(AR_s, \cdot, ^\omega, ^{\omega^{op}})$ above Proposition 3.1.

Theorem 5.1. *Let V be the variety of all models of* Ax *in Definition 3.6. For any set A, the algebra freely generated by A in V is the algebra $(AR_s, \cdot, ^\omega, ^{\omega^{op}})$ of scattered, regular, A-labeled nonempty words.*

For any alphabet C, we have defined the reverse u^r of a word in the word algebra CW as follows: the underlying order of u^r is $(L_u, \geq)$, the reverse of the underlying order $(L_u, \leq)$ of u, and the labeling of points in L_u is the same as that in u. The enrichment of the algebra $(CW, \cdot, ^\omega, ^{\omega^{op}})$ by this reverse operation is denoted CW also.

Now, fix a set A and choose a set $\overline{A}$ disjoint from A and a bijection $a \mapsto \overline{a}$ from $A \to \overline{A}$. We modify the reverse operation in $((A \cup \overline{A})R_s, \cdot, ^\omega, ^{\omega^{op}})$, the algebra of all regular, scattered $A \cup \overline{A}$-labeled linear orders.

$$a^r := \overline{a}$$
$$(\overline{a})^r := a.$$

On the other words in $(A \cup \overline{A})R_s$, we define

$$(u \cdot v)^r := v^r \cdot u^r$$
$$(u^\omega)^r := (u^r)^{\omega^{op}}$$
$$(u^{\omega^{op}})^r := (u^r)^\omega.$$

The last equation follows from the previous one and the fact that $(u^r)^r = u$.

Theorem 5.2. *Let V^r be the variety of all models $(X, \cdot, ^\omega, ^{\omega^{op}}, ^r)$ of the identities (1), (2), (4), (6), (7), and (8). For any set A, the algebra freely generated by A in V^r is $(A \cup \overline{A})R_s$, equipped with the above operations. By letting* **1** *denote the empty word in $(A \cup \overline{A})R_s$, we obtain the algebra freely generated by A in the variety of all models of the complete set of the identities in Section 4.*

6. Other models

Aside from the countable word algebras AW, we mention three other classes of models.

(1) Uncountable words: for any infinite cardinal $\aleph$, and any fixed set A, the collection of all words on A over linear orders of cardinality $\leq \aleph$ satisfies all of the axioms above, with the same definition of the operations.

(2) Partial words: as noted in Remark 2.1, the operations $u \cdot v, u^\omega, u^{\omega^{op}}, u^r$ are meaningful for labeled partially and not necessarily linearly ordered sets. Further, for any infinite cardinal $\aleph$, and any fixed set A, the collection of all A-labeled partially ordered sets of cardinality $\leq \aleph$ satisfies the axioms.

(3) Languages of words: for any set A and any infinite cardinal $\aleph$, the collection of all *languages* of words on A over linear (or partial) orders of cardinal $\leq \aleph$ satisfies the axioms; a language of words is, as usual, a subset of words, and the operations on subsets of words are defined as follows:

$$\begin{aligned}
U \cdot V &:= \{u \cdot v : u \in U,\ v \in V\} \\
U^\omega &:= \begin{cases} \{u_1 \cdot u_2 \ldots : u_i \in U\} & \text{if } \mathbf{1} \notin U \\ \{\mathbf{1}\} \cup (U - \{\mathbf{1}\})^\omega & \text{if } \mathbf{1} \in U \end{cases} \\
U^{\omega^{op}} &:= \begin{cases} \{\ldots u_2 \cdot u_1 : u_i \in U\} & \text{if } \mathbf{1} \notin U \\ \{\mathbf{1}\} \cup (U \ - \{\mathbf{1}\})^{\omega^{op}} & \text{if } \mathbf{1} \in U \end{cases} \\
U^r &:= \{u^r : u \in U\} \\
\mathbf{1} &:= \{\mathbf{1}\}.
\end{aligned}$$

Each of these three classes of models generates the same variety as do the countable words, since all free algebras are subalgebras of algebras in each class.

7. Finite axiomatizability

Using a slight modification of the analogous result in [3], we can show:

Theorem 7.1. *For any finite subset E of the axioms enumerated in Section 4, even the axioms involving the reverse operation ^{r} and the neutral element $\mathbf{1}$, there is some prime number p and an algebra M such that each equation in E is true in M, but the power identity $(x^p)^\omega = x^\omega$ fails in M.*

Thus, by the Compactness Theorem,

Corollary 7.2. *There is no finite axiomatization for any of the varieties considered above.*

Proof of Theorem 7.1. Let $M = \mathbb{N} \cup \{\mathbf{1}, \top, \bot\}$, the disjoint union of the nonnegative integers with a three element set. Let p be a prime. Define the operations $x \cdot y$ and x^ω on M as follows.

$$x \cdot y := \begin{cases} x + y & \text{if } x, y \in \mathbb{N} \\ x & \text{if } y = \mathbf{1} \\ y & \text{if } x = \mathbf{1} \\ \top & \text{if exactly one of } x, y \text{ is } \top \text{ and the other is in } \mathbb{N} \cup \{\mathbf{1}\} \\ \bot & \text{otherwise.} \end{cases}$$

$$x^\omega := \begin{cases} \mathbf{1} & \text{if } x = \mathbf{1} \\ \top & \text{if } x \in \mathbb{N} \text{ and } p|x \\ \bot & \text{otherwise.} \end{cases}$$

$$x^{\omega^{op}} := x^\omega.$$

$$x^r := x.$$

It is easy to check that $(M, \cdot, \mathbf{1})$ is a commutative monoid. Now we verify some of the axioms. We show that $(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega$. There are three possibilities.

If $(x \cdot y)^\omega = \mathbf{1}$, then $x = y = \mathbf{1}$, so that $x \cdot (y \cdot x)^\omega = \mathbf{1}$.

If $(x \cdot y)^\omega = \top$, then $x, y \in \mathbb{N}$ and $p|(x + y)$. But then $x \cdot (y \cdot x)^\omega = x \cdot \top = \top$. Otherwise, $(x \cdot y)^\omega = (y \cdot x)^\omega = \bot$ and $x \cdot \bot = \bot$.

Since the reverse operation is the identity function and since the omega power operations is the same as the omega-op power operation, equations (6) and (8) also hold in M. It follows now that (3) holds.

Last, if $n < p$, and $x \in \mathbb{N}$, then $x^n = nx$, so that $p|nx$ iff $p|x$. Thus, for $x \in \mathbb{N}$ and $n < p$, $(x^n)^\omega = x^\omega$; if $x \in \{\top, \bot\}$, $(x^n)^\omega = x^\omega = \bot$, for all $n \geq 1$. Thus, if p is a prime larger than all exponents k used in the identities $(x^k)^\omega = x^\omega$ and $(x^k)^{\omega^{op}} = x^{\omega^{op}}$ which occur in E, M is a model for E and the identities (1), (2), (3), and all of the reverse axioms and the axioms involving $\mathbf{1}$. However,

$$\begin{aligned} (1^p)^\omega &= p^\omega \\ &= \top \\ &\neq \bot \\ &= 1^\omega, \end{aligned}$$

so that the identity $(x^p)^\omega = x^\omega$ fails in M. □

8. Conjectures and open problems

The algebras of (countable) words, equipped with the operations of product and an initial fixed point operation, defined by Courcelle in [11], can be shown to form *iteration algebras* (or *iteration theories*) [4]. In fact, over all categories, initial fixed points lead to iteration theories, *cf.* Ésik and Labella [12]. We conjecture that the variety generated by algebras of words has a finite axiomatization over the variety of all iteration algebras. Thomas [15] has shown, using methods and results of formal logic, that the equational theory of this variety of iteration algebras is decidable. However, the methods applied in [15] do not provide an elementary upper bound, not even for the equational theory of product, omega power and omega-op power. It would be interesting to find upper and lower bounds.

References

[1] N. Bedon, Finite automata and ordinals. *Theoret. Comput. Sci.* **156** (1996) 119-144.

[2] N. Bedon and O. Carton, An Eilenberg theorem for words on countable ordinals, in *Latin'98: Theoretical Informatics,* edited by C.L. Lucchesi and A.V. Moura. *Lect. Notes Comput. Sci.* **1380** (1998) 53-64.

[3] S.L. Bloom and C. Choffrut, Long words: the theory of concatenation and ω-power. *Theoret. Comput. Sci.* **259** (2001) 533-548.

[4] S.L. Bloom and Z. Ésikn, *Iteration Theories.* Springer (1993).

[5] S.L. Bloom and Z. Ésik, Deciding whether the frontier of a regular tree is scattered. *Fundamenta Informaticae* **55** (2003) 1-21.

[6] V. Bruyère and O. Carton, Automata on linear orderings, in *Proc. Mathematical Foundations of Computer Science. Lect. Notes Comput. Sci.* **2136** (2001) 236-247.

[7] V. Bruyère and O. Carton, Hierarchy among automata on linear orderings, in *Foundation of Information Technology in the Era of Network and Mobile Computing, Proc. TCS 2002.* Kluwer Academic Publishers (2002) 107-118.

[8] J.R. Büchi, On a decision method in restricted second-order arithmetic, in *Int. Congress Logic, Methodology, and Philosophy of Science, Berkeley, 1960.* Stanford University Press (1962) 1-11.

[9] J.R. Büchi, Transfinite automata recursions and weak second order theory of ordinals, in *Int. Congress Logic, Methodology, and Philosophy of Science, Jerusalem, 1964.* North Holland (1965) 2-23.

[10] Y. Choueka, Finite automata, definable sets, and regular expressions over ω^n-tapes. *J. Comp. Syst. Sci.* **17** (1978) 81-97.

[11] B. Courcelle, Frontiers of infinite trees. *RAIRO: Theoret. Informatics Appl./Theor. Comput. Sci.* **12** (1978) 319-337.

[12] Z. Ésik and A. Labella, Equational properties of iteration in algebraically complete categories. *Theoret. Comput. Sci.* **195** (1998) 61-89.

[13] S. Heilbrunner, An algorithm for the solution of fixed-point equations for infinite words. *RAIRO: Theoret. Informatics Appl.* **14** (1980) 131-141.

[14] J.B. Rosenstein, *Linear Orderings.* Academic Press, New York (1982).

[15] W. Thomas, On frontiers of regular trees. *RAIRO: Theoret. Informatics Appl.* **20** (1986) 371-381.

[16] Th. Wilke, An algebraic theory for regular languages of finite and infinite words. *Int. J. Algebra Comput.* **3** (1993) 447-489.

[17] J. Wojciechowski, Finite automata on transfinite sequences and regular expressions. *Fundamenta Informaticae* **8** (1985) 379-396.

Communicated by C. Choffrut.
Received January 5, 2003. Accepted October 10, 2003.