Nonfinite Axiomatizability of the Equational Theory of Shuffle

Zoltán Ésik*
A. József University
Department of Computer Science
Szeged, Hungary
esik@inf.u-szeged.hu

Michael Bertol †
University of Stuttgart
Department of Computer Science
Stuttgart, Germany
bertol@informatik.uni-stuttgart.de

Abstract

We consider language structures $\mathbf{L}_\Sigma = (P_\Sigma, \cdot, \otimes, +, 1, 0)$, where P_Σ consists of all subsets of the free monoid Σ^*; the binary operations $\cdot$, $\otimes$ and $+$ are concatenation, shuffle product and union, respectively, and where the constant 0 is the empty set and the constant 1 is the singleton set containing the empty word. We show that the variety **Lang** generated by the structures $\mathbf{L}_\Sigma$ has no finite axiomatization. In fact we establish a stronger result: The variety **Lang** has no finite axiomatization over the variety of ordered algebras $\mathbf{Lg}_\leq$ generated by the structures $(P_\Sigma, \cdot, \otimes, 1, \subseteq)$, where $\subseteq$ denotes set inclusion. (The nonfinite axiomatizability of $\mathbf{Lg}_\leq$ has been shown recently, cf. [7].)

1 Introduction

In the interleaving or language model of concurrency, the parallel composition of two processes is given by the shuffle product, which also plays an important role in language theory. One would like to have a complete axiomatization of the equational properties of shuffle in conjunction with other operations of interest. In this paper, we consider language structures $\mathbf{L}_\Sigma = (P_\Sigma, \cdot, \otimes, +, 1, 0)$, where P_Σ consists of all subsets of the free monoid Σ^*; the binary operations $\cdot$, $\otimes$ and $+$ are concatenation, shuffle product and union, respectively, and where the constant 0 is the empty set and the constant 1 is the singleton set containing the empty word. We show that the variety **Lang** generated by the structures $\mathbf{L}_\Sigma$ has no finite axiomatization. Thus the equational properties of the shuffle product, in conjunction with the other operations and constants, cannot be captured by a finite number of axioms. In fact we establish the stronger result that **Lang** has no finite axiomatization over the variety of ordered algebras $\mathbf{Lg}_\leq$ generated by the structures $(P_\Sigma, \cdot, \otimes, 1, \subseteq)$, where $\subseteq$ is set inclusion. The fact that $\mathbf{Lg}_\leq$ has no finite axiomatization has been shown very recently, cf. [7]. (This is in contrast with the fact that **Lg**, the variety generated by the reducts $(P_\Sigma, \cdot, \otimes, 1)$, does have a complete axiomatization consisting of a small finite set of simple equational axioms, cf. [6].) Nevertheless the results obtained in [7] are completely independent of those given here, and the present paper contains significant new ideas. For completeness, we also consider the enrichment with the Kleene star and iterated shuffle operations.

*Supported by a grant of the National Foundation for Scientific Research of Hungary and by a fellowship of the Alexander von Humboldt Foundation.

†This research has been supported by the ESPRIT Basic Research Actions No. 6317 ASMICS II.

In our proofs, we make use of the concrete descriptions from [6] of the free algebras in the above varieties. The free algebras in the variety **Lg** are the series-parallel posets. The same series-parallel posets, equipped with the trace ordering, are the free algebras in the variety $\mathbf{Lg}_{\leq}$ of ordered algebras. (The trace ordering is not the same as the subsumption order studied in [12].) Finally, "closed subsets" of series-parallel posets are the free algebras in the variety **Lang**. On the basis of these facts, it is said in [7]: "These results seem to show that two different models of parallelism are equivalent: the so called language or interleaving model and the pomset model, cf. [17]".

2 Basic notions

We assume familiarity with universal algebra. For varieties of ordered algebras the reader is referred to [4].

2.1 Bimonoids

Definition 2.1 *A* **bimonoid** $M = (M, \cdot, \otimes, 1)$ *consists of a monoid* $(M, \cdot, 1)$ *and a commutative monoid* $(M, \otimes, 1)$*. A* **bimonoid morphism** $M \to M'$ *is a function* $h : M \to M'$ *which preserves the unit and the two binary operations.*

The only connection between the two monoids in a bimonoid is the common neutral element 1.

Definition 2.2 *An* **ordered bimonoid** $(M, \leq)$ *is a bimonoid* M *which is equipped with a partial ordering* $\leq$ *such that for all* $x, y, a, b \in M$*,*

$$x \leq a,\ y \leq b \implies x \cdot y \leq a \cdot b \text{ and } x \otimes y \leq a \otimes b.$$

A **morphism of ordered bimonoids** *is an order preserving bimonoid morphism.*

The following structures are examples of bimonoids: $\mathcal{L}_\Sigma := (P_\Sigma, \cdot, \otimes, 1)$, $\mathcal{R}_\Sigma := (R_\Sigma, \cdot, \otimes, 1)$, and $\mathcal{F}_\Sigma := (F_\Sigma, \cdot, \otimes, 1)$. Here P_Σ is the collection of all subsets of the free monoid Σ^*. R_Σ consists of the regular subsets, and F_Σ is the set of the finite subsets. The operation $B \cdot C$ is (complex) concatenation and $B \otimes C$ is the shuffle product of the languages B and C:

$$B \otimes C \quad := \quad \{u_1 v_1 \cdots u_n v_n \mid\ u_1 \cdots u_n \in B,\ v_1 \cdots v_n \in C, u_i, v_i \in \Sigma^*, n \geq 0\}.$$

The constant 1 is the set consisting of the empty word. Equipped with the partial order given by set inclusion, each of the bimonoids $\mathcal{L}_\Sigma$, $\mathcal{R}_\Sigma$ and $\mathcal{F}_\Sigma$ is an ordered bimonoid.

2.2 Shuffle semirings

Definition 2.3 *A* **shuffle semiring** $(S, +, \cdot, \otimes, 0, 1)$ *is a bimonoid* $(S, \cdot, \otimes, 1)$ *enriched with a constant* 0 *and a commutative, associative, idempotent addition operation* $+$*, such that*

$$\begin{aligned} x + 0 &= x \\ x \cdot 0 &= 0 = 0 \cdot x \\ x \otimes 0 &= 0 \\ x \cdot (y + z) &= (x \cdot y) + (x \cdot z) \\ (y + z) \cdot x &= (y \cdot x) + (z \cdot x) \\ x \otimes (y + z) &= (x \otimes y) + (x \otimes z), \end{aligned}$$

for all $x, y, z \in S$. A **morphism of shuffle semirings** *is a function which preserves* $0, 1$ *and the three binary operations* $+, \cdot, \otimes$.

Below, when writing expressions involving the operations $+$, $\cdot$ and $\otimes$, we will assume that $\cdot$ binds more closely than $\otimes$ which in turn binds more closely than $+$.

Notation. The class of all shuffle semirings is denoted $\mathbf{S}$.

The structures $\mathbf{L}_\Sigma := (P_\Sigma, +, \cdot, \otimes, 0, 1)$, $\mathbf{R}_\Sigma := (R_\Sigma, +, \cdot, \otimes, 0, 1)$, and $\mathbf{F}_\Sigma := (F_\Sigma, +, \cdot, \otimes, 0, 1)$ are shuffle semirings where the addition operation in each is given by set union and 0 is the empty set. The other operations and constants were defined above.

Suppose that S is a shuffle semiring. We define a partial order on S by

$$a \leq b \iff a + b = b \iff \exists c\ a + c = b.$$

The operations of S are monotonic with respect to the induced partial order $\leq$. Moreover, every shuffle semiring morphism is monotonic. Thus the reduct $(S, \cdot, \otimes, 1, \leq)$ is an ordered bimonoid. In the structures $\mathbf{L}_\Sigma$, the partial order $\leq$ determined by the additive structure is set inclusion.

2.3 Terms

A shuffle semiring term is a well-formed expression built in the usual way from the operation symbols $\cdot$, $\otimes$, $+$, constants 0, 1, and variables x_i from a countable set. A bimonoid term is a shuffle semiring term not containing the symbols $+$ and 0. The set of variables which actually occur in the term t is denoted $var(t)$. Sometimes we write $t(x_1, \ldots, x_n)$ to indicate that $var(t) \subseteq \{x_1, \ldots, x_n\}$. When S is a shuffle semiring (bimonoid) and $t = t(x_1, \ldots, x_n)$ is a shuffle semiring term (bimonoid term), and if $a_1, \ldots, a_n \in S$, we write $t_S(a_1, \ldots, a_n)$ or just $t(a_1, \ldots, a_n)$ for the value of the term function induced by t in S on the arguments $a_1, \ldots, a_n$. We will consider equations $t = t'$ and inequations $t \leq t'$ between terms t and t'. A class $\mathcal{V}$ of shuffle semirings is a variety if there exists a set E of equations between shuffle semiring terms such that $\mathcal{V}$ is the class of all models of E:

$$\mathcal{V} \quad = \quad \{S \mid S \models E\}.$$

Each inequation $t \leq t'$ between shuffle semiring terms can be considered as an abbreviation for the equation $t + t' = t'$.

A class $\mathcal{B}$ of bimonoids (ordered bimonoids) is a variety if there is a set E of equations (inequations) between bimonoid terms such that $\mathcal{B}$ is the class of all models of E.

3 Results

We define the following varieties:

$$\begin{array}{rcl}
\mathbf{Lg} & := & \text{the variety of bimonoids generated by the language structures } \mathcal{L}_\Sigma. \\
\mathbf{Lg}_\leq & := & \text{the variety of ordered bimonoids generated by the ordered structures } (\mathcal{L}_\Sigma, \subseteq). \\
\mathbf{Lang} & := & \text{the variety of shuffle semirings generated by the language structures } \mathbf{L}_\Sigma.
\end{array}$$

We note that $\mathbf{Lg}$ is also generated by the bimonoids $\mathcal{R}_\Sigma$ or $\mathcal{F}_\Sigma$, and that $\mathbf{Lg}_\leq$ is generated by the ordered bimonoids $(\mathcal{R}_\Sigma, \subseteq)$ or $(\mathcal{F}_\Sigma, \subseteq)$. Further, the variety $\mathbf{Lang}$ is generated by the shuffle semirings $\mathbf{R}_\Sigma$ or $\mathbf{F}_\Sigma$. It was shown in [6] that the (in)equational theory of each of the above varieties is decidable, see also [11, 16]. Our main result is the following theorem.

Theorem 3.1 *The variety* **Lang** *has no finite (equational) axiomatization relative to all valid inequations of* $\mathbf{Lg}_{\leq}$.

Corollary 3.2 *The variety* **Lang** *is not finitely axiomatizable.*

Note that an inequation $t \leq t'$ between bimonoid terms is valid in $\mathbf{Lg}_{\leq}$ if and only if it is valid in **Lang**, in notation: $\mathbf{Lg}_{\leq} \models t \leq t' \iff \mathbf{Lang} \models t \leq t'$.

The essence of Theorem 3.1 is that there exists no finite set E of shuffle semiring equations that together with all valid inequations of the variety $\mathbf{Lg}_{\leq}$ is a complete axiomatization of **Lang**. (Recall that each inequation between bimonoid terms can be considered as an equation.)

It is shown in [7] that $\mathbf{Lg}_{\leq}$ is not finitely axiomatizable. This result and Corollary 3.2 are independent, none of them implies the other (see also Problem 4 in Section 8). On the other hand, **Lg** has a finite axiomatization, for **Lg** is the class of all bimonoids, cf. [6] and Section 4.

The rest of the paper is organized as follows. In Section 4 we review from [6] the concrete descriptions of the free algebras in the varieties **Lg**, $\mathbf{Lg}_{\leq}$ and **Lang**. The description uses labeled posets and is utilized in the proof of the Theorem 3.1. In Section 5, we state a general metatheorem which also provides an outline of the proof of Theorem 3.1, which is in turn completed in Section 6 by giving a concrete construction. A stronger form of Theorem 3.1 and some further results are stated in Section 7. Several open problems are given in Section 8. Detailed proofs are given in the Appendices.

4 Review

A concrete description of the free algebras in the varieties **Lg**, $\mathbf{Lg}_{\leq}$ and **Lang** was obtained in [6]. The description uses labeled posets.

Suppose that A is a set. An A**-labeled poset** $P = (P, \leq, \ell)$ consists of a finite poset $(P, \leq_P)$, usually written just $(P, \leq)$, and a function $\ell : V \to A$ mapping vertices in V to labels in A. Below we will usually say labeled poset, or just poset, in particular when A is understood. A morphism $f : P \to Q$ of labeled posets is a function $P \to Q$ which preserves the ordering and the labeling. We identify isomorphic posets. The operations of sequential or serial product $P \cdot Q$ and parallel or shuffle product $P \otimes Q$ are defined as follows:

$$\begin{aligned} P \cdot Q &:= (P \cup Q, \leq_{P \cdot Q}) \\ P \otimes Q &:= (P \cup Q, \leq_{P \otimes Q}), \end{aligned}$$

where the two sets P and Q are disjoint, and for $v, v' \in P \cup Q$,

$$\begin{aligned} v \leq_{P \cdot Q} v' &\iff v \leq_P v' \text{ or } v \leq_Q v' \text{ or} \\ &\qquad\; v \in P \text{ and } v' \in Q. \\ v \leq_{P \otimes Q} v' &\iff v \leq_P v' \text{ or } v \leq_Q v'. \end{aligned}$$

The labeling is the obvious extension of the labelings of P and Q. Labeled posets with the above operations were introduced by Pratt to model concurrent behavior of processes, cf. [17].

Definition 4.1 *An A-labeled poset is called* **series-parallel** *if it is in the least class of posets containing the empty poset* 1*, the singleton posets* a*, labeled* a*, for each* $a \in A$*, closed under the operations of sequential and parallel product. We let* $\mathbf{SP}(A)$ *denote the collection of all A-labeled series-parallel posets.*

Both $\mathbf{SP}(A)$ and the collection $\mathbf{Pos}(A)$ of all A-labeled posets are bimonoids with the operations sequential and parallel product and the constant 1.

Remark 4.2 A graph theoretic characterization of the series-parallel posets was found in Grabowski [13] and Valdes et al. [21]. A poset P is series-parallel if it does not have an induced subposet consisting of four vertices a, b, c, d whose only nontrivial order relations are given by

$$a < c, \quad a < d, \quad b < d.$$

Thus any subset of a series-parallel poset, equipped with the induced partial order, is series-parallel. This fact will be used several times without mention.

We identify each letter $a \in A$ with the singleton poset whose vertex is labeled a.

Theorem 4.3 [12] $\mathbf{SP}(A)$ *is freely generated by the set A in the variety of all bimonoids.*

Thus the variety of bimonoids is generated by both the bimonoids $\mathbf{SP}(A)$ and the bimonoids $\mathbf{Pos}(A)$.

Let $\overline{A}$ be a disjoint copy of A and suppose that the map $a \mapsto \overline{a}$ is a bijection $A \to \overline{A}$. We define

$$\Sigma(A) \quad := \quad \{a_i, \bar{a}_i \mid a \in A,\ i = 1, 2, \ldots\}.$$

The letters a_i are called open, and the letters $\overline{a}_i$ are closed. Open and closed letters have been used in several papers about action refinement, see e.g. [1, 2] and the references contained therein.

Let $h_0 : \mathbf{SP}(A) \to \mathcal{L}_{\Sigma(A)}$ be the unique bimonoid morphism determined by the map

$$h_0 : a \quad \longmapsto \quad \{a_1\bar{a}_1, a_2\overline{a}_2 \ldots, a_n\bar{a}_n, \ldots\}.$$

Theorem 4.4 [6] *The morphism h_0 is injective. It follows that* $\mathbf{Lg}$ *is the variety of* all *bimonoids.*

The words in Ph_0 satisfy, for $P \in \mathbf{SP}(A)$, the following conditions:

(i) $|u|_{a_i} = |u|_{\overline{a}_i}$, for each $a \in A$. ($|u|_{a_i}$ is the number of occurrences of the letter a_i in the word u.)

(ii) If w is a prefix of u, $|w|_{a_i} \geq |w|_{\overline{a}_i}$, for each $a_i \in \Sigma(A)$.

Definition 4.5 *A monoid endomorphism φ of $(A_N \cup \overline{A}_N)^*$ is* **admissible** *if, for each $a \in A$, $i > 0$, there is some $j > 0$ with $a_i\varphi = a_j$, and $\overline{a}_i\varphi = \overline{a}_j$.*

Definition 4.6 *The preorder $\sqsubseteq$ on the set $\Sigma(A)^*$ is the least reflexive and transitive relation which satisfies the following conditions. $u \sqsubseteq u'$ if, for some words w, w' and distinct letters $a_i, b_j \in \Sigma(A)$,*

$$\begin{array}{ll} u = wa_ib_jw' \quad \textit{and} \quad u' = wb_ja_iw'; & \textit{or} \\ u = w\overline{a}_i\overline{b}_jw' \quad \textit{and} \quad u' = w\overline{b}_j\overline{a}_iw'; & \textit{or} \\ u = w\overline{a}_ib_jw' \quad \textit{and} \quad u' = wb_j\overline{a}_iw'; & \textit{or} \\ u = u'\varphi, \quad \textit{for some admissible } \varphi. & \end{array}$$

For each $P \in \mathbf{SP}(A)$, the set Ph_0 is closed with respect to the preorder $\sqsubseteq$, i.e., if $u \in Ph_0$ and $v \sqsubseteq u$, then $v \in Ph_0$. Thus for each word $v \in Ph_0$ there is a maximal word $u \in Ph_0$ with $v \sqsubseteq u$. Of course, a word $u \in Ph_0$ is maximal if $u' \sqsubseteq u$ for all $u' \in Ph_0$ with $u \sqsubseteq u'$. Each letter occurs at most once in any maximal word.

Definition 4.7 *For A-labeled posets P, Q in $\mathbf{SP}(A)$, $P \leq Q$ iff for each word $u \in Ph_0$ there is a word $u' \in Qh_0$ with $u \sqsubseteq u'$. We call the order $\leq$ the* **trace ordering** *on $\mathbf{SP}(A)$.*

We note some easy consequences of Definition 4.7.

(i) For posets $P, Q \in \mathbf{SP}(A)$, $P \leq Q$ iff one of the following conditions holds:

- (a) $Ph_0 \subseteq Qh_0$.
- (b) Each maximal word in Ph_0 is in Qh_0.
- (c) For each maximal word u in Ph_0 there is a (maximal) word $v \in Qh_0$ with $u \sqsubseteq v$.

(ii) $(\mathbf{SP}(A), \leq)$ is an ordered bimonoid in $\mathbf{Lg}_{\leq}$.

Suppose that P is a nonempty poset in $\mathbf{SP}(A)$. We describe in brief how to construct the maximal words in Ph_0. First, replace each vertex v of P labeled a by the two-element chain $v < \overline{v}$ with v labeled a_i and $\overline{v}$ labeled $\overline{a}_i$, for some integer i, but such that each letter of $\Sigma(A)$ is used at most once. Vertex v is called an open vertex, and $\overline{v}$ is a closed vertex. Let P' denote the resulting series-parallel $\Sigma(A)$-labeled poset. A linearization of P' can be represented by a word $w = x_1 \ldots x_{2n}$ composed of the vertices x_i of P'. We can rewrite the word w as $w = s_0 p_1 \ldots s_{k-1} p_k$, where each s_i is a nonempty word formed of open vertices and each p_j is a nonempty word of closed vertices. Call the linearization w maximal if whenever the open vertex v is listed in s_i and the closed vertex $\overline{u}$ is an immediate predecessor of v, then $\overline{u}$ is listed in the word p_i. Thus s_0 is a word listing all the minimal (open) vertices, and p_k is a word listing all the maximal (closed) vertices of P'. Each maximal word in Ph_0 is the label sequence corresponding to a maximal linearization of P'.

Example. Let $P = a \cdot (b \otimes c) \otimes (a \otimes a) \cdot d$. Then, up to admissible isomorphism and commutations between open or closed letters, there are two maximal words in Ph_0:

$$\begin{aligned} u_1 &= a_1 a_2 a_3 \overline{a}_1 b_1 c_1 \overline{a}_2 \overline{a}_3 d_1 \overline{b}_1 \overline{c}_1 \overline{d}_1 \\ u_2 &= a_1 a_2 a_3 \overline{a}_1 \overline{a}_2 d_1 \overline{a}_3 b_1 c_1 \overline{b}_1 \overline{c}_1 \overline{d}_1 . \end{aligned}$$

Let $Q = a \cdot (a \otimes a) \otimes (a \otimes a) \cdot a$. Then, up to admissible isomorphism, there is a unique maximal word in Qh_0:

$$u_1 = a_1 a_2 a_3 \overline{a}_1 a_4 a_5 \overline{a}_2 \overline{a}_3 a_6 \overline{a}_4 \overline{a}_5 \overline{a}_6 .$$

Theorem 4.8 [6] *For each set A, $(\mathbf{SP}(A), \leq)$ is the free ordered bimonoid generated by A in the variety of ordered bimonoids $\mathbf{Lg}_{\leq}$.*

We end this section by recalling from [6] the concrete description of the free shuffle semirings in the variety **Lang**.

Definition 4.9 *A subset B of $\mathbf{SP}(A)$ is closed if for all $P \in \mathbf{SP}(A)$, $Ph_0 \subseteq Bh_0$ implies $P \in B$.*

In the above definition, Bh_0 denotes the union of the sets Qh_0 for Q in B. Note that Bh_0 is closed for the preorder $\sqsubseteq$.

We list some easy consequences of the definition.

(i) The empty set $\emptyset$ is closed.

(ii) If B_j, $j \in J$, are closed, then so is the intersection $\cap_{j\in J} B_j$. Thus each set $B \subseteq \mathbf{SP}(A)$ is contained in a least closed set, denoted $cl(B)$.

(iii) Each closed set is an ideal; i.e., if B is closed and $P \leq Q$ and $Q \in B$, then $P \in B$.

(iv) Each principal (i.e. one-generated) ideal $(P] = \{Q \mid Q \leq P\}$ in $\mathbf{SP}(A)$ is closed. In particular, the ideal $(a] = \{a\}$ is a closed set, for each $a \in A$.

(v) If $B = cl(B_0)$ and $C = cl(C_0)$, then the inclusion $B \subseteq C$ is equivalent to either one of the following conditions:

  (a) $Bh_0 \subseteq C_0h_0$, i.e., $Ph_0 \subseteq C_0h_0$, for each $P \in B_0$.

  (b) Each word which is maximal in B_0h_0 is in C_0h_0.

  (c) For each (maximal) word $u \in B_0h_0$ there is a (maximal) word $v \in C_0h_0$ with $u \sqsubseteq v$.

(vi) If $P, Q \in \mathbf{SP}(A)$, then $P \leq Q$ iff $(P] \subseteq (Q]$.

Definition 4.10 *Let $\mathbf{I}_\omega(A)$ denote the set of all finite closed subsets of $\mathbf{SP}(A)$:*

$$\mathbf{I}_\omega(A) \quad := \quad \{cl(B_0) \mid B_0 \subseteq \mathbf{SP}(A),\ B_0 \textit{ finite}\}.$$

Remark 4.11 Note that a closed subset of $\mathbf{SP}(A)$ is finite iff it is finitely generated, since the closure of a finite set is finite.

Definition 4.12 *Suppose that $B, C \in \mathbf{I}_\omega(A)$. Then we define:*

$$\begin{aligned} B + C &:= cl(B \cup C) \\ B \cdot C &:= cl(\{P \cdot Q \mid P \in B,\ Q \in C\}) \\ B \otimes C &:= cl(\{P \otimes Q \mid P \in B,\ Q \in C\}) \\ 0 &:= \emptyset \\ 1 &:= cl(\{1\}) \ = \ \{1\}. \end{aligned}$$

If $B, C \in \mathbf{I}_\omega(A)$ then $B + C$, $B \cdot C$, $B \otimes C$ are in $\mathbf{I}_\omega(A)$. If $B = cl(B_0)$ and $C = cl(C_0)$, with B_0 and C_0 finite, then

$$\begin{aligned} B + C &= cl(B_0 \cup C_0) \\ B \cdot C &= cl(\{P \cdot Q \mid P \in B_0,\ Q \in C_0\}) \\ B \otimes C &= cl(\{P \otimes Q \mid P \in B_0,\ Q \in C_0\}). \end{aligned}$$

Equipped with the above operations and constants, $\mathbf{I}_\omega(A)$ is a shuffle semiring in which the partial order determined by the additive structure is set inclusion. The principal ideals $(P]$, for $P \in \mathbf{SP}(A)$ determine an ordered sub bimonoid of $\mathbf{I}_\omega(A)$ isomorphic to $\mathbf{SP}(A)$.

We identify each letter $a \in A$ with the principal ideal $(a] = \{a\}$.

Theorem 4.13 [6] *The shuffle semiring* $\mathbf{I}_\omega(A)$ *is freely generated by* A *in* **Lang**.

For later use, we note several properties of closed sets.

Lemma 4.14 *Suppose that* $P \in \mathbf{SP}(A)$ *and* $X \subseteq \mathbf{SP}(A)$. *If* $P \in cl(X)$ *then there exists a poset* $Q \in X$ *with the following properties:*

(i) For each $a \in A$, *the number of vertices of* P *labeled* a, $|P|_a$, *is the same as* $|Q|_a$. *Thus the number of vertices of* P, $|P|$, *is the same as* $|Q|$.

(ii) For each $a \in A$, *the number of minimal (maximal) vertices of* P *labeled* a *is at most the number of minimal (maximal) vertices of* Q *labeled* a.

(iii) The height of P *is at least the height of* Q.

(iv) The number of isolated vertices of P *is at most the number of isolated vertices of* Q.

5 The metatheorem

In this section A denotes a nonempty set. By a closed ideal we mean a finite closed set in $\mathbf{I}_\omega(A)$. When t is a shuffle semiring term, the total number of occurrences of variables in t is denoted $|t|$.

Theorem 5.1 *Suppose that for each* $n \geq 1$ *we are given a poset* $P_n \in \mathbf{SP}(A)$ *and a closed ideal* $I_n = cl(X_n) \in \mathbf{I}_\omega(A)$ *with the following properties.*

(P1) $|P_n| = |P| > n$, *for all* $P \in I_n$.

(P2) $(P_n] \subset I_n$ *and* $P_n \notin X_n$.

(P3) For all $X \subseteq \mathbf{SP}(A)$, *if* $(P_n] \subseteq cl(X) \subset I_n$ *then* $P_n \in X$.

(P4) I_n *has no nontrivial sequential or parallel decomposition, i.e., if* $I_n = I \cdot J$ *or* $I_n = I \otimes J$, *for some* $I, J \in \mathbf{I}_\omega(A)$, *then* $I = 1$ *or* $J = 1$.

(P5) If t *is a bimonoid term and* t' *is a shuffle semiring term with* $\mathrm{var}(t) = \mathrm{var}(t') = \{x_1, \ldots, x_k\}$, *and if*

$$(P_n] \quad \subseteq \quad t(J_1, \ldots, J_k) \quad \subset \quad I_n$$

and

$$t'(J_1, \ldots, J_k) \quad = \quad I_n,$$

for some $J_1, \ldots, J_k \in \mathbf{I}_\omega(A)$, *then* $|t| > n$.

Then for each finite set E *of equations between shuffle semiring terms with* **Lang** $\models E$ *there exists a finite shuffle semiring* S_E *and shuffle semiring terms* p *and* p' *such that* **Lang** $\models p \leq p'$, $S_E \models E$, *but* $S_E \not\models p \leq p'$. *Moreover,* $S_E \models q \leq q'$, *for all bimonoid terms* q *and* q' *with* **Lang** $\models q \leq q'$.

Remark 5.2 Note that for any poset $P \in \mathbf{SP}(A)$, if I is the principal ideal $(P]$, so that I is also a closed ideal, then the set $\{P\}$ is the only minimal generating set of I. Further, each generating set of a closed ideal in $\mathbf{I}_\omega(A)$ contains a minimal generating set. Thus if $(P_n] \subseteq I_n = cl(X_n)$ and $P_n \notin X_n$, then $(P_n] \subset I_n$. Thus in (P2) we can require $(P_n] \subseteq I_n$ instead of the strict inclusion $(P_n] \subset I_n$.

We briefly describe the construction of S_E. The details of the construction can be found in Appendix A.

Let E be a finite set of equations between shuffle semiring terms with $\mathbf{Lang} \models E$, and let $n = max\{|t|, |t'| \mid t = t' \in E\}$, $N = |P_n|$, so that $N > n$. First we collapse into a single point all closed ideals in $\mathbf{I}_\omega(A)$ which contain at least one "bad" poset, or two posets of different size. A poset $P \in \mathbf{SP}(A)$ is bad if $|P| > N$, or $|P| = N$ but $P \notin I_n$, or there is a letter $a \in A$ which is the label of some vertex of P, but which is not the label of any vertex of a poset in I_n. We do this so that we don't need to worry about bad posets and in order to obtain a finite model. The quotient shuffle semiring S'_E so obtained is in $\mathbf{Lang}$ and I_n is an element of S'_E. Since by (P2) $(P_n] \subset I_n$, the principal ideal $(P_n]$ is also in S'_E. We then modify the additive structure slightly to obtain S_E from S'_E. As a result, whenever $(P_n] \subseteq I \subset I_n$ holds for the closed ideal I, the two ideals I and I_n become incomparable in the induced partial order of S_E, in notation: $I \not\leq I_n$.

All of the conditions (P2)–(P4) are used to establish the fact that S_E is indeed a shuffle semiring. Property (P4) proves that $S_E \models q \leq q'$ for all inequations $q \leq q'$ between the bimonoid terms q and q' with $\mathbf{Lg}_\leq \models q \leq q'$. (Recall that $\mathbf{Lg}_\leq \models q \leq q'$ iff $\mathbf{Lang} \models q \leq q'$.)

The fact that $S_E \models E$ follows by (P5). In fact we show that for all bimonoid terms t and shuffle semiring terms t' with $|t|, |t'| \leq n$, if $\mathbf{Lang} \models t \leq t'$ then $S_E \models t \leq t'$. This suffices to establish $S_E \models E$ for the following reason. First, if t and t' are shuffle semiring terms, $S_E \models t = t'$ iff $S_E \models t \leq t'$ and $S_E \models t' \leq t$, for S_E is a shuffle semiring. Consider the inequation $t \leq t'$. Using the defining equations of shuffle semirings, in particular the distributive and zero laws, we can transform t into a sum $t_1 + \ldots + t_k$, where t_i is a bimonoid term for all $i \in [k]$. (When $k = 0$ this sum is the term 0.) We have $|t_i| \leq |t|$, for all $i \in [k]$. Since S_E is a shuffle semiring, $S_E \models t \leq t'$ iff $S_E \models t_i \leq t'$, for all $i \in [k]$. But if $t = t'$ is in E, we have $\mathbf{Lang} \models t_i \leq t'$ and $|t_i|, |t'| \leq n$.

The shuffle semiring terms p and p' are found easily: We let $p = p(x_1, \ldots, x_k)$ and $p' = p'(x_1, \ldots, x_k)$ be terms with $(P_n] = p_{S_E}((a_1], \ldots, (a_k])$ and $I_n = p'_{S_E}((a_1], \ldots, (a_k])$, for some letters $a_1, \ldots, a_k \in A$ which appear as labels of some vertices of posets in I_n. Since $(P_n] \not\leq I_n$ in S_E, we have $S_E \not\models p \leq p'$. But $\mathbf{Lang} \models p \leq p'$, for it follows from our construction that $(P_n] = p_{\mathbf{I}_\omega(A)}((a_1], \ldots, (a_k])$ and $I_n = p'_{\mathbf{I}_\omega(A)}((a_1], \ldots, (a_k])$.

6 A concrete construction

In this section we give a concrete construction of the posets P_n and the closed ideals I_n satisfying the conditions (P1)–(P5) of the metatheorem, Theorem 5.1. For a nonnegative integer k we denote by $[k]$ the set $\{1, \ldots, k\}$.

Let A be the set

$$A \;:=\; \{a, b_1, b_2, \ldots\}.$$

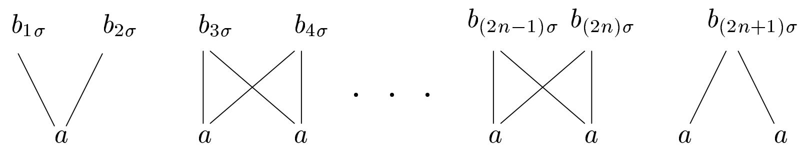
Thus

$$\Sigma(A) \;=\; \{a_j, \bar{a}_j, b_{i,j}, \bar{b}_{i,j} \mid i, j \geq 1\}.$$

Suppose that n is a positive integer. We assign to each permutation $\sigma : [2n+1] \to [2n+1]$ the poset $P_\sigma \in \mathbf{SP}(A)$:

$$P_\sigma \;=\; a \cdot (b_{1\sigma} \otimes b_{2\sigma}) \;\otimes\; \left(\bigotimes_{i=2}^{n} (a \otimes a) \cdot (b_{(2i-1)\sigma} \otimes b_{(2i)\sigma}) \right) \;\otimes\; (a \otimes a) \cdot b_{(2n+1)\sigma}$$

i.e., P_σ is the poset



The construction of the posets P_n and closed ideals $I_n = cl(X_n)$ is given in the following definition.

Definition 6.1 *For each $n \geq 1$, we let X_n stand for the collection of all posets P_σ, where σ is a permutation $[2n+1] \to [2n+1]$. Moreover, we define*

$$\begin{aligned} P_n &:= \bigotimes_{i=1}^{2n+1} a \cdot b_i \\ I_n &:= cl(X_n). \end{aligned}$$

It is obvious that (P1) of the metatheorem holds. In fact, we have $|P_n|_x = |P|_x$, for all $P \in I_n$ and for all letters $x \in A$. The rest of the properties are proved in Appendix B.

7 Further results

There is a stronger version of Theorem 3.1.

Theorem 7.1 *For each finite set E of shuffle semiring equations with* **Lang** $\models E$ *there is a finite shuffle semiring S_E and an equation $p = p'$ with* **Lang** $\models p = p'$ *between shuffle semiring terms p and p' in* **one** *variable such that $S_E \models E$, $S_E \models q \leq q'$, for all bimonoid inequations $q \leq q'$ with* **Lang** $\models q \leq q'$, *but $S_E \not\models p = p'$.*

This result can be proved by a slight change in the concrete construction of the posets P_n and closed ideals I_n. Instead of the infinite set $A = \{a, b_1, b_2, \ldots\}$ one uses a singleton set $\{a\}$. Then each letter b_i gets replaced by a poset in $\mathbf{SP}(\{a\})$. We need to be careful by selecting these posets, but the replacement $b_i \mapsto a^i$ works. The technical details of the argument are more complex, though similar.

We briefly consider the enrichment with the Kleene star operation. For an alphabet Σ, let $\mathbf{L}_\Sigma^*$ denote the structure $(P_\Sigma, \cdot, \otimes, +, {}^*, 0, 1)$. Let $\mathbf{Lang}^*$ be the variety generated by the structures $\mathbf{L}_\Sigma^*$.

Theorem 7.2 $\mathbf{Lang}^*$ *has no finite (equational) axiomatization over* **Lang**.

Thus, in addition to all valid equations of **Lang**, an infinite number of equations involving the operation * are needed to obtain a complete axiomatization of the variety $\mathbf{Lang}^*$. The same result holds if one considers iterated shuffle † defined by:

$$x^\dagger \quad := \quad 1 + x + x \otimes x + x \otimes x \otimes x + \ldots$$

But there is nothing surprising here, Theorem 7.2 follows from the fact that the regular sets (over the one letter alphabet) do not have a finite axiomatization, cf. [19], [9]. The proof of Theorem 7.2 using this fact is standard.

There are other operations of interest. In contrast with the star operation, the equational laws of reversal $\breve{}$ (mirror image) can be captured by the involution axioms relative to any variety considered above:

$$\begin{aligned}(x+y)\breve{} &= \breve{x}+\breve{y}\\ (x\cdot y)\breve{} &= \breve{y}\cdot\breve{x}\\ (x\otimes y)\breve{} &= \breve{x}\otimes\breve{y}\\ (x^*)\breve{} &= (\breve{x})^*\\ (x^\dagger)\breve{} &= (\breve{x})^\dagger\\ \breve{\breve{x}} &= x\end{aligned}$$

It follows from the other axioms that $\breve{0}=0$ and $\breve{1}=1$.

8 Open Problems

Problem 1 Give nontrivial infinite (in)equational axiomatizations of the varieties $\mathbf{Lg}_\leq$, **Lang**, and $\mathbf{Lang}^*$. Do there exist minimal equational axiomatizations?

Problem 2 Does there exist a finitely based first order theory (e.g. universal Horn theory) whose equational part is the equational theory of **Lang**, or $\mathbf{Lang}^*$, or the (in)equational theory of some other variety discussed above other than **Lg**?

Problem 3 Is it possible to add some more natural operations to the collection of operations we have been considering such that the variety generated by the resulting language structures has a finite axiomatization?

Problem 4 Does the inequational theory of $\mathbf{Lg}_\leq$ have a finite axiomatization in terms of equations between shuffle semiring terms which hold in **Lang**? (More precisely, the question is whether there exists a finite set E of shuffle semiring equations with $\mathbf{Lang} \models E$ such that for all inequations $t \leq t'$ between bimonoid terms t and t', if $\mathbf{Lg}_\leq \models t \leq t'$ then $E \models t \leq t'$.)

Each variety has a minimal first order axiomatization, but there are varieties with no minimal equational axiomatization. The second question of Problem 1 asks if the varieties $\mathbf{Lg}_\leq$, **Lang** and $\mathbf{Lang}^*$ studied here are such.

When one considers the regular operations $\cdot$, $+$, * on languages together with the constants 0 and 1, the corresponding variety (that we denote **L** below) has no finite axiomatization. Infinite sets of equational axioms were obtained in [15, 5], but these are not minimal. For the variety **L**, positive answers to Problems 2 and 3 are given in [20, 3, 15, 14, 8, 18]. Due to Theorem 4.4, there is an $\mathcal{O}(n \log n)$ algorithm for deciding the equational theory of **Lg**. By modifying the proof of Theorem 3.1 in [10], it is shown in [6] that deciding the inequational theory of the variety $\mathbf{Lg}_\leq$ is Π_2-complete in the polynomial hierarchy. The same fact holds for the equational theory of **Lang**. Further, deciding the equational theory of the variety $\mathbf{Lang}^*$ is PSPACE-complete. There is a further difference between the two varieties **Lg** and $\mathbf{Lg}_\leq$, or **Lang**, the variety **Lg** has a finite axiomatization but $\mathbf{Lg}_\leq$ and **Lang** do not. This difference is reflected by the complexity result.

References

[1] L. Aceto. Full abstraction for series-parallel pomsets. In *Proceedings of TAPSOFT '91*, volume 493 of *Lecture Notes in Computer Science*, pages 1–40. Springer-Verlag, 1991.

[2] L. Aceto and M. Hennessy. Towards action refinement in process algebras. *Information and Computation*, 103(2):204–269, 1993.

[3] K. B. Arkhangelskii and P. V. Gorshkov. Implicational axioms for the algebra of regular languages. *Dokl. Akad. Nauk USSR Ser. A*, 10:67–69, 1987. (in Russian)

[4] S. L. Bloom. Varieties of ordered algebras. *Journal of Computer and System Sciences*, 45:200–212, 1976.

[5] S. L. Bloom and Z. Ésik. Equational axioms for regular sets. *Mathematical Stuctures in Computer Science*, 3:1–24, 1993.

[6] S. L. Bloom and Z. Ésik. Free shuffle algebras in language varieties. Full version submitted for publication. Extended abstract to appear in the proceedings of LATIN '95.

[7] S. L. Bloom and Z. Ésik. Nonfinite axiomatizability of shuffle inequalities. In: *Proceedings of TAPSOFT '95*, LNCS 915, Springer–Verlag, 1995, 318–333.

[8] M. Boffa. Une remarque sur les systèmes complets d'identites rationelles. *Theoret. Inform. Appl.*, 24:419–423, 1990.

[9] J. Conway. *Regular Algebra and Finite Machines.* Chapman & Hall, London, 1971.

[10] J. Feigenbaum, J. A. Kahn, C. Lund. Complexity results for pomset languages. *SIAM Journal of Discrete Mathematics*, 6(3):432–444, 1993.

[11] Jay Loren Gischer. *Partial orders and the axiomatic theory of shuffle.* PhD thesis, Stanford University, Computer Science Dept., 1984.

[12] Jay Loren Gischer. The equational theory of pomsets. *Theoretical Computer Science*, 61:199–224, 1988.

[13] Jan Grabowski. On partial languages. *Fundamenta Informatica*, IV(2):427–498, 1981.

[14] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation, 110:366–390, 1994.

[15] D. Krob. Complete systems of B-rational identities. *Theoretical Computer Science*, 89:207–343, 1991.

[16] A. Meyer and A. Rabinovich. Private communication.

[17] Vaughan Pratt. Modeling concurrency with partial orders. *International Journal of Parallel Processing*, 15(1):33–71, 1986.

[18] Vaughan Pratt. Action structures and pure induction. Technical Report, Stanford University, Dept. of Computer Science, April 1991.

[19] V. N. Redko. On defining relations for the algebra of regular events. *Ukrain. Mat. Z.*, 16:120–126, 1964. (in Russian)

[20] Arto Salomaa. Two complete axiom systems for the algebra of regular events. *J. ACM*, 13:158–169, 1966.

[21] J. Valdes, R. E. Tarjan, and E. L. Lawler. The recognition of series-parallel digraphs. *SIAM Journal of Computing*, 11(2):298–313, 1981.

A Proof of the metatheorem

In this appendix we give a detailed proof of the metatheorem, Theorem 5.1, which we restate here as Theorem A.1 for the reader's convenience. If k is a nonnegative integer, $[k]$ denotes the set $\{1, \ldots, k\}$.

Theorem A.1 *Suppose that for each $n \geq 1$ we are given a poset $P_n \in \mathbf{SP}(A)$ and a closed ideal $I_n = cl(X_n) \in \mathbf{I}_\omega(A)$ with the following properties.*

(P1) $|P_n| = |P| > n$, *for all* $P \in I_n$.

(P2) $(P_n] \subset I_n$ *and* $P_n \notin X_n$.

(P3) For all $X \subseteq \mathbf{SP}(A)$, *if* $(P_n] \subseteq cl(X) \subset I_n$ *then* $P_n \in X$.

(P4) I_n *has no nontrivial sequential or parallel decomposition, i.e., if* $I_n = I \cdot J$ *or* $I_n = I \otimes J$, *for some* $I, J \in \mathbf{I}_\omega(A)$, *then* $I = 1$ *or* $J = 1$.

(P5) If t is a bimonoid term and t' is a shuffle semiring term with $\mathrm{var}(t) = \mathrm{var}(t') = \{x_1, \ldots, x_k\}$, *and if*

$$(P_n] \quad \subseteq \quad t(J_1, \ldots, J_k) \quad \subset \quad I_n$$

and

$$t'(J_1, \ldots, J_k) \quad = \quad I_n,$$

for some $J_1, \ldots, J_k \in \mathbf{I}_\omega(A)$, *then* $|t| > n$.

Then for each finite set E of equations between shuffle semiring terms with $\mathbf{Lang} \models E$ *there exists a finite shuffle semiring S_E and shuffle semiring terms p and p' such that* $\mathbf{Lang} \models p \leq p'$, $S_E \models E$, *but* $S_E \not\models p \leq p'$. *Moreover,* $S_E \models q \leq q'$, *for all bimonoid terms q and q' with* $\mathbf{Lang} \models q \leq q'$.

Proof. Let $n = \max\{|t|, |t'| \mid t = t' \in E\}$ and $N = |P_n|$, so that $N > n$. Let $\mathcal{A} \subseteq \mathbf{I}_\omega(A)$ consist of the closed ideals $I \in \mathbf{I}_\omega(A)$ such that either there is a poset $P \in I$ with $|P| > N$, or there is a poset $P \in I$ with $|P| = N$ but $P \notin I_n$, or some vertex of a poset in I is labeled by a letter $a \in A$ which is not the label of any vertex of a poset in I_n, or I contains posets of different sizes, i.e., posets P, Q with $|P| \neq |Q|$.

Fact Suppose $I \in \mathcal{A}$ and $J \in \mathbf{I}_\omega(A)$. Then $I + J \in \mathcal{A}$. Moreover, when J is a nonzero closed ideal, $I \cdot J, J \cdot I, I \otimes J$ all belong to $\mathcal{A}$.

It follows that the relation $\sim$ defined on $\mathbf{I}_\omega(A)$ by

$$I \sim J \quad \Longleftrightarrow \quad I = J \text{ or } I, J \in \mathcal{A}$$

is a shuffle semiring congruence. Let S'_E denote the quotient $\mathbf{I}_\omega(A)/\!\sim$. Each congruence class is either a singleton containing a closed ideal not in $\mathcal{A}$ or the set $\mathcal{A}$. Thus we may alternatively represent S'_E as the shuffle semiring whose elements are the closed ideals not in $\mathcal{A}$ and the element $\#$ which represents the congruence class $\mathcal{A}$. The shuffle semiring operations and constants are defined in a straightforward manner, so that $I + \# = J \cdot \# = \# \cdot J = J \otimes \# = \#$, for all $I, J \in S'_E$, $J \neq 0$. It follows that if $t = t(x_1, \ldots, x_k)$ is a shuffle semiring term with $var(t) = \{x_1, \ldots, x_k\}$, and if $J_1, \ldots, J_k \in S'_E - \{\#\}$, then

$$t_{S'_E}(J_1, \ldots, J_k) \quad = \quad t_{\mathbf{I}_\omega(A)}(J_1, \ldots, J_k)$$

except the case that $t_{\mathbf{I}_\omega(A)}(J_1,\dots,J_k) \in \mathcal{A}$. In this case, $t_{S'_E}(J_1,\dots,J_k) = \#$. Moreover, when t does not contain an occurrence of 0 and $J_i = \#$, for some $i \in [k]$, then $t_{S'_E}(J_1,\dots,J_k) = \#$.

The shuffle semiring S_E is obtained from S'_E by modifying the structure of S'_E slightly. Let Z_0 denote the set

$$Z_0 \ := \ I_n - \{P_n\}.$$

We define

$$S_E \ := \ (S'_E - \{I_n\}) \cup \{Z_0\}.$$

There is a bijection

$$\varphi : S_E \ \longrightarrow \ S'_E$$

which maps Z_0 to I_n and is the identity map on $S_E - \{I_n\}$. We define the shuffle semiring operations and constants on S_E so that φ becomes an isomorphism except that

$$I + J \ = \ \#$$

whenever $I, J \subseteq I_n$, $P_n \in I \cup J$ and $cl(I \cup J) = I_n$. Thus, in particular, $Z_0 + (P_n] = \#$, but $Z_0 + Z_0 = Z_0$.

Remark A.2 We will prove below that S_E is indeed a shuffle semiring. Thus the additive structure determines a partial order which can be described as follows. For all $I, J \in S_E$, $I \leq J$ if and only if $J = \#$ or $I \neq \# \neq J$ and $I \subseteq J$. Thus, since $P_n \notin Z_0$, $(P_n] \not\leq Z_0$. Similarly, if $(P_n] \subseteq I \subset I_n$, for some closed ideal I, then $I \not\leq Z_0$.

Remark A.3 For later use we note that $cl(Z_0) = I_n$. Indeed, since by (P2) $P_n \notin X_n$, $X_n \subseteq Z_0 \subset I_n$. Thus

$$I_n = cl(X_n) \subseteq cl(Z_0) \subseteq cl(I_n) = I_n.$$

Lemma A.4 *Suppose that $t = t(x_1,\dots,x_k)$ is a shuffle semiring term with $\mathrm{var}(t) = \{x_1,\dots,x_k\}$ which does not contain 0. Let $J_1 \dots, J_k \in S_E$.*

(i) If $J_i = \#$, for some $i \in [k]$, then $t_{S_E}(J_1,\dots,J_k) = t_{S'_E}(\varphi(J_1),\dots,\varphi(J_k)) = \#$.

Suppose that $J_1,\dots,J_k \neq \#$.

(ii) If $t_{\mathbf{I}_\omega(A)}(\varphi(J_1),\dots,\varphi(J_k)) \in \mathcal{A}$, then

$$t_{S_E}(J_1,\dots,J_k) \quad = \quad t_{S'_E}(\varphi(J_1),\dots,\varphi(J_k)) \quad = \quad \#.$$

(iii) If $t_{\mathbf{I}_\omega(A)}(\varphi(J_1),\dots,\varphi(J_k)) = I_n$, then

$$\begin{aligned} &t_{S_E}(J_1,\dots,J_k) \in \{Z_0, \#\} \\ &t_{S'_E}(\varphi(J_1),\dots,\varphi(J_k)) = I_n. \end{aligned}$$

(iv) If $t_{\mathbf{I}_\omega(A)}(\varphi(J_1),\dots,\varphi(J_k)) = I$, for some $I \in S_E - \{Z_0, \#\}$, then $J_i \in S_E - \{Z_0, \#\}$ and hence $\varphi(J_i) = J_i$ for all $i \in [k]$, and

$$\begin{aligned} t_{S_E}(J_1,\dots,J_k) &\ = \ I \\ t_{S'_E}(J_1,\dots,J_k) &\ = \ I. \end{aligned}$$

We omit the simple induction argument proving Lemma A.4.

Corollary A.5 *Suppose that $t = t(x_1, \ldots, x_k)$ and $t' = t'(x_1, \ldots, x_k)$ are shuffle semiring terms with $\mathrm{var}(t) = \mathrm{var}(t') = \{x_1, \ldots, x_k\}$ which do not contain an occurrence of 0. Let $J_1, \ldots, J_k \in S_E$ with*

$$I = t_{S_E}(J_1, \ldots, J_k) \quad \neq \quad t'_{S_E}(J_1, \ldots, J_k) = I'$$

and

$$t_{S'_E}(\varphi(J_1), \ldots, \varphi(J_k)) \quad = \quad t'_{S'_E}(\varphi(J_1), \ldots, \varphi(J_k)).$$

Then $J_1, \ldots, J_k \neq \#$ and $\{I, I'\} = \{Z_0, \#\}$. Further,

$$t_{S'_E}(\varphi(J_1), \ldots, \varphi(J_k)) \quad = \quad I_n$$

and

$$t_{\mathbf{I}_\omega(A)}(\varphi(J_1), \ldots, \varphi(J_k)) = t'_{\mathbf{I}_\omega(A)}(\varphi(J_1), \ldots, \varphi(J_k)) = I_n.$$

Lemma A.6 *Suppose that $I, J \in S_E$.*

(i) $I + J = Z_0$ if and only if $I, J \neq \#$, $cl(I \cup J) = I_n$ and $P_n \notin I \cup J$.

(ii) $I + J = \#$ if and only if $I = \#$ or $J = \#$, or $I, J \neq \#$ and either there exist some $P \in I$ and $Q \in J$ with $|P| \neq |Q|$, or $cl(I \cup J) = I_n$ and $P_n \in I \cup J$.

(iii) In all other cases, $I, J \neq \#$ and $I + J = cl(I \cup J)$.

Remark A.7 The conditions formulated in (i) can alternatively be expressed by $I, J \subseteq Z_0$, $cl(I \cup J) = I_n$, for $P_n \notin Z_0$.

Proof. We prove (i). Suppose that $I, J \in S_E$ with $I + J = Z_0$. Then $I, J \neq \#$. Let $I' = \varphi(I)$, $J' = \varphi(J)$. Then, by Lemma A.4,

$$I' + J' = cl(I' \cup J') = I_n, \tag{1}$$

both in S'_E and in $\mathbf{I}_\omega(A)$. Since $I \subseteq I'$ and $J \subseteq J'$, $cl(I \cup J) \subseteq I_n$. If $cl(I \cup J) \subset I_n$, then by Remark A.3, $I, J \neq Z_0$ and thus $I' = I$ and $J' = J$, so that we obtain a contradiction to (1). Thus $cl(I \cup J) = I_n$. If $P_n \in I \cup J$ then $I + J = \#$, by definition. Thus $P_n \notin I \cup J$. The converse direction holds by definition. □

Lemma A.8 *For all $I, J, K \in S_E$,*

$$(I + J) + K = Z_0 \quad \Longleftrightarrow \quad I, J, K \subseteq Z_0 \text{ and } cl(I \cup J \cup K) = I_n.$$

Proof. Suppose that $(I + J) + K = Z_0$. Then, by Lemma A.6, $I + J, K \subseteq Z_0$ and

$$cl((I + J) \cup K) \quad = \quad I_n. \tag{2}$$

Case 1: $I + J = Z_0$. Then, again by Lemma A.6, $I, J \subseteq Z_0$ and $cl(I \cup J) = I_n$. Thus,

$$\begin{aligned} cl(I \cup J \cup K) &= cl(cl(I \cup J) \cup K) \\ &= cl(I_n \cup K) \\ &= I_n, \end{aligned}$$

since $K \subseteq Z_0 \subset I_n$ and I_n is closed.

Case 2: $I + J \subset Z_0$. Then $I + J$ is a closed ideal strictly included in I_n. Thus, by Lemma A.6, part (iii), $I + J = cl(I \cup J)$. Thus,

$$\begin{aligned} cl(I \cup J \cup K) &= cl(cl(I \cup J) \cup K) \\ &= cl((I + J) \cup K) \\ &= I_n, \end{aligned}$$

by (2).

Since $I \cup J \subseteq cl(I \cup J) = I + J \subset Z_0$, we have $I, J \subset Z_0$.

For the converse direction, suppose that $I, J, K \subseteq Z_0$ and $cl(I \cup J \cup K) = I_n$.

Case 1: $cl(I \cup J) = I_n$. Since $P_n \notin I \cup J$, $I + J = Z_0$. Since $P_n \notin K$, $Z_0 + K = Z_0$ either by definition or by Lemma A.6.

Case 2: $cl(I \cup J) \subset I_n$. Then, in S_E, $I + J = cl(I \cup J)$, by Lemma A.6. Thus, since $P_n \notin K$, $(I + J) + K = Z_0$ unless $P_n \in cl(I \cup J)$. But if $P_n \in cl(I \cup J)$, we have $(P_n] \subseteq cl(I \cup J) \subset I_n$. Thus, by (P3), $P_n \in I \cup J$, a contradiction. □

Lemma A.9 *S_E is a shuffle semiring.*

Proof. Since the bijection $\varphi : S_E \to S'_E$ preserves the constants and the operations of sequential and shuffle product, all those defining equations of shuffle semirings hold in S_E which do not involve sum. The fact that sum is commutative and idempotent is immediate. Further, the zero laws hold in S_E. The distributive laws are easy consequences of (P4). Indeed, suppose that

$$I \cdot (J + K) \quad \neq \quad I \cdot J + I \cdot K, \tag{3}$$

for some $I, J, K \in S_E$. By Corollary A.5, this is possible only if one side of (3) is Z_0 and the other side is $\#$. Moreover, $I, J, K \neq \#$, and defining $I' = \varphi(I)$, $J' = \varphi(J)$ and $K' = \varphi(K)$ we have, both in S'_E and in $\mathbf{I}_\omega(A)$,

$$I' \cdot (J' + K') = I' \cdot J' + I' \cdot K' = I_n.$$

But then, by (P4), either $I' = 1$ or $J' + K' = 1$. If $I' = 1$ then $I = 1$, and if $J' + K' = 1$ then $J' = K' = J = K = 1$. In either case, we obviously have $I \cdot (J + K) = I \cdot J + I \cdot K$, contradicting (3). The argument based on (P4) that the other distributive laws hold, is similar.

Thus the only nontrivial fact to be proved is that sum is associative. But let $I, J, K \in S_E$. By Lemma A.8, and since sum is commutative,

$$\begin{aligned} (I + J) + K = Z_0 \quad &\iff \quad I + (J + K) = Z_0 \\ &\iff \quad I, J, K \subseteq Z_0 \text{ and } cl(I \cup J \cup K) = I_n, \end{aligned}$$

for all $I, J, K \in S_E$. Thus by Corollary A.5, $(I + J) + K = I + (J + K)$. □

Generalizing the argument given in the proof of Lemma A.8, we can show:

Corollary A.10 *Suppose that $I_1, \ldots, I_k \in S_E$, $k > 0$. Then $I_1 + \ldots + I_k = Z_0$ iff $I_1, \ldots, I_k \subseteq Z_0$ and $cl(I_1 \cup \ldots \cup I_k) = I_n$.*

To prove that S_E satisfies all bimonoid inequations $t \leq t'$ with $\mathbf{Lang} \models t \leq t'$, we need a simple observation. For a variable x, let $|t|_x$ denote the number of occurrences of x in t. Hence $|t| = \sum_x |t|_x$, where the sum is taken over all variables $x \in var(t)$ occurring in t.

Lemma A.11 *Suppose that $t = t(x_1, \ldots, x_k)$ and $t' = t'(x_1, \ldots, x_k)$ are bimonoid terms with* $\mathbf{Lang} \models t \le t'$. *Then $|t|_{x_i} = |t'|_{x_i}$, for all $i \in [k]$, so that $var(t) = var(t')$ and $|t| = |t'|$.*

Proof. Let B be the k-element set $\{b_1, \ldots, b_k\}$. Since $\mathbf{Lang} \models t \le t'$, we have $\mathbf{Lg}_{\le} \models t \le t'$ and thus

$$P = t_{\mathbf{SP}(B)}(b_1, \ldots, b_k) \quad \le \quad t'_{\mathbf{SP}(B)}(b_1, \ldots, b_k) = P'.$$

But then $(P] \subseteq (P']$, and since $|P|_{b_i} = |t|_{x_i}$ and $|P'|_{b_i} = |t'|_{x_i}$, for all $i \in [k]$, the result follows from Lemma 4.14. □

We return to the proof of the metatheorem, Theorem A.1. Suppose that $t = t(x_1, \ldots, x_k)$ and $t' = t'(x_1, \ldots, x_k)$ are bimonoid terms with $\mathbf{Lang} \models t \le t'$. We need to show that $S_E \models t \le t'$. Since S_E is a shuffle semiring, and by Lemma A.11, we may assume without loss of generality that the constant 1 does not occur in the terms t and t'. If $S_E \not\models t \le t'$, then there exist $J_1, \ldots, J_k \in S_E$ with

$$J = t_{S_E}(J_1, \ldots, J_k) \quad \not\le \quad t'_{S_E}(J_1, \ldots, J_k) = J' \tag{4}$$

i.e.,

$$J + J' \quad \ne \quad J'.$$

We may assume that $J_1, \ldots, J_k \ne 1$. By Corollary A.5, $J_1, \ldots, J_k \ne \#$ and $\{J + J', J'\} = \{Z_0, \#\}$. But if $J' = \#$, then $J + J' = J + \# = \#$, so that $J' = Z_0$. Hence, by Lemma A.4, $t'_{\mathbf{I}_\omega(A)}(\varphi(J_1), \ldots, \varphi(J_k)) = I_n$. But since I_n has neither a nontrivial sequential decomposition nor a nontrivial parallel decomposition (property (P4)), and since t' contains no occurrence of 1 and $\varphi(J_1), \ldots, \varphi(J_k) \ne 1$, t' must be a variable x_i. But then, by Lemma A.11, t is also x_i, contradiction to (4). Thus $S_E \models t \le t'$.

Before proving that $S_E \models E$ we need some preparations.

Lemma A.12 *Suppose that $t = t(x_1, \ldots, x_k)$ is a bimonoid term and $t' = t'(x_1, \ldots, x_k)$ is a shuffle semiring term. If* $\mathbf{Lang} \models t \le t'$ *then $var(t) \subseteq var(t')$.*

Proof. This follows from the fact that if a poset $P \in \mathbf{SP}(B)$ is in the closed ideal $I = cl(X) \in \mathbf{I}_\omega(B)$, and if some vertex of P is labeled $b \in B$, then there is a poset $Q \in X$ which also has a vertex labeled b. To give another proof, consider the set $\Sigma = \{c\}$ and the shuffle semiring $\mathbf{L}_\Sigma$. In order to obtain a contradiction, assume that $var(t) - var(t') \ne \emptyset$. Then, for each $i \in [k]$, let $a_i = \{c\}$ if $x_i \in var(t) - var(t')$, and let $a_i = 1$ if $x_i \in var(t')$. Then $t(a_1, \ldots, a_k)$ contains a nonempty word but $t'(a_1, \ldots, a_k)$ does not. □

Lemma A.13 *Suppose that t and t' are a shuffle semiring terms. Let t'' be the term obtained from t' by substituting 0 for each occurrence of each variable not in $var(t)$. Then for all shuffle semirings S,*

$$S \models t \le t' \iff S \models t \le t''.$$

Proof. Since the operations are monotonic, $S \models t'' \le t'$. Thus, if $S \models t \le t''$, then $S \models t \le t'$. The converse is obvious. □

Lemma A.14 *Suppose that x is a variable and t is a shuffle semiring term. If* $\mathbf{Lang} \models x \le t$ *then there exists some term t' with* $\mathbf{S} \models t = t' + x$, *so that* $\mathbf{S} \models x \le t$.

We omit the easy proof which uses Lemma 4.14.

We now prove that $S_E \models E$. Since S_E is a shuffle semiring, this will follow if we can show that $S_E \models t \leq t'$ for all bimonoid terms t and all shuffle semiring terms t' such that $|t|, |t'| \leq n$ and **Lang** $\models t \leq t'$. (Recall the definition of the integer n.) Let E' denote the collection of all such inequations $t \leq t'$.

Assume to the contrary that $S_E \not\models E'$. Then choose $t \leq t'$ in E' such that $S_E \not\models t \leq t'$ and $|t'|$ is minimal. Since S_E is a shuffle semiring we may assume that 0 does not occur in t' and 1 does not occur in t. By Lemmas A.12 and A.13 we have $var(t) = var(t') = \{x_1, \ldots, x_k\}$, say.

Since $S_E \not\models t \leq t'$, there exist some $J_1, \ldots, J_k \in S_E$ with

$$t_{S_E}(J_1, \ldots, J_k) \quad \not\leq \quad t'_{S_E}(J_1, \ldots, J_k). \tag{5}$$

Thus $J_i \notin \{0, \#\}$, for all $i \in [k]$. Moreover, since $|t'|$ is minimal, $J_1, \ldots, J_k \neq 1$. The shuffle semiring S'_E is in **Lang**. Since **Lang** $\models t \leq t'$,

$$t_{S'_E}(J'_1, \ldots, J'_k) \quad \leq \quad t'_{S'_E}(J'_1, \ldots, J'_k), \tag{6}$$

where $J'_i = \varphi(J_i)$, for all $i \in [k]$. Comparing (5) and (6) it follows by Corollary A.5 that

$$t'_{S_E}(J'_1, \ldots, J'_k) \quad = \quad Z_0,$$

hence

$$\begin{aligned} t'_{\mathbf{I}_\omega(A)}(J'_1, \ldots, J'_k) \quad &= \quad I_n \\ t_{\mathbf{I}_\omega(A)}(J'_1, \ldots, J'_k) \quad &\subseteq \quad I_n, \end{aligned}$$

by Lemma A.4 and since **Lang** $\models t \leq t'$. Suppose that $t_{\mathbf{I}_\omega(A)}(J'_1, \ldots, J'_k) = I_n$. Then, since I_n has no nontrivial sequential or parallel decomposition, and since 1 does not occur in t and $J'_1, \ldots, J'_k \neq 1$, the term t must be a variable. In particular, since $var(t) = \{x_1, \ldots, x_k\}$, we have $k = 1$ and $t = x_1$. But then, since **Lang** $\models t \leq t'$, by Lemma A.14 we must have $\mathbf{S} \models t \leq t'$, contradicting (5). We conclude that

$$t_{\mathbf{I}_\omega(A)}(J'_1, \ldots, J'_k) \quad \subset \quad I_n.$$

Thus, by Lemma A.4, $J_i = J'_i$, for all $i \in [k]$, and

$$t_{S_E}(J_1, \ldots, J_k) \quad = \quad t_{S'_E}(J_1, \ldots, J_k).$$

Hence, $t_{S_E}(J_1, \ldots, J_k) \leq Z_0$ unless $(P_n] \subseteq t_{\mathbf{I}_\omega(A)}(J'_1, \ldots, J'_k)$, so that

$$(P_n] \quad \subseteq \quad t_{\mathbf{I}_\omega(A)}(J'_1, \ldots, J'_k) \quad \subset \quad I_n.$$

But then $|t| > n$, by (P5), contradicting the assumption $|t| \leq n$. Thus $S_E \models E$.

To complete the proof of the metatheorem, we need to find the terms p and p' with **Lang** $\models p \leq p'$ and $S_E \not\models p \leq p'$. Let $A_0 \subseteq A$ consist of the letters $a \in A$ such that some poset in I_n (or in X_n) has a vertex labeled a. Then A_0 is a finite nonempty set, $A_0 = \{a_1, \ldots, a_k\}$, say. Note that the principal ideals $(a_i]$, $i \in [k]$, are in S_E.

Lemma A.15 *There exists a bimonoid term $p = p(x_1, \ldots, x_k)$ and a shuffle semiring term $p' = p'(x_1, \ldots, x_k)$ such that*

$$\begin{aligned} (P_n] \quad &= \quad p_{S_E}((a_1], \ldots, (a_k]) &(7)\\ Z_0 \quad &= \quad p'_{S_E}((a_1], \ldots, (a_k]) &(8)\\ (P_n] \quad &= \quad p_{\mathbf{I}_\omega(A)}((a_1], \ldots, (a_k]) &(9)\\ I_n \quad &= \quad p'_{\mathbf{I}_\omega(A)}((a_1], \ldots, (a_k]) &(10) \end{aligned}$$

Thus, since $(P_n] \not\leq Z_0$, $S_E \not\models p \leq p'$. But by (9) and (10), and since $(P_n] \subseteq I_n$ in the free shuffle semiring $\mathbf{I}_\omega(A)$ in the variety **Lang**, we have $\mathbf{Lang} \models p \leq p'$.

Proof of Lemma A.15. Let p be any bimonoid term with $P_n = p_{\mathbf{SP}(A)}(a_1, \ldots, a_k)$. Then (9) follows from the fact that $\mathbf{SP}(A)$ is isomorphic to the sub bimonoid of $\mathbf{I}_\omega(A)$ determined by the principal ideals. Since $(P_n] \subset I_n$, (7) follows from Lemma A.4, part (iv).

The term p' is obtained in the following way. Let $X_n = \{Q_1, \ldots, Q_m\}$. Using the fact that each series-parallel poset with two or more vertices has either a nontrivial sequential or parallel decomposition, but $I_n = cl(X_n)$ does not, it follows that $m > 1$. For each $i \in [m]$, choose a bimonoid term $q_i(x_1, \ldots, x_k)$ with $Q_i = (q_i)_{\mathbf{I}_\omega(A)}(a_1, \ldots, a_k)$, i.e. $(Q_i] = (q_i)_{\mathbf{I}_\omega(A)}((a_1], \ldots, (a_k])$. We define $p' = q_1 + \ldots + q_m$. (More precisely, $p' = \overline{q}_m$, where $\overline{q}_1 = q_1$ and $\overline{q}_{i+1} = \overline{q}_i + q_{i+1}$, for $i \in [m-1]$.) It follows that $(P_n] \not\subseteq (Q_i]$, for all $i \in [m]$. Indeed, if $(P_n] \subseteq (Q_1]$, say, then $(P_n] \subseteq (Q_1] = cl(\{Q_1\}) \subseteq I_n$. But $P_n \neq Q_1$, (property (P2)), thus $(Q_1] = I_n$, (property (P3)), which in turn is impossible, (property (P4)). Thus $(Q_i] \subseteq Z_0$, for all $i \in [m]$, and $cl((Q_1] \cup \ldots \cup (Q_m]) = cl(X_n) = I_n$. Hence (8) holds by Corollary A.10 which in turn implies (10), by Lemma A.4. □

The proof of the metatheorem is complete.

B Proof of the construction

In this appendix we prove that the posets P_n and the closed ideals $I_n = cl(X_n)$ defined in Section 6 satisfy the properties (P1)–(P5) of the metatheorem. For the reader's convenience we repeat the definitions.

Let A be the set

$$A \quad := \quad \{a, b_1, b_2, \ldots\}.$$

Thus

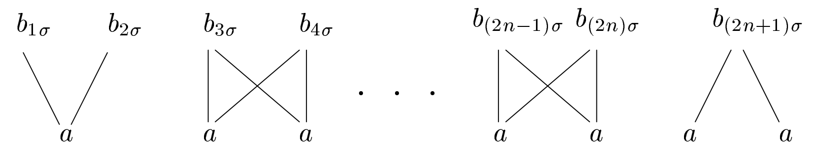
$$\Sigma(A) \quad = \quad \{a_j, \bar{a}_j, b_{i,j}, \bar{b}_{i,j} \mid i, j \geq 1\}.$$

Below we will often write a for a_1 and b_i for $b_{i,1}$.

Suppose that n is a positive integer. We assign to each permutation $\sigma : [2n+1] \to [2n+1]$ the poset $P_\sigma \in \mathbf{SP}(A)$:

$$P_\sigma \quad = \quad a \cdot (b_{1\sigma} \otimes b_{2\sigma}) \otimes \left(\bigotimes_{i=2}^{n} (a \otimes a) \cdot (b_{(2i-1)\sigma} \otimes b_{(2i)\sigma}) \right) \otimes (a \otimes a) \cdot b_{(2n+1)\sigma}$$

i.e., P_σ is the poset



Definition B.1 *For each $n \geq 1$, we let X_n stand for the collection of all posets P_σ, where σ is a permutation $[2n+1] \to [2n+1]$. Moreover, we define*

$$P_n \quad := \quad \bigotimes_{i=1}^{2n+1} a \cdot b_i$$

$$I_n \quad := \quad cl(X_n).$$

We note some properties of the posets P_σ.

Lemma B.2 *Suppose that $Y \subseteq X_n$. Then for each permutation $\tau : [2n+1] \to [2n+1]$,*

$$P_\tau \in cl(Y) \quad \Longleftrightarrow \quad P_\tau \in Y.$$

Proof. Assume that $P_\tau \in cl(Y)$. Define

$$u \;=\; a^{2n+1}\bar{a}b_{1\tau}b_{2\tau}\bar{a}^2 b_{3\tau}b_{4\tau}\ldots\bar{a}^2 b_{(2n-1)\tau}b_{(2n)\tau}\bar{a}^2 b_{(2n+1)\tau}\bar{b}_1\ldots\bar{b}_{2n+1}. \tag{11}$$

Since $u \in P_\tau h_0$ and $P_\tau \in cl(Y)$, there exists some $P_\sigma \in Y$ with $u \in P_\sigma h_0$. But this is possible only if $P_\tau = P_\sigma$. □

Corollary B.3 *The following four conditions are equivalent for posets $P_\tau, P_\sigma \in X_n$.*

(i) *The word u defined in (11) is in $P_\sigma h_0$.*

(ii) $P_\tau \leq P_\sigma$.

(iii) $P_\tau = P_\sigma$.

(iv) $\{1\tau, 2\tau\} = \{1\sigma, 2\sigma\}$ *and*

$$\{\{(2i-1)\tau,\ (2i)\tau\} \mid 1 < i \leq n\} \;=\; \{\{(2i-1)\sigma,\ (2i)\sigma\} \mid 1 < i \leq n\},$$

so that also $(2n+1)\tau = (2n+1)\sigma$. □

Thus, there are distinct permutations σ and τ with $P_\sigma = P_\tau$.

Lemma B.4 $(P_n] \subset I_n$.

Proof. Up to admissible isomorphism, the maximal words in $P_n h_0$ are the words

$$u_\pi \;=\; a_1\ldots a_{2n+1}\bar{a}_1 b_{1\pi}\ldots\bar{a}_{2n+1}b_{(2n+1)\pi}\bar{b}_1\ldots\bar{b}_{2n+1},$$

where π is a permutation $[2n+1] \to [2n+1]$. But $u_\pi \in P_\pi h_0 \subseteq X_n h_0$, proving $P_n \in I_n$. Hence $(P_n] \subseteq I_n$. But $(P_n] \neq I_n$, so that $(P_n] \subset I_n$. □

Thus (P2) has been established.

Lemma B.5 *Suppose that $\sigma, \tau : [2n+1] \to [2n+1]$ are permutations. Then the word*

$$u \;=\; a^{2n+1}\bar{a}b_{1\tau}\ldots\bar{a}b_{(2n+1)\tau}\bar{b}_1\ldots\bar{b}_{2n+1} \tag{12}$$

is in $P_\sigma h_0$ iff $P_\sigma = P_\tau$.

Proof. Use Corollary B.3, part (iv). □

Lemma B.6 *Suppose that $Y \subseteq X_n$. If $P_n \in cl(Y)$ then $Y = X_n$.*

Proof. Suppose that $P_n \in cl(Y)$ but $Y \neq X_n$, so that $P_\sigma \notin Y$, for some permutation $\sigma : [2n+1] \to [2n+1]$. Let u denote the word (12), Then $u \in P_n h_0$. But $u \notin cl(Y)$, by Lemma B.5. □

We now establish (P3) in the following form.

Lemma B.7 *Suppose that $I \in \mathbf{I}_\omega(A)$ with*

$$(P_n] \subseteq I \subseteq I_n.$$

Let X be a minimal generating set of I, so that $cl(X) = I$ and $cl(X') \subset I$ whenever $X' \subset X$. If $P_n \notin X$ then $X = X_n$ and thus $I = I_n$.

Proof. By definition, each poset P in I has $4n+2$ vertices, $2n+1$ labeled a and a vertex labeled b_i, for each $i \in [2n+1]$. Further, P has at most $2n+1$ minimal and $2n+1$ maximal vertices and no isolated vertex. Each minimal vertex is labeled by a, and each maximal vertex is labeled by some b_i (Lemma 4.14).

Suppose that π is a permutation $[2n+1] \to [2n+1]$. Then the word

$$u_\pi = a_1 \ldots a_{2n+1} \bar{a}_1 b_{1\pi} \ldots \bar{a}_{2n+1} b_{(2n+1)\pi} \bar{b}_1 \ldots \bar{b}_{2n+1}$$

is in $P_n h_0$. Since $P_n \in cl(X)$, there exists a poset $R_\pi \in X$ with $u_\pi \in R_\pi h_0$. We note several properties of the poset R_π.

(i) The vertices of R_π can be arranged in two levels, level 0 and level 1. Level 0 contains $2n+1$ minimal vertices labeled a, and level 1 consists of $2n+1$ maximal vertices, one maximal vertex labeled b_i, for each $i \in [2n+1]$. Each level 0 vertex is less than at least one level 1 vertex, and each level 1 vertex is greater than at least one level 0 vertex. No other nontrivial order relations exist.

(ii) Since R_π is series-parallel, R_π is the parallel product of connected components of the form

$$R = (ka) \cdot (b_{i_1} \otimes \ldots \otimes b_{i_l}),$$

where $k, l > 0$ and ka stands for the k-fold parallel product of a with itself. Let us call the integer $l - k$ the rank of R.

(iii) The rank of each connected component R is at most 1. Indeed, if $l - k > 1$ for the component R, then there is some word $a^k \overline{a}^k b_{i_1} \ldots b_{i_l} u$ in $R_\pi h_0$. But there is no such word in $X_n h_0$.

(iv) For the same reason, R_π does not have two connected components of positive rank.

(v) Thus, since the sum of the ranks of the connected components is zero, either each component has rank 0, or there is a connected component of rank 1 and a connected component of rank -1, and all other components have rank 0.

(vi) Since $R_\pi \neq P_n$ and since $u_\pi \in R_\pi h_0$, R_π must have a connected component of rank 1. Thus, R_π has exactly one connected component of rank 1, and exactly one connected component of rank -1. Moreover, the connected component of rank 1 must be the poset $a \cdot (b_i \otimes b_j)$, and the connected component of rank -1 the poset $(a \otimes a) \cdot b_k$, for some distinct integers $i, j, k \in [2n+1]$.

(vii) Suppose R_π has a connected component which is a two-element chain $a \cdot b_l$. Then there is a word u such that $a\bar{a}b_i b_j a\bar{a}b_l u$ is in $R_\pi h_0$. But there is no such word in $X_n h_0$.

(viii) But R_π cannot have a connected component

$$(ka) \cdot (b_{i_1} \otimes \ldots \otimes b_{i_k})$$

where $k > 2$, for otherwise u_π would not be in $R_\pi h_0$.

(ix) Thus, R_π must be one of the posets in X_n.

Consider now the set $Y \subseteq X$ of the posets R_π, where $\pi : [2n+1] \to [2n+1]$ is a permutation. We have seen that $Y \subseteq X_n$ and that $u_\pi \in Y h_0$, for each permutation π. But, up to admissible isomorphism, the words u_π are all of the maximal words in $P_n h_0$. Thus $P_n \in cl(Y)$, and since $Y \subseteq X_n$, we have $Y = X_n$, by Lemma B.6. But then $I = I_n$ and $X = X_n$, since X is a minimal generating set of I_n. □

Lemma B.8 *Suppose that $I = cl(X) \subseteq I_n$. Then $X_n \cap I \subseteq X$.*

Proof. Suppose that $P_\sigma \in X_n \cap I$. The word

$$u \quad = \quad a^{2n+1}\bar{a}b_{1\sigma}b_{2\sigma}\bar{a}^2 b_{3\sigma}b_{4\sigma}\ldots\bar{a}^2 b_{(2n-1)\sigma}b_{(2n)\sigma}\bar{a}^2 b_{(2n+1)\sigma}\bar{b}_1\ldots\bar{b}_{2n+1}$$

is in $P_\sigma h_0$, hence there exists a poset R_σ in X with $u \in R_\sigma h_0$. Using similar arguments as before, we can show that R_σ is in X_n. Thus R_σ is in fact P_σ, by Corollary B.3. □

Corollary B.9 *If $Y \subseteq X_n$, then Y is the unique minimal generating set of $cl(Y)$. In particular, X_n is the unique minimal generating set of I_n.* □

Corollary B.10 *Suppose that $I \in \mathbf{I}_\omega(A)$ and $I \subseteq I_n$. If $I = J + K$, for some $J, K \in \mathbf{I}_\omega(A)$, then*

$$I \cap X_n \quad \subseteq \quad (J \cap X_n) \cup (K \cap X_n).$$

Proof. Since $I = cl(J \cup K)$, each $P_\sigma \in I \cap X_n$ is in $J \cup K$, by Lemma B.8. □

Lemma B.11 *I_n has no nontrivial parallel decomposition.*

Proof. Assume to the contrary that $J \otimes K$ is a nontrivial parallel decomposition of I_n. Then there exists a number $r \in \{0, 1, \ldots, 2n+1\}$ such that each poset in J has r vertices labeled a, and each poset in K has $s = 2n+1-r$ vertices labeled a. Further, the set $[2n+1]$ is the disjoint union $U \cup V$ such that the posets in J have exactly one vertex labeled b_i, for each $i \in U$, and no vertex labeled b_j, if j is not in U. Similarly, the posets in K have exactly one vertex labeled b_i, for each $i \in V$, and no vertex labeled b_j, if j is not in V. Since $J, K \neq 1$, $|U| + r \neq 0$ and $|V| + s \neq 0$.

Since $I_n = J \otimes K$, we have $I_n = cl(X)$, where

$$X \quad = \quad \{P \otimes Q \mid P \in J, Q \in K\}.$$

But by Corollary B.9, each generating set of I_n contains all the posets in X_n. Thus $X_n \subseteq X$. If $J \cup K$ contains a poset which has a minimal vertex labeled by some b_i, $i \in [2n+1]$, then so does X. But by Lemma 4.14, there is no such poset in I_n. For a similar reason, there exists no poset in $J \cup K$ which has a maximal vertex labeled by a. In particular, $r, s > 0$ and $|U|, |V| > 0$. Let $i \in U$ and $j \in V$, and let τ be a permutation $[2n+1] \to [2n+1]$ with $1\tau = i$ and $2\tau = j$. Then the poset P_τ is not in X. □

Lemma B.12 *Suppose that $I \in \mathbf{I}_\omega(A)$ is a nonempty closed ideal consisting of posets of some equal positive size m. If I contains a poset $R = R_1 \otimes R_2$ where $R_1, R_2 \neq 1$, then I has no nontrivial sequential decomposition.*

Proof. In order to obtain a contradiction, suppose that $I = J \cdot K$, for some $J, K \in \mathbf{I}_\omega(A)$ such that $J, K \neq 1$. Then there exist positive integers m_1 and m_2 such that the posets in J have size m_1 and the posets in K have size m_2. Indeed, otherwise I would contain posets of different size. The set

$$Y \;=\; \{P \cdot Q \mid P \in J, Q \in K\}$$

is a generating set of I. Thus $Rh_0 \subseteq Yh_0$. If $u = u_1 u_2 \in Yh_0$ where u_1 is the length $2m_1$ prefix of u, we have $|u_1|_c = |u_1|_{\bar{c}}$, for all $c \in \Sigma(A)$. But it is easy to construct a word in Rh_0 which does not have this property. One needs to consider a lower ideal $U \subseteq R$ with $|U| = m_1 - 1$ such that both $R_1 - U$ and $R_2 - U$ are nonempty. Since $m_1, m_2 > 0$, there is such a lower ideal. □

Corollary B.13 *I_n has no nontrivial sequential decomposition.* □

Property (P4) is established.

Lemma B.14 *Property (P5) holds. In more detail, suppose that t is a bimonoid term and t' is a shuffle semiring term with $\mathsf{var}(t) = \mathsf{var}(t') = \{x_1, \ldots, x_k\}$. If*

$$(P_n] \;\subseteq\; J \;=\; t(J_1, \ldots, J_k) \;\subset\; I_n \tag{13}$$

and

$$t'(J_1, \ldots, J_k) \;=\; I_n, \tag{14}$$

for some $J_1, \ldots, J_k \in \mathbf{I}_\omega(A)$, then $|t| > n$.

Proof. It is obvious that none of the J_i is empty. We may also assume that $J_i \neq 1$, for all $i \in [k]$. Since $J \subseteq I_n$, each poset P in J has $4n + 2$ vertices, one vertex labeled b_i, for each $i \in [2n + 1]$, and $2n + 1$ vertices labeled a. Moreover, each minimal vertex of P is labeled by a and each maximal vertex is labeled by some b_i in the set $\{b_1, \ldots, b_{2n+1}\}$ (Lemma 4.14). In particular, P has no isolated vertex. It follows that for each $i \in [k]$ there exists an integer $r_i \geq 0$ and a set $U_i \subseteq \{b_1, \ldots, b_{2n+1}\}$ such that each poset $Q \in J_i$ has exactly r_i vertices labeled a, exactly one vertex labeled b_j, if $b_j \in U_i$, and no vertex labeled b_j, if $b_j \notin U_i$.

The integers r_i and the sets U_i satisfy the following conditions.

(i) For each $i \in [k]$, $r_i > 0$ or $|U_i| > 0$.

(ii) If $i, j \in [k]$ and $i \neq j$, then $U_i \cap U_j = \emptyset$.

(iii) $\sum_{i=1}^{k} r_i |t|_{x_i} = 2n + 1$, where $|t|_{x_i}$ is the number of occurrences of the variable x_i in t.

(iv) $\bigcup_{i=1}^{k} U_i = \{b_1, \ldots, b_{2n+1}\}$.

(v) For each $i \in [k]$, if $U_i \neq \emptyset$, then $|t|_{x_i} = 1$.

Consider the X-labeled series-parallel poset

$$R \;:=\; t_{\mathbf{SP}(X)}(x_1,\ldots,x_k),$$

where X denotes the set of variables $\{x_1,\ldots,x_k\}$. Note that R has exactly $|t|_{x_i}$ vertices labeled x_i, for each $i\in[k]$.

By (13) and the above properties of the integers r_i and the sets U_i, the following conditions hold for the poset R.

(i) The height of R is at most 1. Indeed, otherwise the height of each poset in J would be at least 2, by Lemma 4.14, contradicting $P_n \in J$.

(ii) If v is a minimal vertex of R and v is labeled by x_i, then $r_i > 0$. Indeed, if $r_i = 0$ then $|U_i| > 0$. But then some poset in J would have a minimal vertex labeled by a letter $b_j \in U_i$.

(iii) If v is a maximal vertex of R and v is labeled by x_i, then $|U_i| > 0$.

(iv) Thus, if v is an isolated vertex of R and v is labeled by x_i, then $r_i > 0$ and $|U_i| > 0$. Moreover, if P is in J_i, then each minimal vertex of P is labeled by a, and each maximal vertex of P is labeled by some letter in U_i.

(v) If $v_1 < v_2$ for the vertices v_1 and v_2 labeled x_{i_1} and x_{i_2}, respectively, so that v_1 is a minimal vertex and v_2 is a maximal vertex, then $r_{i_1} = 1$ and $U_{i_1} = \emptyset$. Moreover, v_1 is the only predecessor of vertex v_2. Indeed, $r_{i_1} > 0$, by (ii), and $U_{i_2} \neq \emptyset$, by (iii). Let $b_j \in U_{i_2}$. If $r_{i_1} \neq 1$ or $U_{i_1} \neq \emptyset$, or if v_1 is no the only predecessor of v_2, then there exists no word $a\bar{a}b_ju$ in Jh_0, but there is such a word in P_nh_0.

(vi) Under the assumptions of (v), $r_{i_2} = 0$ and $|U_{i_2}| = 1$ or $|U_{i_2}| = 2$. Indeed, if $r_{i_2} \neq 0$, then each poset $P \in J_{i_2}$ contains a vertex labeled by a. But no vertex of P labeled by a is a maximal vertex, for otherwise some poset in J would have a maximal vertex labeled by a. It follows again that Jh_0 contains no word of the form $a\bar{a}b_ju$, where $b_j \in U_{i_2}$. On the other hand, if $|U_{i_2}| \geq 3$, say $b_{j_1}, b_{j_2}, b_{j_3} \in U_{i_2}$, then by (v) Jh_0 contains a word $a\bar{a}b_{j_1}b_{j_2}b_{j_3}u$, but there is no such word in X_nh_0.

There exist bimonoid terms $t_i(x_1,\ldots,x_k)$, $i\in[s]$, $s>0$, such that $\mathbf{S} \models t' = t_1 + \ldots + t_s$. Let us define $K_i := t_i(J_1,\ldots,J_k)$, $i\in[s]$. Then $cl(K_1\cup\ldots\cup K_s) = I_n$, so that $X_n \subseteq K_1\cup\ldots\cup K_s$, by Corollary B.9. For each term t_j and for each variable x_i, if $U_i \neq \emptyset$, then x_i occurs in t_j exactly once, since otherwise (14) would fail. But by the above argument, if $U_i = \emptyset$ then $r_i = 1$, so that $J_i = \{a\} = (a]$ is a singleton set. It follows that $K_j = cl(K'_j)$, where

$$K'_j \;=\; \{(t_j)_{\mathbf{SP}(A)}(R_1,\ldots,R_k) \mid R_i \in J_i, i\in[k]\}.$$

Hence

$$cl(K'_1\cup\ldots\cup K'_s) \;=\; I_n$$

and

$$X_n \;\subseteq\; K'_1\cup\ldots\cup K'_s. \tag{15}$$

We show that if v_1 is an isolated vertex of R, then $R = \{v_1\}$. Suppose that $R \neq \{v_1\}$. Then R has a maximal vertex v_2 other than v_1. Suppose that v_1 is labeled x_{i_1} and v_2 is labeled x_{i_2}. Then $U_{i_1}, U_{i_2} \neq \emptyset$ and $U_{i_1}\cap U_{i_2} = \emptyset$. Thus, there exist distinct letters $b_{j_1}\in U_{i_1}$ and $b_{j_2}\in U_{i_2}$. Let τ be a permutation $[2n+1]\to[2n+1]$ with $1\tau = j_1$ and $2\tau = j_2$. Since v_1 is isolated, for each poset $P\in J_{i_1}$ the vertex v of P labeled b_{i_1} is larger than some vertex v' labeled a. It follows that there exists no bimonoid term $\bar{t}(x_1, \ldots, x_k)$ such that $\bar{t}(R_1, \ldots, R_k) = P_\tau$ for some $R_1 \in J_1, \ldots, R_k \in J_k$. Indeed, the vertex v_1 of the poset $\bar{t}(R_1, \ldots, R_k)$ which is labeled by b_{j_1} has an immediate predecessor which is not a predecessor of the vertex v_2 labeled by b_{j_2}. Thus $P_\tau \notin K'_1 \cup \ldots \cup K'_s$, contradicting (15).

But if R is a singleton, $k = 1$ and $\mathbf{S} \models t = x_1$. It follows that $\mathbf{S} \models t' = x_1$, which is impossible by (13) and (14).

Thus R has no isolated vertex. But then R has at least $2n + 1$ vertices, since for each $i \in [k]$ either $r_i = 0$ or $r_i = 1$, and since $\sum_{i=1}^{k} r_i = 2n + 1$. Thus $|R| = |t| > n$. □

We have established all of the properties (P1)–(P5). The proof of Theorem 3.1 is complete.