

S. L. BLOOM

Z. ÉSIK

## **Shuffle binoids**

*Informatique théorique et applications*, tome 32, n° 4-6 (1998), p. 175-198.

[http://www.numdam.org/item?id=ITA\\_1998\\_\\_32\\_4-6\\_175\\_0](http://www.numdam.org/item?id=ITA_1998__32_4-6_175_0)

© AFCET, 1998, tous droits réservés.

L'accès aux archives de la revue « Informatique théorique et applications » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

## SHUFFLE BINOIDS (\*)

by S. L. BLOOM<sup>#</sup> (1) and Z. ÉSIK<sup>†</sup> (2)

Communicated by C. CHOFFRUT

---

Abstract. – We study the equational properties of the shuffle operation on finitary and  $\omega$ -languages in combination with both binary concatenation  $L \cdot L'$  and  $\omega$ -powers,  $L^\omega = L \cdot L \cdots$ . © Elsevier, Paris

### 1. MOTIVATION: LANGUAGES AND CONCURRENCY

For a fixed alphabet  $\Sigma$ , consider the two sorted structure  $L(\Sigma) = (\Sigma_f, \Sigma_\omega)$  consisting of all finitary languages i.e., subsets of  $\Sigma^*$ , denoted  $\Sigma_f$ , and all  $\omega$ -languages, i.e., subsets of  $\Sigma^\omega$ , denoted  $\Sigma_\omega$ , equipped with the following operations.

$$L, W \mapsto L \cdot W,$$

for  $L \in \Sigma_f$  and  $W$ , a finitary or  $\omega$ -language;

$$U, W \mapsto U \otimes W,$$

such that both  $U, W$  are finitary or both are  $\omega$ -languages, where,  $U \otimes W$  denotes the shuffle product of the languages  $U$  and  $W$ , namely the language

$$\{u_1 v_1 u_2 v_2 \dots : u_1 u_2 \dots \in U, v_1 v_2 \dots \in V, u_i, v_i \in \Sigma^*\}.$$

---

(\*) Received May 1998.

<sup>#</sup> Supported in part by the U.S.-Hungarian Joint Fund, grant 351 and by LIAFA, Université Paris 7.

<sup>†</sup> Partially supported by a grant of the National Foundation for Scientific Research of Hungary and the U.S.-Hungarian Joint Fund, grant 351.

(1) Stevens Institute of Technology, Department of Computer Science, Hoboken, NJ 07030, e-mail:bloom@cs.stevens-tech.edu

(2) A. József University, Department of Computer Science, Szeged, Hungary. e-mail:esik@inf.u-szeged.hu

If  $L$  is finitary, we include the function

$$L \mapsto L^\omega,$$

where  $L^\omega$  is the set of all infinite words obtained by concatenating nonempty words in  $L$ . If  $1$  is the set consisting of the empty word,  $1^\omega$  is the empty set, and  $(\Sigma_f, \cdot, \otimes, 1)$  is a “bimonoid”, in the terminology of [BÉ96]. (For example  $a^\omega \otimes b^\omega$  is the set of all words containing infinitely many  $a$ 's and  $b$ 's.) Aside from the operations of concatenation and  $\omega$ -powers, we allow binary shuffle products of finitary or  $\omega$ -languages.

We want to know: *What are all of the equations which hold in all language structures?*

The study of the algebraic properties of operations on languages has a long history. Most previous work has focused on the “regular operations” of finite concatenation, union and iteration. Recently there has been renewed interest in this subject (see [Kr91, Bof90, Bof95, BÉSt, Koz94, És98].) The study of the shuffle operation on languages was initiated by Pratt [Pra86] and Gischer [Gis94], and later continued by Tschantz [Tsc94] and others [BÉ96, BÉ95, BÉ97, ÉBr95]. In the “interleaving model” of concurrency, sequential and parallel composition are modeled by concatenation and shuffle on languages. The extension of the model to  $\omega$ -powers is natural, because in this context, this operation models infinite looping behavior.

Another model of concurrency, also suggested by Pratt [Pra86], uses labeled posets. Sequential and parallel composition are modeled in a very natural way. We define an  $\omega$ -power operation on posets, and show here that for the operations of sequential and parallel product (concatenation and shuffle in languages) and  $\omega$ -powers, the language model and the poset model of concurrency satisfy the same equations, a result which was established without the  $\omega$ -power operation in [Tsc94, BÉ96].

The method used to prove that the equations (1)-(8) below are complete, both for labeled posets and languages, is also of interest. A model of these equations is called a “shuffle binoid”. We show that a certain class of labeled posets is free in the equational class of all shuffle binoids, and use this fact to then show that these posets embed in the shuffle binoid of languages. This embedding is a nice way of coding posets by languages so that the operations are preserved. However, it is not clear how efficient this encoding is.

## 2. SOME EQUATIONAL PROPERTIES

We note some properties of the operations on the language structures  $L(\Sigma) = (\Sigma_f, \Sigma_\omega)$ , for any  $\Sigma$ . Of course, concatenation and shuffle on finite languages are associative, and shuffle is associative and commutative on finitary and  $\omega$ -languages. Thus,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad (1)$$

$$a \cdot (b \cdot v) = (a \cdot b) \cdot v \quad (2)$$

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c \quad (3)$$

$$u \otimes (v \otimes w) = (u \otimes v) \otimes w \quad (4)$$

$$a \otimes b = b \otimes a \quad (5)$$

$$u \otimes v = v \otimes u \quad (6)$$

for  $a, b, c \in \Sigma_f$  and  $u, v, w \in \Sigma_\omega$ . For any  $a, b \in \Sigma_f$ , the operation of  $\omega$ -power satisfies at least the following equations:

$$(a \cdot b)^\omega = a \cdot (b \cdot a)^\omega \quad (7)$$

$$(a^n)^\omega = a^\omega, \quad n \geq 1. \quad (8)$$

These operations happen to form an enrichment of a *Wilke algebra* [Wil91].

**DEFINITION 2.1:** A **Wilke algebra** is a two-sorted algebra  $(S_f, S_\omega)$  equipped with three operations, an associative product on  $S_f$ , a mixed product  $S_f \times S_\omega \rightarrow S_\omega$  which satisfies (2), and a map  $a \mapsto a^\omega$  from  $S_f$  to  $S_\omega$  satisfying, for all  $a, b \in S_f$  the equations (7)-(8) above. A **morphism**  $\varphi : (S_f, S_\omega) \rightarrow (T_f, T_\omega)$  of Wilke algebras is a pair of functions  $\varphi_f : S_f \rightarrow T_f$  and  $\varphi_\omega : S_\omega \rightarrow T_\omega$  which preserve all operations, e.g.,  $\varphi_\omega(a^\omega) = \varphi_f(a)^\omega$ .

The Wilke algebras were called “binoids” by Wilke in [Wil91].

**DEFINITION 2.2:** A **shuffle binoid** is a two-sorted structure  $B = (F, I)$  equipped with a polymorphic “shuffle” operation in addition to the operations

of a Wilke algebra; the shuffle operation is defined on all pairs  $u, v \in F$  or  $u, v \in I$  and the structure satisfies all of the equations (1)-(8) above.

A **morphism of shuffle binoids**  $\varphi : (F, I) \rightarrow (F', I')$  is a pair of functions  $\varphi_F : F \rightarrow F'$  and  $\varphi_I : I \rightarrow I'$  which preserve all of the operations, e.g.,

$$\begin{aligned}\varphi_I(a^\omega) &= (\varphi_F(a))^\omega, \quad a \in F \\ \varphi_I(a \cdot x) &= \varphi_F(a) \cdot \varphi_I(x), \quad a \in F, x \in I.\end{aligned}$$

Note that the equations (8) may be replaced by the subset

$$(x^p)^\omega = x^\omega, \quad p \text{ prime}, \quad (9)$$

since, e.g., if  $p$  is prime and just the identities (9) hold,  $(x^{pq})^\omega = ((x^q)^p)^\omega = (x^q)^\omega$ . Note also that the equation  $aa^\omega = a^\omega$  is derivable from the facts that  $(aa)^\omega = a(aa)^\omega$ , as a special case of (7), and  $(aa)^\omega = a^\omega$ , as a special case of (8).

We will show that the equations defining shuffle binoids completely characterize these operations on languages. Our method is the following. We let  $\mathbf{L}$  denote the variety of shuffle binoids generated by the language structures described above. We let  $V$  denote the variety of all shuffle binoids. Clearly,  $\mathbf{L} \subseteq V$ . We will give a concrete description of the free algebras in  $V$  and use this description to show that  $V = \mathbf{L}$ . The description is used also to give a polynomial time algorithm to decide the validity of equations in  $V$ . Last, we show that there is no finite axiomatization of  $V$ .

### 3. $\text{SP}^\omega(A, B)$

Let  $X$  be a nonempty set. Suppose that  $P = (P, \leq_P)$  and  $Q = (Q, \leq_Q)$  are  $X$ -labeled posets (meaning that each vertex is labeled by some element of  $X$ ), with disjoint underlying sets. Following [VTL81, Pra86], define the **series product** of  $P$  and  $Q$  by

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

where

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

so that every element of  $P$  is less than each element of  $Q$ ; similarly, define the **parallel** or **shuffle product** of  $P$  and  $Q$  by

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

where

$$x \leq_{P \otimes Q} y \Leftrightarrow x \leq_P y \text{ or } x \leq_Q y,$$

so that elements in  $P$  and  $Q$  are incomparable. The labeling on  $P \cdot Q$  and  $P \otimes Q$  is inherited from the labeling of  $P$  and  $Q$  respectively. If  $P$  is any poset, define  $P^\omega$  as the countable series product of  $P$  with itself:

$$P^\omega := P \cdot P \cdot P \cdot \dots$$

(More formally, we define  $P^\omega = (P \times \{1, 2, \dots\}, \leq)$ , where  $(p, i) \leq (p', j)$  if  $i < j$  or  $i = j$  and  $p \leq_P p'$ . The label of  $(p, i)$  is the label of  $p$ .) Without further comment, we identify isomorphic  $X$ -labeled posets, so that, for example, there is a small set of all finite (or countably infinite)  $X$ -labeled posets.

For disjoint sets  $A, B$  let  $Pos(A, B) = (P_f(A), P_\omega(A, B))$  denote the two-sorted structure, where  $P_f(A)$  is all finite  $A$ -labeled posets, and  $P_\omega(A, B)$  is all finite or countably infinite  $(A \cup B)$ -labeled posets in which a vertex is labeled by an element in  $B$  iff it is maximal. The operations are the shuffle binoid operations  $\cdot, \otimes, \omega$ , where  $\cdot$  and  $\otimes$  are appropriately polymorphic.

PROPOSITION 3.1:  $Pos(A, B)$  is a shuffle binoid.  $\square$

REMARK 3.2: Another shuffle binoid may be obtained by taking sets of posets in  $Pos(A, B)$ . The series and parallel product operations are the complex operations derived from the corresponding operations on  $Pos(A, B)$ , and for a set  $X \subseteq P_f(A)$ , we define  $X^\omega$  as the set of all posets  $P_1 \cdot P_2 \cdot \dots$ , for  $P_i \in X$ .

DEFINITION 3.3: For a pair of disjoint nonempty sets  $A, B$ , let  $\mathbf{SP}^\omega(A, B)$  denote the pair  $(F_A, I_{A,B})$ , in which  $F_A$  is the least collection of  $A$ -labeled posets containing the singletons  $a$ , for each  $a \in A$  closed under series and parallel product, and where  $I_{A,B}$  is the least collection of labeled posets containing

- the singleton poset  $b$ , for  $b \in B$ ;
- the posets  $P^\omega$ , for  $P \in F_A$ ;
- $P \cdot Q$ , for  $P \in F_A, Q \in I_{A,B}$ ;
- $Q \otimes Q'$ , for  $Q, Q' \in I_{A,B}$ .

PROPOSITION 3.4: For any disjoint sets  $A, B$ ,  $\mathbf{SP}^\omega(A, B)$  is a shuffle binoid.  $\square$

In fact,  $\mathbf{SP}^\omega(A, B)$  is a sub shuffle binoid of  $\text{Pos}(A, B)$ .

REMARK 3.5: Recall that any maximal vertex of a poset in  $P_\omega(A, B)$  is labeled by an element of  $B$ . Thus, if  $B$  is empty, and  $Q \in I_{A, B}$ , then  $Q$  has no maximal elements.

It is not difficult to prove the next Proposition.

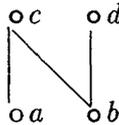
PROPOSITION 3.6 [Gis84]:  $F_A$  is freely generated by the set  $A$  in the variety of all models of the following three equations:

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

This fact will be useful in Section 5. We will call a model of the equations listed in Proposition 3.6 a **bi-semigroup**.

#### 4. CHARACTERIZATION OF $\mathbf{SP}^\omega(A, B)$

Recall that a poset  $P$  satisfies the “N-condition” if it has no “N’s”, i.e., there is no four element subset  $\{a, b, c, d\}$  of  $P$  whose **only** nontrivial order relations are:  $a < c$ ,  $b < c$  and  $b < d$ .



The posets in  $F_A$  are the  $A$ -labeled series-parallel posets, i.e., those in the least class of posets containing the singletons closed under series and parallel product. The series-parallel posets have been characterized as those finite nonempty posets satisfying the  $N$ -condition, see [VTL81]. But the infinite posets in  $\mathbf{SP}^\omega(A, B)$  also satisfy this condition, see below.

We recall some elementary poset notions. A poset  $P$  has *finite width* if there is some nonnegative integer  $n$  such that ‘whenever  $v_1, \dots, v_k$  are

unrelated vertices in  $P$ , then  $k \leq n$ ; the least such  $n$  is called the **width** of  $P$ . Thus, a nonempty poset  $P$  has width one iff  $P$  is a total order. A **filter**  $F$  in a poset  $P$  is a nonempty, upward closed subset of  $P$ .

DEFINITION 4.1: A poset  $Q$  satisfies the **generalized  $N$ -conditions** if

1.  $Q$  satisfies the  $N$ -condition.
2. For each  $q \in Q$ , the principal ideal  $(q) = \{x \in Q : x \leq q\}$  is finite.
3. Up to isomorphism, there is a finite number of filters in  $Q$ .

We note that if  $Q$  is a nonempty poset that satisfies the generalized  $N$ -conditions, then  $Q$  has at least one, but only finitely many, minimal elements. Moreover, each element of  $Q$  is over some minimal element. Note also that a finite poset satisfies the generalized  $N$ -conditions iff it satisfies the  $N$ -condition.

REMARK 4.2: If  $Q$  satisfies the generalized  $N$ -conditions, then  $Q$  has finite width. Indeed, if  $\{x_1, x_2, \dots\}$  is an infinite set of incomparable elements, the filters  $F_n = \{y \in Q : y \geq x_i, \text{ for some } i \leq n\}$  are pairwise nonisomorphic.

REMARK 4.3: For countable posets  $Q$ , the condition 2 in the definition of the generalized  $N$ -condition is equivalent to the requirement that  $Q$  has a linearization which is an  $\omega$ -chain.

PROPOSITION 4.4: Let  $Q$  be any infinite poset in  $\mathbf{SP}^\omega(A, B)$ . Then  $Q$  satisfies the generalized  $N$ -conditions.

*Proof:* We use induction on the number of operations needed to construct  $Q$ . It is clear that if  $P$  satisfies the generalized  $N$ -conditions, so does  $P^\omega$ , since the width of  $P^\omega$  is the same as the width of  $P$ , and any " $N$ " must be inside some copy of  $P$ ; the filters in  $P^\omega$  are of the form  $F \cdot P^\omega$ , for some filter  $F$  in  $P$ . Thus  $P^\omega$  has, up to isomorphism, the same number of filters  $P$  has. Lastly, a principle ideal in  $P^\omega$  is also a principle ideal in  $P^n$ , for some  $n \geq 1$ , and since  $P$  is finite, all principle ideals in  $P^\omega$  are finite.

It is clear that if  $P$  is finite and  $Q$  is infinite, and both satisfy the generalized  $N$ -conditions, then so does  $P \cdot Q$ ; if  $Q, Q'$  satisfy all four conditions, so does  $Q \otimes Q'$ .  $\square$

Now we prove the converse

THEOREM 4.5: Suppose that  $Q$  is an  $A \cup B$ -labeled poset which satisfies the generalized  $N$ -conditions. Suppose also that a vertex is maximal iff it is  $B$ -labeled. Then  $Q$  is in  $\mathbf{SP}^\omega(A, B)$ .

*Proof:* We may as well assume that  $Q$  is infinite, since if a finite poset satisfies the  $N$ -condition, it is series-parallel. The assumption on the labeling ensures such finite series-parallel posets are in  $\mathbf{SP}^\omega(A, B)$ .

Now if  $Q$  is infinite, and appropriately labeled, we use induction on the width of the poset to show it is in  $\mathbf{SP}^\omega(A, B)$ . First, note the following fact.

LEMMA 4.6: *If  $Q$  is a poset which satisfies the generalized  $N$ -conditions, then*

- any subposet satisfies the  $N$ -condition;
- any filter in  $Q$  satisfies the generalized  $N$ -conditions, so that in particular if  $Q = Q_1 \otimes Q_2$ , then  $Q_i$  satisfies the generalized  $N$ -conditions,  $i = 1, 2$ , and if  $Q = P \cdot Q'$ , then  $Q'$  satisfies the generalized  $N$ -conditions;
- if  $Q = P \cdot Q'$ , where  $Q'$  is nonempty, then  $P$  is finite. □

A **path**  $u \rightsquigarrow v$  in a poset is a sequence of vertices  $u = q_0, q_1, \dots, q_k = v$  such that for each  $i$ ,  $1 \leq i \leq k$ , either  $q_{i-1} < q_i$  or  $q_{i-1} > q_i$ . Say  $Q$  is **connected** if for any two vertices  $u, v$  of  $Q$  there is a path  $u \rightsquigarrow v$ . Note that  $Q$  is not connected iff  $Q = Q_1 \otimes Q_2$ , for some nonempty posets  $Q_1, Q_2$ .

LEMMA 4.7: *Suppose that  $Q$  satisfies the  $N$ -condition. If  $q_0, q_1, \dots, q_k$  is a shortest path  $q_0 \rightsquigarrow q_k$ , then  $k < 3$ .*

*Proof:* Otherwise,  $\{q_0, q_1, q_2, q_3\}$  is an “ $N$ ”. □

LEMMA 4.8: *Suppose that  $Q$  is a connected poset which satisfies the generalized  $N$ -conditions and has at least two elements. There is some vertex  $q \in Q$  which is strictly larger than all of the minimal elements.*

*Proof:* Since  $Q$  satisfies the generalized  $N$ -conditions,  $Q$  has finitely many minimal elements, say  $\mu_1, \dots, \mu_m$ . By induction on  $k$ , we prove the existence of a vertex above at least the first  $k$  of the minimal elements, for each  $k \leq m$ . The case  $k = 1$  is trivial, since  $|Q| > 1$ . Now assume that  $x > \mu_1, \dots, \mu_k$ , for  $k < m$ . If  $x > \mu_{k+1}$ , we are done. Otherwise, there is a shortest path  $\mu_{k+1} \rightsquigarrow x$ . The length of the path is necessarily one or two, by Lemma 4.7; but the length is not one, by assumption, so that there is some  $y \in Q$  with  $\mu_{k+1} < y$  and  $y > x$ . But then  $y > \mu_i$ , for  $i = 1, 2, \dots, k + 1$ , completing the induction. □

LEMMA 4.9: *Suppose that  $Q$  is a connected poset which satisfies the generalized  $N$ -conditions and has at least two elements. Then  $Q$  has a*

nontrivial series decomposition as  $Q = P \cdot Q'$  for some (nonempty) finite poset  $P$ , and  $P$  has no nontrivial serial decomposition <sup>1</sup>.

*Proof:* Let  $\mu_1, \dots, \mu_m$  be all minimal vertices in  $Q$ . Let  $Q'$  be the set of all vertices strictly above all of these minimal vertices. By Lemma 4.8,  $Q'$  is nonempty. Let  $P = Q - Q'$ . Every element of  $P$  is below every element of  $Q'$ . Indeed, if  $p \in P$  and  $q \in Q'$ , either  $p < q$  or  $p$  and  $q$  are incomparable, since  $Q'$  is upward closed. Suppose, in order to obtain a contradiction, that  $p, q$  are incomparable. There is at least one minimal element  $\mu$  incomparable with  $p$  (or  $p \in Q'$ ), and at least one minimal element  $\mu'$  with  $\mu' \leq p$ . Now if  $\mu' = p, p < q$  by definition of  $Q'$ . Otherwise,  $\{\mu, \mu', p, q\}$  forms an  $N$ , a contradiction. Thus,  $p < q$ . It follows that  $P$  is finite, since  $P$  is the union of the principal ideals generated by the minimal elements of  $Q'$  (minus these elements). Lastly, if  $P = P_1 \cdot P_2$ , for nonempty  $P_1, P_2$ , every element of  $P_2$  is in  $Q'$ , contradicting the definition of  $P$ .  $\square$

Call a poset  $Q$  **eventually disconnected** if  $Q = P \cdot (Q_1 \otimes Q_2)$ , for some nonempty posets  $P, Q_1, Q_2$ .

LEMMA 4.10: *Suppose that  $Q$  is an infinite, connected poset satisfying the generalized  $N$ -conditions. Then either*

- $Q$  is eventually disconnected and

$$Q = P_1 \cdot \dots \cdot P_k \cdot (Q_1 \otimes \dots \otimes Q_t),$$

where  $k > 0, t > 1, Q_1, \dots, Q_t$  are nonempty, connected posets and each of  $P_1, \dots, P_k$  is finite, nonempty and has no nontrivial serial decomposition, or

- $Q$  is not eventually disconnected, and there is a finite set  $P_1, \dots, P_k, \dots, P_{k+1}, k \geq 0, t > 0$ , of finite nonempty posets which have no nontrivial serial decomposition such that

$$Q = P_1 \cdot \dots \cdot P_k \cdot (P_{k+1} \cdot \dots \cdot P_{k+t})^\omega.$$

*Proof:* By Lemma 4.9, we have  $Q = P_1 \cdot Q'$ , for some posets  $P_1, Q'$  such that  $P_1$  is finite and nonempty and has no nontrivial serial decomposition. Necessarily,  $Q'$  is infinite. Now either  $Q'$  is connected or not. If not, since  $Q'$  has finite width by Lemma 4.6,  $Q' = Q_1 \otimes \dots \otimes Q_t$ , for some nonempty

---

<sup>1</sup> A decomposition  $P = P' \cdot P''$  is trivial if either  $P'$  or  $P''$  is the empty poset.

connected posets  $Q_i$ ,  $i = 1, \dots, t$ , each of which satisfy the generalized  $N$ -conditions. If  $Q'$  is connected, then again applying Lemma 4.9,  $Q' = P_2 \cdot Q''$ , for some finite nonempty  $P_2$  and some infinite  $Q''$  such that  $P_2$  has no nontrivial serial decomposition. If the process stops after  $k$  steps, there are nonempty connected posets  $Q_1, \dots, Q_t$ ,  $t > 1$ , with

$$Q = P_1 \cdot \dots \cdot P_k \cdot (Q_1 \otimes \dots \otimes Q_t),$$

as claimed.

If this process continues forever, then  $Q = P_1 \cdot P_2 \cdot \dots$ , where each  $P_i$  is finite, nonempty, and has no nontrivial serial decomposition. Every element of  $Q$  belongs to some  $P_i$ , since principal ideals are finite. Now, using the fact that  $Q$  has only finitely many nonisomorphic filters, there is a pair of integers  $k, t$  such that  $P_{k+1} \cdot P_{k+2} \cdot \dots = P_{k+t+1} \cdot P_{k+t+2} \cdot \dots$ , so that

$$Q = P_1 \cdot \dots \cdot P_k \cdot (P_{k+1} \cdot \dots \cdot P_{k+t})^\omega. \quad \square$$

We now complete the proof of Theorem 4.5. Let  $Q$  be an appropriately labeled infinite poset which satisfies the generalized  $N$ -conditions. We use induction on the width of  $Q$  to show  $Q \in \mathbf{SP}^\omega(A, B)$ . If  $Q$  is not connected, then  $Q = Q_1 \otimes Q_2$  for some nonempty posets  $Q_1, Q_2$ . Each of  $Q_1, Q_2$  has width less than  $Q$ , so that by Lemma 4.6, each is in  $\mathbf{SP}^\omega(A, B)$ . Thus  $Q \in \mathbf{SP}^\omega(A, B)$ . If  $Q$  is eventually disconnected, write  $Q = P \cdot (Q_1 \otimes Q_2)$ , for nonempty  $P, Q_i$ , where  $P$  is finite. Each of  $P, Q_1, Q_2$  belongs to  $\mathbf{SP}^\omega(A, B)$ , and thus, so does  $Q$ . Otherwise,  $Q = P \cdot (P')^\omega$ , for some finite nonempty  $P, P'$ , by Lemma 4.10, and hence  $Q \in \mathbf{SP}^\omega(A, B)$ .  $\square$

REMARK 4.11: It follows from Theorem 4.5 that an infinite poset satisfying the generalized  $N$ -conditions is countably infinite.

DEFINITION 4.12: For any set  $X$ , we use the following notation.

$$\begin{aligned} \text{Pos}(X) &:= \text{Pos}(X, \emptyset) \\ \mathbf{SP}^\omega(X) &:= \mathbf{SP}^\omega(X, \emptyset). \end{aligned}$$

PROPOSITION 4.13: Let  $A, B$  be disjoint sets and let  $X = A \cup B$ . Then  $\text{Pos}(A, B)$  is isomorphic to a sub shuffle binoid of  $\text{Pos}(X)$  containing the singletons  $a \in A$  and the posets  $b^\omega$ , for  $b \in B$ . An injective morphism  $\text{Pos}(A, B) \rightarrow \text{Pos}(X)$  is given by the assignment that maps each poset  $P \in \text{Pos}(A, B)$  to the poset obtained by replacing each vertex of  $P$

labeled  $b \in B$  by the chain  $b^\omega$ . Similarly, the unique binoid morphism  $\mathbf{SP}^\omega(A, B) \rightarrow \mathbf{SP}^\omega(X)$  determined by the functions

$$\begin{aligned} a \in A &\mapsto a \\ b \in B &\mapsto b^\omega. \end{aligned}$$

is injective. □

**5. PROOF OF FREENESS**

In this section, we prove the following theorem. (Each letter  $x$  in  $A \cup B$  denotes the singleton poset labeled  $x$ .)

**THEOREM 5.1:**  $\mathbf{SP}^\omega(A, B)$  is freely generated by  $A$  and  $B$  in the variety  $V$  of all shuffle binoids.

*Proof:* Suppose that  $C = (F, I)$  is a shuffle binoid and  $h_1 : A \rightarrow F$  and  $h_2 : B \rightarrow I$  are any functions. We will show that there is a unique shuffle binoid morphism  $\varphi : \mathbf{SP}^\omega(A, B) \rightarrow C$  which extends  $h_1$  and  $h_2$  on the singletons. It follows from Proposition 3.6 that  $\varphi_F : F_A \rightarrow F$  is forced to be the unique structure preserving morphism extending  $h_1$ . On the singleton posets  $b$  in  $I_{A,B}$ , the definition of  $\varphi$  is forced to be  $bh_2$ . On the other posets, we use induction on the width of the poset, using Lemma 4.10. Below, unless stated otherwise, we will only consider nonempty posets.

If  $Q$  is not connected, then write  $Q = Q_1 \otimes \dots \otimes Q_t, t > 1$ , where  $Q_j \in I_{A,B}, j \in [t]$ , are nonempty, connected posets. Then define

$$Q\varphi_I := Q_1\varphi_I \otimes \dots \otimes Q_t\varphi_I.$$

If  $Q$  is connected and has the form

$$Q = P_1 \cdot \dots \cdot P_k \cdot (P_{k+1} \cdot \dots \cdot P_{k+t})^\omega,$$

where  $P_1, \dots, P_{k+t}$  have no nontrivial serial decomposition, and  $k$  is least such that for some  $n > 0, P_{k+1} \cdot \dots = P_{k+n+1} \cdot \dots$ , and if  $t$  is the least  $n$  such that  $Q$  has this representation, then define

$$Q\varphi_I := P_1\varphi_F \cdot \dots \cdot P_k\varphi_F \cdot (P_{k+1}\varphi_F \cdot \dots \cdot P_{k+t}\varphi_F)^\omega.$$

If  $Q$  is connected and has the form

$$Q = P_1 \cdot \dots \cdot P_k \cdot b,$$

where again  $P_1, \dots, P_k$  have no nontrivial serial decomposition and  $b \in B$ , then define

$$Q\varphi := P_1\varphi_F \cdot \dots \cdot P_k\varphi_F \cdot b\varphi_I.$$

Otherwise, if

$$Q = P_1 \cdot \dots \cdot P_k \cdot (Q_1 \otimes \dots \otimes Q_t),$$

with  $Q_i$  connected, for each  $i \in [t]$  and  $t \geq 2$ , then define

$$Q\varphi_I = P_1\varphi_F \cdot \dots \cdot P_k\varphi_F \cdot (Q_1\varphi_I \otimes \dots \otimes Q_t\varphi_I),$$

which is defined since the width of each  $Q_j$  is less than that of  $Q$ .

The definition of  $\varphi$  was forced, so we need only show that with this definition,  $\varphi$  is a shuffle binoid morphism, i.e., it preserves all the operations. It is enough to prove the following facts.

1. If  $P \in F_A$ ,

$$(P^\omega)\varphi_I = (P\varphi_F)^\omega. \quad (10)$$

Suppose that we decompose  $P$  as  $P_1 \cdot \dots \cdot P_k$  where none of the  $P_i$  can be decomposed into a nontrivial serial product. Then

$$P^\omega = P_1 \cdot \dots \cdot P_k \cdot P_1 \cdot \dots \cdot P_k \cdot \dots$$

The definition of  $P^\omega\varphi$  requires finding the least  $t$  such that

$$P^\omega = (P_1 \cdot \dots \cdot P_t)^\omega,$$

and perhaps for some  $t$  which divides  $k$ , and some  $n$ ,

$$P_1 \cdot \dots \cdot P_k = (P_1 \cdot \dots \cdot P_t)^n.$$

Thus, by definition,

$$\begin{aligned} P^\omega\varphi_I &:= ((P_1 \cdot \dots \cdot P_t)^n)^\omega\varphi_I \\ &= ((P_1 \cdot \dots \cdot P_t)\varphi_F)^\omega, && \text{by definition of } P\varphi_I \\ &= (((P_1 \cdot \dots \cdot P_t)\varphi_F)^n)^\omega, && \text{since } B \text{ is a shuffle binoid} \\ &= (P\varphi_F)^\omega, && \text{since } \varphi_F \text{ preserves composition.} \end{aligned}$$

2. If  $P \in F_A$  and  $Q \in I_{A,B}$ , then

$$(P \cdot Q)\varphi_I = P\varphi_F \cdot Q\varphi_I. \quad (11)$$

There are several subcases to this one, depending on the form of  $Q$ . First, assume that  $Q$  is either disconnected or eventually disconnected. Then write  $Q = P' \cdot (Q_1 \otimes \dots \otimes Q_t)$ , where  $P'$  may be empty, but is finite, and each  $Q_i$  is connected. Then, by definition,

$$\begin{aligned} (P \cdot Q)\varphi_I &= (P \cdot P')\varphi_F \cdot (Q_1\varphi_I \otimes \dots \otimes Q_t\varphi_I) \\ &= P\varphi_F \cdot (P'\varphi_F \cdot (Q_1\varphi_I \otimes \dots \otimes Q_t\varphi_I)) \\ &= P\varphi_F \cdot Q\varphi_I, \end{aligned}$$

(If  $P'$  is empty, so is  $P'\varphi_F$ .)

Second, assume  $Q$  is infinite and not eventually disconnected. Write

$$Q = S_0 \cdot \dots \cdot S_{k-1} \cdot (S_k \cdot \dots \cdot S_{k+t-1})^\omega,$$

where each of the  $S_i$  is finite and has no nontrivial serial decomposition. We may also assume that  $k$  is least such that for some  $n > 0$ ,  $S_k \cdot S_{k+1} \cdot \dots = S_{k+n} \cdot \dots$ , and that  $t$  is the least such  $n$ . Write  $P = P_0 \cdot \dots \cdot P_m$  where the  $P_i$  have no nontrivial serial decomposition. Thus, if  $k > 0$ , or if  $k = 0$  and  $P_m \neq S_0$ , then by definition  $(P \cdot Q)\varphi_I = P\varphi_F \cdot Q\varphi_I$ . If  $k = 0$  and  $P_m = S_0$ , we can find integers  $i \leq m$  and  $j \leq t$  such that

$$P \cdot Q = P_0 \cdot \dots \cdot P_{i-1} \cdot (S_j \cdot \dots \cdot S_{t-1} \cdot S_0 \cdot \dots \cdot S_{j-1})^\omega$$

and such that either  $i = 0$  or  $P_{i-1} \neq S_j$ . By repeated applications of (7), it follows again that  $(P \cdot Q)\varphi_I = P\varphi_F \cdot Q\varphi_I$ .

3. If  $Q$  is finite and not eventually disconnected, then  $Q = P_1 \cdot \dots \cdot P_k \cdot b$  as above. The details are routine.
4. If  $P, Q \in I_{A,B}$ , then

$$(P \otimes Q)\varphi_I = P\varphi_I \otimes Q\varphi_I. \quad (12)$$

We use the associativity and commutativity of shuffle. Just write  $P$  and  $Q$  as a parallel product of posets which cannot be further decomposed. Then, if  $P = P_1 \otimes \dots \otimes P_k$  and  $Q = Q_1 \otimes \dots \otimes Q_t$ ,

$$\begin{aligned} (P \otimes Q)\varphi_I &= (P_1 \otimes \dots \otimes P_k \otimes Q_1 \otimes \dots \otimes Q_t)\varphi_I \\ &= (P_1\varphi_I \otimes \dots \otimes P_k\varphi_I) \otimes (Q_1\varphi_I \otimes \dots \otimes Q_t\varphi_I). \quad \square \end{aligned}$$

**COROLLARY 5.2:** *For any pair of disjoint sets  $A, B$ , the free Wilke algebra generated by  $A$  and  $B$  can be represented as the two sorted algebra  $(A^+, A^*B \cup A^u)$ , where  $A^u$  denotes the set of all **ultimately periodic** words in  $A^\omega$ , equipped with the polymorphic concatenation operation and the usual  $\omega$ -operation.*

## 6. $V = L$

We use Theorem 5.1 to show that the variety of shuffle binoids generated by the language structures is the variety of all shuffle binoids. Indeed, we show how to embed the shuffle binoid  $\mathbf{SP}^\omega(A, \emptyset)$  into  $(\Sigma_f, \Sigma_\omega)$ , for a particular alphabet  $\Sigma$ . This fact is sufficient, by Proposition 4.13 above. Recall that no poset in  $I_{A, \emptyset}$  has a maximal element. We use a modified version of a construction introduced in [Tsc94, BÉ96].

Given the set  $A$ , let  $\Sigma_A$  denote the alphabet  $A \times [2] \times \mathbf{N}$ , and use the following notation:

$$\begin{aligned} a_i &:= (a, 1, i) \\ \bar{a}_i &:= (a, 2, i), \end{aligned}$$

for  $i \in \mathbf{N}$  and  $a \in A$ .

**DEFINITION 6.1:**  $h_0$  is the unique shuffle binoid morphism from  $\mathbf{SP}^\omega(A, \emptyset)$  to the language structure  $L(\Sigma_A)$  determined by the functions taking  $a \in A$  to

$$\{a_1\bar{a}_1, a_2\bar{a}_2, a_3\bar{a}_3, \dots\}.$$

Recall that a topological sort of an unlabeled poset  $P$  is a listing of the vertices of  $P$  in such a way that if  $v \leq_P v'$  then  $v$  is listed before  $v'$ . If  $v_1, v_2, \dots$  is a topological sort of the vertices of a labeled poset, then the list  $\lambda(v_1)\lambda(v_2)\dots$ , where  $\lambda$  is the labeling function, is a **trace of the labeled poset**. For example, if  $P$  is the two element poset with unrelated vertices 1, 2, both labeled  $a$ , say, then the vertices of  $P$  have two topological sorts, 1, 2 and 2, 1 but only one trace, namely the word  $aa$ .

If  $Q$  is a finite or infinite poset in  $\mathbf{SP}^\omega(A, \emptyset)$ , the  $h_0$ -image of  $Q$  is the set of all words which are traces of ‘expansions’ of  $Q$ . An expansion  $Q'$  of  $Q$  is obtained by replacing each vertex  $v$  by a two-element chain  $v(1) < v(2)$ ; the ordering on  $Q'$  is:  $v(i) \leq v'(j)$  iff  $v = v'$  and  $i \leq j$  or  $v < v'$  in  $Q$ . If  $v$  is labeled by  $A \in A$  in  $Q$ , then in  $Q'$ , for some  $i \geq 1$ ,  $v(1)$  is labeled

$a_i$  and  $v(2)$  is labeled  $\bar{a}_i$ . (see [BÉ96]). A (finite or infinite) word  $u$  is a **distinguishing trace** of an expansion  $Q'$  of  $Q$  if  $u$  is a trace of  $Q'$  and

$$u = op_1s_1p_2s_2 \dots$$

where:

- Each word  $o, p_i, s_i$  is nonempty.
- Each letter  $a_i, \bar{a}_i$  occurs at most once; if  $\bar{a}_i$  occurs then  $a_i$  occurs earlier.
- The word  $o$  contains the labels of all minimal vertices of  $Q'$ .
- Each word  $p_i$  contains only overlined letters  $\bar{a}_j$ , and each word  $s_i$  contains only nonoverlined letters  $a_j$ .
- If a letter  $\bar{a}_i$  occurs in  $p_j$ , then the letters which occur in  $s_j$  are precisely all of the labels of the immediate successors of the vertex labeled  $\bar{a}_i$  in  $Q'$ .
- If a letter  $a_i$  occurs in  $s_j$ , then the letters which occur in  $p_j$  are precisely all of the letters which label the immediate predecessors of the vertex labeled  $a_i$  in  $Q'$ .

Thus, from a distinguishing trace of  $Q'$ , one can determine both the poset  $Q'$  and the poset  $Q$ .

**PROPOSITION 6.2:** *Any expansion  $Q'$  of a finite or infinite poset  $Q$  in  $\mathbf{SP}^\omega(A, \emptyset)$  such that the vertices of  $Q'$  are labeled by distinct letters has a distinguishing trace.*

*Proof:* This statement was proved for finite posets in [BÉ96]. For infinite posets, the claim may be proved by induction on the number of operations needed to produce the poset. For example, if  $u = op_1s_1 \dots$  and  $v = o'p'_1s'_1 \dots$  are distinguishing traces of expansions  $P'$  of  $P$  and  $Q'$  of  $Q$ , respectively, where  $P$  is finite and  $Q$  is infinite, and if  $u, v$  have no common letters, (which may be assumed), then  $uv$  is a distinguishing trace of  $P' \cdot Q'$  and any expansion of  $P \cdot Q$  has this form. Further, if both  $P$  and  $Q$  are infinite,  $oo'p_1s_1p'_1s'_1p_2s_2p'_2s'_2 \dots$  is a distinguishing trace of  $P' \otimes Q'$  and any expansion of  $P \otimes Q$  has this form. We omit the simple argument for  $P^\omega$ .  $\square$

We extend the **trace order relation** introduced in [BÉ96] to infinite words on the alphabet  $\Sigma_A$ .

First, if  $\varphi : N \rightarrow N$  is any function, we extend  $\varphi$  to a function on the finite and infinite words in the alphabet  $\Sigma_A$  by

$$u\varphi := x_1\varphi x_2\varphi \dots,$$

where  $u = x_1x_2 \dots$

**DEFINITION 6.3:** For two finite or infinite words  $u, v$  on  $\Sigma_A$ , we say  $u \leq v$  according to the trace order if it follows that  $u \leq v$  by applying the subscript, permutation or interchange laws a finite number of times. These laws are defined as follows. We say

1.  $u \leq v$  according to the subscript law if  $u = v\varphi$ , for some  $\varphi : N \rightarrow N$ .
2.  $u \leq v$  according to the permutation law if

$$\begin{aligned} u &= s_0 p_1 s_1 p_2 s_2 \dots \\ v &= s'_0 p'_1 s'_1 \dots \end{aligned}$$

and for each  $i \geq 0$ ,  $s_i, s'_i$  are “open words”, i.e., words on the letters  $a_k, k \geq 1, a \in A$ , and  $p_i, p'_i$  are “closed words”, words on the letters  $\bar{a}_k, k \geq 1, a \in A$ , and  $s'_i$  is a permutation of the letters in  $s_i$  and  $p'_i$  is a permutation of the letters in  $p_i$ . (The permutations depend on  $i$ .)

3.  $u \leq v$  according to the interchange law if there are letters  $a_i, \bar{b}_j$ , for  $a_i \neq b_j$ , such that

$$v = u_1 a_i \bar{b}_j u_2 \quad \text{and} \quad u = u_1 \bar{b}_j a_i u_2. \quad (13)$$

Note that the trace order is a preorder on the finite and infinite words on  $\Sigma_A$ .

The rule (13) is clearly “irreversible”, unlike the subscript law for injective functions  $\varphi$  and the permutation law.

A word  $u \in Qh_0$  is **maximal** (in the trace order) if whenever  $u \leq v$  and  $v \in Qh_0$ , then  $v \leq u$ .

**REMARK 6.4:** For any  $Q \in \mathbf{SP}^\omega(A, B)$ ,  $Qh_0$  is always downward closed. If  $Q$  is finite, every word in  $Qh_0$  is below some maximal word. But this is not the case for some infinite posets. For example, if  $Q = a^\omega \otimes a^\omega$ , a maximal word is

$$a_1 a_2 \bar{a}_1 a_3 \bar{a}_2 a_4 \bar{a}_3 a_5 \bar{a}_4 a_6 \dots$$

but, for example, the word

$$(a_1 a_1 \bar{a}_1 \bar{a}_1)^\omega$$

is not below any maximal word in  $Qh_0$ .

**PROPOSITION 6.5:** For each infinite poset  $Q \in \mathbf{SP}^\omega(A, \emptyset)$ , there is a maximal word  $u$  in  $Qh_0$ , and, moreover, a word  $U \in Qh_0$  is maximal iff  $u$  is a distinguishing trace of an expansion of  $Q$ .

*Proof:* Note that a word  $u$  is maximal in  $Qh_0$  iff each letter in  $\Sigma_A$  occurs at most once and there is no word  $v \in Qh_0$  such that  $u < v$  according to the interchange law. It is clear that any distinguishing trace of an expansion of  $Q$  is maximal in  $Qh_0$ , and we have shown that each expansion of a poset in  $\mathbf{SP}^\omega(A, \emptyset)$  in which the vertices are labeled by distinct letters has a distinguishing trace.

Now assume that

$$u = op_1s_1 \dots$$

is maximal in  $Qh_0$ . Since  $u \in Qh_0$ ,  $u$  is a trace of some expansion  $Q'$  of  $Q$ . We show that  $u$  is a distinguishing trace of  $Q'$ .

First, no letter  $a_i$  occurs more than once, or else there is a word  $v \in Qh_0$  such that  $u \leq v$  via the subscript law and  $v \not\leq u$ . Thus, we may identify a letter, say  $x_i$ , that occurs in  $u$  with the vertex of  $Q'$  labeled  $x_i$ . We will show that if  $\bar{a}_i$  occurs in the closed word  $p_k$ , say, and if  $b_j$  occurs in the open word  $s_k$ , then  $\bar{a}_i$  is an immediate predecessor of  $b_j$  in  $Q'$ . First, if  $\bar{a}_i$  is not below  $b_j$ , then the word  $v$  obtained from  $u$  by interchanging  $\bar{a}_i$  and  $b_j$  is in  $Qh_0$  and  $u$  is not maximal in  $Qh_0$ . If  $\bar{a}_i$  is below  $b_j$  but is not an immediate predecessor of  $b_j$ , there is some letter  $c_t$  with  $\bar{a}_i < c_t < \bar{c}_t < b_j$  in  $Q'$ . But then  $u$  is not a trace of  $Q'$ .

Now, for the converse. Suppose that  $\bar{a}_i$  is an immediate predecessor of  $b_j$  in  $Q'$  and  $b_j$  occurs in  $s_k$ . We show  $\bar{a}_i$  occurs in  $p_k$ . Indeed, since  $u$  is a trace of  $Q'$ ,  $\bar{a}_i$  occurs in  $p_t$ , for some  $t \leq k$ . Suppose, in order to obtain a contradiction, that  $t < k$ . Let  $d_r$  be a letter in  $s_t$ , and  $\bar{c}_s$  be a letter in  $p_k$ . Then, by the above,  $\bar{c}_s$  is an immediate predecessor of  $b_i$  and  $\bar{a}_i$  is an immediate predecessor of  $d_r$ . But, by the  $N$ -condition, it follows that  $\bar{c}_s$  is also an immediate predecessor of  $d_r$ . But then  $u$  is not a trace of  $Q'$ .  $\square$

**COROLLARY 6.6:** *If  $Qh_0 = Q'h_0$ , where  $Q, Q' \in \mathbf{SP}^\omega(A, \emptyset)$ , then  $Q = Q'$ . Thus,  $\mathbf{SP}^\omega(A, \emptyset)$  is isomorphic to a sub shuffle binoid of  $L(\Sigma_A)$ .*  $\square$

**COROLLARY 6.7:**  *$V = \mathbf{L}$ , i.e., the variety of all shuffle binoids is exactly the variety of shuffle binoids generated by the language structures  $L(\Sigma)$ .*  $\square$

According to Proposition 4.13 that there is an embedding

$$\iota : \mathbf{SP}^\omega(A, B) \rightarrow \mathbf{SP}^\omega(A \cup B, \emptyset),$$

and we have just proved that

$$h_0 : \mathbf{SP}^\omega(A \cup B, \emptyset) \rightarrow L(\Sigma_{A \cup B})$$

is an injective shuffle binoid morphism. The composite

$$\mathbf{SP}^\omega(A, B) \rightarrow L_{\Sigma_{A \cup B}}$$

is the unique morphism

$$\begin{aligned} a \in A &\mapsto \{a_i \bar{a}_i : i \geq 1\} \\ b \in B &\mapsto \{b_{i_1} \bar{b}_{i_1} b_{i_2} \bar{b}_{i_2} \dots : i_j \geq 1\}. \end{aligned}$$

A more economical embedding is  $a \in A \mapsto \{a_i \bar{a}_i : i \geq 1\}$  and  $b \in B \mapsto \{b_i^\omega : i \geq 1\}$ . We denote this composite by  $h_0$ .

### 6.1. Decidability

In this section, we discuss the decidability and complexity of the validity of identities in  $V$ .

We note the following fact. For any alphabet  $\Sigma$ , let  $R_f(\Sigma)$  denote the collection of all regular finitary languages in  $\Sigma_f$  and let  $R_\omega(\Sigma)$  denote the collection of all regular  $\omega$ -languages in  $\Sigma_\omega$ .

LEMMA 6.8:  $(R_f(\Sigma), R_\omega(\Sigma))$  is a sub shuffle binoid of  $(\Sigma_f, \Sigma_\omega)$ .

*Proof:* Indeed, when  $L, L' \in \Sigma_f$  are regular, so are  $L \cdot Q', L \otimes Q'$  and  $L^\omega$ . When  $U, V \in \Sigma_\omega$  are both regular, so are  $U \otimes V, L \cdot U$ .  $\square$

For any pair of disjoint sets  $A, B$ , the posets in  $\mathbf{SP}^\omega(A, B)$  have finite width. Thus, one may obtain traces which characterize a poset without the need for infinitely many subscripts, but only as many as the width of the poset.

For each  $n \geq 1$ , define the morphism  $h_n$  as the unique shuffle binoid morphism from  $\mathbf{SP}^\omega(A, B)$  to the language structure  $L(\Sigma_{A \cup B})$  such that

$$\begin{aligned} ah_n &= \{a_1 \bar{a}_1, a_2 \bar{a}_2, \dots, a_n \bar{a}_n\}, \quad a \in A \\ bh_n &= \{b_i^\omega : 1 \leq i \leq n\}, \quad b \in B. \end{aligned}$$

PROPOSITION 6.9: Suppose that  $Q, Q'$  are posets in  $\mathbf{SP}^\omega(A, B)$  of width at most  $n$ . If  $Qh_n = Q'h_n$ , then  $Q = Q'$ .  $\square$

COROLLARY 6.10: There is an algorithm to determine, given two sorted shuffle binoid terms  $s, t$  whether  $s = t$  holds in all shuffle binoids.

*Proof:* From the terms  $s, t$ , we can determine the maximum width, say  $n$ , of the two posets they denote. We then apply the morphism  $h_n$  to these posets, obtaining two regular languages, or  $\omega$ -languages, by Lemma 6.8. Since the equivalence problem for regular languages and regular  $\omega$ -languages is decidable (see [WT90]), the theorem follows.  $\square$

We can say more about the complexity of a decision procedure. Using a tree representation of the free bi-semigroups, and a result in [Kuc90], it was shown in [BÉ96] that the equational theory of bi-semigroups is decidable in  $O(n \log n)$  time. We now outline a  $O(n^2 \log n)$  algorithm to decide for any two sorted shuffle binoid terms  $s, t$ , whether  $s = t$  holds in all shuffle binoids, where  $n$  denotes the length of the equation  $s = t$ . In the first step of the algorithm, we transform each side of the equation to a directed **alternating tree** whose non-leaf vertices have labels in the set  $\{\cdot, \otimes, \omega\}$  and whose leaves are labeled by sorted variables. Moreover, any vertex labeled by  $\cdot$  or  $\otimes$  has at least two successors and no two consecutive vertices are labeled by the same symbol. Moreover, the successors of any a vertex labeled  $\cdot$  are linearly ordered. This transformation requires linear time. The trees satisfy some further restrictions, e.g., no descendant of a vertex labeled  $\omega$  is labeled  $\omega$ . These restrictions are due to the fact that the trees come from sorted binoid terms. In the second step, we reduce the trees by repeatedly replacing subtrees of the form

$$\omega(\cdot(t_1, \dots, t_k, \dots, t_1, \dots, t_k)) \quad (14)$$

by the tree

$$\omega(\cdot(t_1, \dots, t_k)),$$

or by

$$\omega(t_1),$$

when  $k = 1$ , and subtrees

$$\cdot(t_1, \dots, t_k, t, \omega(\cdot(s_1, \dots, s_m, t))) \quad (15)$$

by

$$\cdot(t_1, \dots, t_k, \omega(\cdot(t, s_1, \dots, s_m))),$$

or by

$$\omega(\cdot(t, s_1, \dots, s_m))$$

when  $k = 0$ . The resulting **reduced trees** do not have any subtree of the form (14) or (15). Since isomorphism of trees can be checked in  $O(n \log n)$  time (see [Kuc90]) and since at most  $O(n)$  reductions suffice, the second step requires  $O(n^2 \log n)$  time. Finally, in the third step of the algorithm, we check whether the reduced trees obtained after the second step are isomorphic.

PROPOSITION 6.11: *The equational theory of shuffle binoids is decidable in polynomial time.*  $\square$

REMARK 6.12: In the same way, the equational theory of binoids is also decidable in polynomial time.

REMARK 6.13: Identifying any two terms that differ only up to the bi-semigroup identities, the rewriting system consisting of the directed rules

$$\begin{aligned} (t^n)^\omega &\rightarrow t^\omega \\ tt^\omega &\rightarrow t^\omega \\ t(st)^\omega &\rightarrow (ts)^\omega, \end{aligned}$$

where  $t$  and  $s$  are terms and  $n > 1$ , is complete, i.e., confluent and noetherian. The reduced trees mentioned above correspond to the normal forms of this rewriting system.

## 7. NO FINITE AXIOMATIZATION

We show, by modifying an argument in [ÉB95] that there is no finite axiomatization of the variety  $V$ . Indeed, by the compactness theorem, if there is any finite axiomatization, then there is a finite subset of the identities (1)-(8) which axiomatizes the variety of all shuffle binoids  $(F, I)$ , where now the variables  $a, b, c$  range over  $F$  and  $u, v, w$  range over  $I$ .

THEOREM 7.1: *For any finite subset  $E$  of the identities (1)-(8) there is a model of  $E$  which fails to satisfy all of the identities (8). Indeed, for any prime  $p$  there is a model  $M_p = (F_p, I_p)$  of the identities (1)-(7) and the power identities*

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

*for all  $n < p$ , such that the identity  $(x^p)^\omega = x^\omega$  fails in  $M_p$ . Thus,  $\mathbf{L}$  does not have a finite axiomatization.*

*Proof:* Fix a prime  $p$ . Let  $M_p = (F_p, I_p)$  be the following structure.  $F_p$  consists of all positive integers, and let  $I_p$  consist of the set of positive integers  $n$  satisfying the implication

$$q|n \Rightarrow q \geq p, \tag{16}$$

for all primes  $q$ . Thus  $I_p$  contains 1 and all numbers  $n$  whose prime factorization contains no prime less than  $p$ . Lastly, we put an additional element  $\top$  in  $I_p$ . If  $n$  is a positive integer, let  $\rho(n)$  be the quotient of  $n$  by the product of all primes  $< p$  which occur in the prime factorization of  $n$ , so that  $\rho(n)$  is the largest quotient of  $n$  which belongs to  $I_p$ . The operations on  $M_p$  are defined as follows, for  $a, b \in F_p, u, v \in I_p, u, v \neq \top$  :

$$\begin{aligned} a \cdot b &:= a + b \\ a \otimes b &:= a + b \\ a^\omega &:= \rho(a) \\ a \cdot u &:= u \\ u \otimes v &:= \top \\ a \cdot \top &:= \top \\ u \otimes \top &:= \top \otimes u = \top \otimes \top = \top. \end{aligned}$$

It is clear that the identities (1)-(7) hold. However, for any positive integers  $a, n$ ,

$$(a^n)^\omega = \rho(na) = \rho(\overbrace{a + \dots + a}^n)$$

and  $a^\omega = \rho(a)$ , but  $\rho(na) = \rho(a)$  iff every prime divisor of  $n$  is less than  $p$ . □

### 8. ORDERED SHUFFLE BINOIDS

Note that if  $L_1 \subseteq L_2$  are finite languages, then  $L_1^\omega \subseteq L_2^\omega$ . Thus, all of the shuffle binoid operations on languages preserve the subset order. We consider now the class of all **ordered shuffle binoids**, which are two-sorted algebras  $B = (F, I, \leq_F, \leq_I)$  such that both  $(F, \leq_F)$  and  $(I, \leq_I)$  are posets, and  $(F, I)$  is a shuffle binoid, and all operations preserve the order. For example, for  $a_1, a_2 \in F, x, x', y, y' \in F$  or  $x, x', y, y' \in I$

$$\begin{aligned} a_1 \leq_F a_2, x \leq x' &\Rightarrow a_1 \cdot x \leq a_2 \cdot x' \\ a_1 \leq_F a_2 &\Rightarrow a_1^\omega \leq_I a_2^\omega \\ x \leq x', y \leq y' &\Rightarrow x \otimes y \leq y \otimes y', \end{aligned}$$

where we omit the subscript on  $\leq$ , since it depends on the type of  $x, x'$ , etc. We put an order on each component of  $\mathbf{SP}^\omega(A, B)$  using the morphism  $h_0$  : for  $P_1, P_2 \in \mathbf{SP}(A)$ ,  $P_1 \leq_F P_2$  if  $P_1 h_0 \subseteq P_2 h_0$ ; similarly, if  $Q_1, Q_2$  are infinite posets in  $\mathbf{SP}^\omega(A, B)$ ,  $Q_1 \leq_I Q_2$  if  $Q_1 h_0 \subseteq Q_2 h_0$ .

For ease of notation, an ordered shuffle binoid will be denoted  $(F, I, \leq)$ .

In [BÉ96] it is shown that for any  $P, P' \in F_A$ , if  $P h_0 \subseteq P' h_0$ , then  $P g \subseteq P' g$ , for any structure preserving morphism  $g : F_A \rightarrow L_\Sigma$ , for any alphabet  $\Sigma$ . An extension of this argument shows that

LEMMA 8.1: *For any  $P, P'$  in  $\mathbf{SP}^\omega(A, B)$ , if  $P h_0 \subseteq P' h_0$ , then for any shuffle binoid morphism  $g : \mathbf{SP}^\omega(A, B) \rightarrow (\Sigma_f, \Sigma_\omega)$ ,  $P g \subseteq P' g$ .  $\square$*

DEFINITION 8.2: *We let  $\mathbf{L}_{\leq}$  denote the variety of ordered shuffle binoids generated by all language structures  $(\Sigma_f, \Sigma_\omega, \subseteq)$ .*

From Lemma 8.1, we obtain the following theorem.

THEOREM 8.3: *The ordered shuffle binoid  $(F_A, I_{A,B}, \leq)$  is freely generated in  $\mathbf{L}_{\leq}$  by  $A$  and  $B$ .*

We omit the argument to establish the following Lemma.

LEMMA 8.4: *If  $P, Q$  in  $\mathbf{SP}^\omega(A, B)$  have width at most  $n$  and  $P h_n \subseteq Q h_n$ , then  $P h_0 \subseteq Q h_0$ .  $\square$*

COROLLARY 8.5: *There is a decision procedure to determine whether  $t \leq t'$  is valid in the variety  $\mathbf{L}_{\leq}$ .*

Indeed, using  $h_n$ , the problem is reduced to the inclusion problem for regular languages.

## 9. OPEN QUESTIONS

1. One might wish to axiomatize those two-sorted language structures in which one may shuffle finite languages with infinite ones (in addition to the shuffle binoid operations). This operation is clearly meaningful for labeled posets, and is both associative and commutative. For posets, these are the only axioms one needs to add, but we are not sure that the same may be said of languages, although we suspect that this is the case. Indeed, we can show that a class of labeled posets is free in the corresponding variety, but we cannot show that the embedding used above remains injective for this larger class of posets.

2. What is an axiomatization of the language structures of shuffle binoids enriched by the  $\omega$ -shuffle operation  $L \mapsto L \otimes L \otimes \dots$ ? The corresponding operation is meaningful on posets, but widths become infinite. This fact makes the characterization of the free structures difficult.
3. What are the free structures in the variety generated by the structures obtained by enriching the language shuffle binoids with a polymorphic binary union operation?

## 10. ACKNOWLEDGMENT

This research has been carried out while the authors were visiting each other's departments in the spring of 1998 and in part while the first author was visiting LIAFA at the University of Paris 7, in May, 1998. He would like to thank C. Choffrut, C. Frougny, J.-E. Pin and especially Irene Guessarian for their hospitality.

## REFERENCES

- [Blo76] S. L. BLOOM, Varieties of ordered algebras. *Journal of Computer and System Sciences*, Vol. 45, 1976, pp. 200-212.
- [BÉ95] S. L. BLOOM and Z. ÉSIK, Nonfinite axiomatizability of shuffle inequalities. In *Proceedings of TAPSOFT'95*, volume 915 of *Lecture Notes in Computer Science*, 1995, pp. 318-333.
- [BÉ96] S. L. BLOOM and Z. ÉSIK, Free shuffle algebras in language varieties. *Theoretical Computer Science*, Vol. 163, 1996, pp. 55-98.
- [BÉ97] S. L. BLOOM and Z. ÉSIK, Axiomatizing shuffle and concatenation in languages. *Information and Computation*, Vol. 139, 1997, pp. 62-91.
- [BÉSt] S. L. BLOOM, Z. ÉSIK and Gh. STEFANESCU, Equational theories of relations and regular sets. In *Proc. of Words, Languages and Combinatorics, II*, M. ITO and M. JÜRGENSEN Eds., Kyoto, 1992 World Scientific, 1994, pp. 40-48.
- [Bof90] M. BOFFA, Une remarque sur les systèmes complets d'identités rationnelles, *Theoret. Inform. Appl.*, Vol. 24, 1990, pp. 419-423.
- [Bof95] M. BOFFA, Une condition impliquant toutes les identités rationnelles, *Theoret. Inform. Appl.*, Vol. 29, 1995, pp. 515-518.
- [ÉB95] Z. ÉSIK and L. BERNÁTSKY, Scott induction and equational proofs, in: *Mathematical Foundations of Programming Semantics'95*, ENTCS, Vol. 1, 1995.
- [ÉBrt95] Z. ÉSIK and M. BERTOL, Nonfinite axiomatizability of the equational theory of shuffle. In *Proceedings of ICALP'95*, volume 944 of *Lecture Notes in Computer Science*, 1995, pp. 27-38.
- [És98] Z. ÉSIK, Group axioms for iteration, *Information and Computation*, to appear.
- [Gis84] J. L. GISCHER, Partial Orders and the Axiomatic Theory of Shuffle. *PhD thesis*, Stanford University, Computer Science Dept., 1984.

- [Gis88] J. L. GISCHER, The equational theory of pomsets. *Theoretical Computer Science*, Vol. 61, 1988, pp. 199-224.
- [Gra81] J. GRABOWSKI, On partial languages. *Fundamenta Informatica*, Vol. IV(2), 1981, pp. 427-498.
- [Koz94] D. KOZEN, A completeness theorem for Kleene algebras and the algebra of regular events, *Information and Computation*, Vol. 110, 1994, pp. 366-390.
- [Kr91] D. KROB, Complete systems of B-rational identities, *Theoretical Computer Science*, Vol. 89, 1991, pp. 207-343.
- [Kuc90] L. KUCERA, Combinatorial Algorithms, Adam Hilger (Bristol and Philadelphia), 1990.
- [Pra86] V. PRATT, Modeling concurrency with partial orders. *Internat. J. Parallel Processing*, Vol. 15, 1986, pp. 33-71.
- [WT90] W. THOMAS, Automata on infinite objects. In *Handbook of Theoretical Computer Science*, Vol. B, *Formal Models and Semantics*, MIT Press, 1990, pp. 133-192.
- [Tsc94] Steven T. TSCHANTZ, Languages under concatenation and shuffling, *Mathematical Structures in Computer Science*, Vol. 4, 1994, pp. 505-511.
- [VTL81] J. VALDES, R. E. TARJAN and E. L. LAWLER, The recognition of series-parallel digraphs. *SIAM Journal of Computing*, Vol. 11(2), 1981, pp. 298-313.
- [Wil93] T. WILKE, An algebraic theory for regular languages of finite and infinite words. *International Journal of Algebra and Computation*, Vol. 3, 1993, pp. 447-489.
- [Wil91] T. WILKE, An Eilenberg Theorem for  $\infty$ -languages. In "Automata, Languages and Programming", *Proc. of 18th ICALP Conference*, Vol. 510 of *Lecture Notes in Computer Science*, 1991, pp. 588-599.