

## ON THE EXTENSION PROBLEM FOR PARTIAL PERMUTATIONS

K. AUINGER AND B. STEINBERG

(Communicated by Stephen D. Smith)

ABSTRACT. A family of pseudovarieties of solvable groups is constructed, each of which has decidable membership and undecidable extension problem for partial permutations. Included are a pseudovariety  $\mathbf{U}$  satisfying no non-trivial group identity and a metabelian pseudovariety  $\mathbf{Q}$ . For each of these pseudovarieties  $\mathbf{V}$ , the inverse monoid pseudovariety  $\mathbf{SI}*\mathbf{V}$  has undecidable membership problem. As a consequence, it is proved that the pseudovariety operators  $*$ ,  $**$ ,  $\textcircled{w}$ ,  $\diamond$ ,  $\diamond_n$ , and  $\mathbf{P}$  do not preserve decidability. In addition, several joins, including  $\mathbf{A} \vee \mathbf{U}$ , are shown to be undecidable.

### 1. INTRODUCTION

A fundamental question in mathematics is the following: given a mathematical structure  $X$  and a set of partial automorphisms  $\mathcal{S}$  of  $X$ , is it possible to find a superstructure  $Y \supseteq X$  and a set of automorphisms  $\mathcal{T}$  extending the partial automorphisms of  $\mathcal{S}$ , possibly subject to some constraints on  $Y$  and  $\mathcal{T}$ . As an example of the ubiquity of this problem, consider group theory: given a group  $G$  and a collection  $\{\varphi_i \mid i \in I\}$  of partial automorphisms of  $G$ , Higman, Neumann and Neumann [11] constructed a larger group  $H$  in which these partial automorphisms are induced by (inner) automorphisms of  $H$ . The construction is now known as an *HNN-extension*. A variation of the problem is especially important in finite model theory. Hrushovski [12] studied this problem for the class of all finite graphs with the constraint that  $Y$  be finite and showed that appropriate  $Y$  and  $\mathcal{T}$  can always be found. This was later generalized to exclusion classes of arbitrary relational structures by Herwig and Lascar [10]. Further examples can be found in the book of Lawson [14].

In the present paper, we shall deal with the following variant. Let  $\mathbf{H}$  be a pseudovariety of groups (that is, a class of finite groups closed under taking finite direct products, subgroups and quotients) with decidable membership problem. The *extension problem for partial permutations for  $\mathbf{H}$*  (also called the extension problem for  $\mathbf{H}$ , for short) asks for an algorithm to determine, given a finite set  $X$  and a set  $\mathcal{S}$  of partial permutations of  $X$ , whether there exists a finite superset

---

Received by the editors October 31, 2001 and, in revised form, April 10, 2002.

2000 *Mathematics Subject Classification*. Primary 20M07, 20M18, 20M35, 20B05, 20D10.

The authors gratefully acknowledge support from INTAS project 99–1224. The second author was supported in part by FCT through the *Centro de Matemática da Universidade do Porto*, and by the FCT and POCTI approved project POCTI/32817/MAT/2000 in participation with the European Community Fund FEDER.

$Y \supseteq X$  and a set  $\mathcal{T}$  of permutations of  $Y$  extending those of  $\mathcal{S}$  such that  $\mathcal{T}$  generates a group in  $\mathbf{H}$ . Equivalently, one asks for an algorithm to determine whether a finite *inverse automaton* [33] can be embedded in a permutation automaton with transition group in  $\mathbf{H}$ . Note that, if  $\mathbf{H}$  has decidable membership then the set of these automata is recursively enumerable.

For the pseudovariety  $\mathbf{G}$  of all finite groups, the problem is trivial since one can always take  $Y = X$  and extend the partial permutations to total permutations; this is used implicitly by Stallings [32] and McAlister [17]. Margolis, Sapir, and Weil studied this problem systematically in [15] for more general pseudovarieties. In particular, they showed that the extension problem for  $\mathbf{H}$  is decidable if there exists a uniform algorithm to determine membership for the closure of a finitely generated subgroup of a free group  $F$  in the pro- $\mathbf{H}$  topology. Ribes and Zalesskii [21] provided such an algorithm for the pro- $p$  topology (refined to polynomial time in [15]); therefore the extension problem is decidable for the pseudovariety of all finite  $p$ -groups  $\mathbf{G}_p$ . By the analogous result for the pseudovariety of all finite nilpotent groups  $\mathbf{G}_{nil}$  [15], the extension problem is decidable for  $\mathbf{G}_{nil}$ . It follows from results of the second author [26] that the extension problem is decidable for each pseudovariety of Abelian groups  $\mathbf{H}$  with decidable membership. The extension problem for the pseudovariety of all finite solvable groups is open and is considered to be one of the most important open questions in finite monoid theory. A solution would have important consequences in logic; see Straubing and Thérien [34].

Our main result is the construction of a family of pseudovarieties of solvable groups, each of which has decidable membership problem but undecidable extension problem. Among these are: a pseudovariety  $\mathbf{U}$  which does not satisfy any non-trivial group identity; a metabelian pseudovariety  $\mathbf{Q} \subseteq \mathbf{U}$  — this is in marked contrast to the aforementioned situation for Abelian pseudovarieties; for each  $n \geq 3$  a pseudovariety  $\mathbf{Q}_n$  consisting of solvable groups of derived length at most  $n$  (and containing a group of derived length equal to  $n$ ). As an application, we obtain many undecidability results for the theory of finite monoid pseudovarieties, including that virtually all frequently considered pseudovariety operators do not preserve decidability. Let us put this result in context.

In [1], Albert, Baldinger and Rhodes presented a striking example of a finite set of identities  $E$  for which the join  $[[E]] \vee \mathbf{Com}$  of  $[[E]]$ , the pseudovariety defined by  $E$ , with the pseudovariety  $\mathbf{Com}$  of all commutative monoids has undecidable membership — clearly,  $\mathbf{Com}$  and  $[[E]]$  do have decidable membership. Some generalizations have been obtained by Sapir; the reader is referred to the interesting survey on algorithmic problems in algebra by Kharlampovich and Sapir [13]. Similar examples (with slightly different choices of  $E$ ) have been constructed by Rhodes [22] showing that the semidirect, the two-sided semidirect, and the Mal'cev products of two pseudovarieties with decidable membership may no longer be decidable. Also, Rhodes proved [22] that the 2-fold Schützenberger product operator  $\diamond_2$  applied to a decidable pseudovariety (of the above sort) can yield an undecidable pseudovariety (see Pin [19, 20] for relevant definitions). Rhodes and the second author [23] showed that  $[[E]]$  also has undecidable pointlike sets. All these examples use the fact that it is undecidable which identities are satisfied by the members of  $[[E]]$ . None of the pseudovarieties in the above undecidability results are pseudovarieties of groups.

For the decidable pseudovariety  $\mathbf{U}$ , we shall find plenty of examples of decidable pseudovarieties of monoids [semigroups]  $\mathbf{V}$  for which  $\mathbf{V} * \mathbf{U} = \mathbf{V} ** \mathbf{U}$ ,  $\mathbf{V} \circledast \mathbf{U}$ ,

and  $\mathbf{V} \vee \mathbf{U}$  are undecidable. Amongst these are:  $\mathbf{Sl} * \mathbf{U}$ ,  $\mathbf{J} * \mathbf{U}$ ,  $\mathbf{J}^{(m)} \mathbf{U}$ ,  $\mathbf{R} * \mathbf{U}$ ,  $\mathbf{L} * \mathbf{U}$ ,  $\mathbf{DA} * \mathbf{U}$  (note that, for the latter three, the semidirect product  $*$  may be replaced with the Mal'cev product, but  $\mathbf{J} * \mathbf{U} \neq \mathbf{J}^{(m)} \mathbf{U}$  by [6]),  $\mathbf{Com} \vee \mathbf{U}$  and  $\mathbf{A} \vee \mathbf{U}$ . For the monoid  $C_{2,1} = \langle a \mid a^2 = 0 \rangle = \{1, a, a^2 = 0\}$ , we also show that  $\langle C_{2,1} \rangle \vee \mathbf{U}$  is undecidable. Moreover, all the pseudovarieties  $\diamond_n \mathbf{U}$  are undecidable as is the full Schützenberger product  $\diamond \mathbf{U}$  (for relevant definitions, consult [19, 20]). The same results hold for  $\mathbf{U}$  replaced with  $\mathbf{Q}$  or  $\mathbf{Q}_n$ . The results imply, in particular, that it is hopeless to attempt to establish the decidability of the dot depth hierarchy via a general result on the preservation of decidability by the Schützenberger operator  $\diamond$  (see [19, 20] for more information on this open problem in language theory). In addition, the power pseudovariety  $\mathbf{PU}$  is undecidable (see Almeida [2] for the relevant definitions). Analogous results are obtained replacing  $\mathbf{U}$  with  $\mathbf{LU}$ .

## 2. THE CONSTRUCTION

Let us first state two straightforward facts. (With the exception of free groups, all semigroups and groups in this paper are finite.)

**Lemma 2.1.** *Let  $G$  and  $H$  be groups of co-prime order; then, for each  $(g, h) \in G \times H$ , there is a positive integer  $n$  such that  $g^n = g$  and  $h^n = 1$ .*

This implies that each subgroup  $K$  of  $G \times H$  (including each normal one) is of the form  $K = G_1 \times H_1$  with  $G_1 \leq G$  and  $H_1 \leq H$ . In particular, each quotient of  $G \times H$  is of the form  $G/G_1 \times H/H_1$ . An immediate consequence is the following.

**Lemma 2.2.** *Let  $\mathbf{H}_n$ ,  $n \in \mathbb{N}$ , be pseudovarieties of groups with pairwise trivial intersection. Then the join*

$$\bigvee_{n \in \mathbb{N}} \mathbf{H}_n$$

*consists of all finite direct products  $H_{n_1} \times H_{n_2} \times \dots \times H_{n_k}$  with  $H_{n_i} \in \mathbf{H}_{n_i}$  and  $\{n_1, \dots, n_k\}$  a finite subset of  $\mathbb{N}$ .*

Let  $\mathbf{G}_{com}$  be the pseudovariety of all Abelian groups; for a prime  $p$ , let  $\mathbf{G}_p$  be the pseudovariety of all  $p$ -groups,  $\mathbf{G}_{p,com} = \mathbf{G}_p \cap \mathbf{G}_{com}$  and  $\mathbf{Ab}_p$  the pseudovariety of all Abelian groups of exponent  $p$ . For two pseudovarieties of groups  $\mathbf{K}, \mathbf{L}$ , let  $\mathbf{K} * \mathbf{L}$  denote the pseudovariety generated by all semidirect products of members of  $\mathbf{K}$  by members of  $\mathbf{L}$ . By the theorem of Kaloujnine-Krasner (see Eilenberg [8]),  $\mathbf{K} * \mathbf{L}$  is the class of all groups which are extensions of a group in  $\mathbf{K}$  by a group in  $\mathbf{L}$ . In particular, if  $\mathbf{K}$  and  $\mathbf{L}$  have decidable membership, then so does  $\mathbf{K} * \mathbf{L}$ .

We observe that the existence of a recursively enumerable subset of  $\mathbb{N}$  which is not recursive is the same as asserting that there exists a computable injective function  $f : \mathbb{N} \rightarrow \mathbb{N}$  for which the image of  $f$  is not recursive.

Let  $p_1 < p_2 < \dots$  be the sequence of all primes in increasing order. Let  $A$  consist of the primes with odd index and  $B$  the primes with even index. Since  $A$  and  $B$  are isomorphic to  $\mathbb{N}$  by computable isomorphisms, there exists an injective recursive function  $f : A \rightarrow B$  whose range  $C = f(A)$  is not recursive. Set  $D = B \setminus C$ . Observe that  $A \cup C$  is recursively enumerable, but not recursive, and that  $D$  is not recursively enumerable and therefore not recursive.

Define the pseudovariety  $\mathbf{U}$  by

$$\mathbf{U} = \bigvee_{p \in A} \mathbf{G}_p * \mathbf{G}_{f(p),com} \vee \bigvee_{p \in D} \mathbf{G}_{p,com}.$$

For convenience, set  $\mathbf{U}_p = \mathbf{G}_p * \mathbf{G}_{f(p),com}$  and  $\mathbf{V}_p = \langle \mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/f(p)\mathbb{Z} \rangle$  for  $p \in A$ , and put

$$\mathbf{Q} = \bigvee_{p \in A} \mathbf{V}_p \vee \bigvee_{p \in D} \mathbf{Ab}_p.$$

Note that  $\mathbf{V}_p \subseteq \mathbf{U}_p$  and  $\mathbf{V}_p$  has decidable membership since it is finitely generated. If in the definition of  $\mathbf{Q}$ , each  $\mathbf{V}_p$  is replaced with  $\mathbf{Ab}_p * \dots * \mathbf{Ab}_p * \mathbf{Ab}_{f(p)}$  ( $\mathbf{Ab}_p$  taken  $n - 1$  times), then one gets a pseudovariety  $\mathbf{Q}_n$  of groups of derived length at most  $n$  (containing groups with derived length equal to  $n$ ), and  $\mathbf{Q} \subseteq \mathbf{Q}_n \subseteq \mathbf{U}$  for all  $n \geq 3$ . All results stated in this paper about  $\mathbf{Q}_n$  assume  $n \geq 3$ .

**Proposition 2.3.** *The pseudovarieties  $\mathbf{U}$ ,  $\mathbf{Q}$  and  $\mathbf{Q}_n$  have decidable membership.*

*Proof.* We handle the case of  $\mathbf{U}$ , the others being analogous. Let  $G$  be a group and let  $a_1, \dots, a_k$  be those prime divisors of  $|G|$  which are in  $A$ , and  $d_1, \dots, d_n$  those which are in  $B \setminus \{f(a_1), \dots, f(a_k)\}$ . Then, by Lemma 2.2,  $G \in \mathbf{U}$  if and only if

$$G \in \bigvee_{i=1}^k \mathbf{U}_{a_i} \vee \bigvee_{j=1}^n \mathbf{G}_{d_j,com}$$

and the latter has decidable membership, again by Lemma 2.2 (or using [28, Corollary 14.3]). □

The intuition behind this construction is that, although each of these pseudovarieties has decidable membership, it is undecidable whether a given group  $G$  admits a “good” co-extension within the respective pseudovariety. More precisely, this means the following.

**Lemma 2.4.** *Let  $\mathbf{V}$  be any of  $\mathbf{U}$ ,  $\mathbf{Q}_n$  or  $\mathbf{Q}$ .*

- (1) *For each  $p \in A \cup C$  there exists a prime  $q$  so that each co-extension of  $\mathbb{Z}/p\mathbb{Z}$  by an elementary Abelian  $q$ -group is in  $\mathbf{V}$ .*
- (2) *For each  $p \in D$ , if  $G$  is an Abelian  $p$ -group in  $\mathbf{V}$ , then each co-extension of  $G$  in  $\mathbf{V}$  is of the form  $K \times H$  where  $H$  is an Abelian  $p$ -group co-extending  $G$  and  $|K|$  is co-prime with  $p$ .*

Notice also that the set of quasi-identities of the form

$$x^n = 1 \rightarrow xy = yx \quad (n \in \mathbb{N})$$

satisfied by all members of  $\mathbf{U}$  [respectively,  $\mathbf{Q}$ ,  $\mathbf{Q}_n$ ] is not recursive.

### 3. THE EXTENSION PROBLEM

The main result of the paper is the following.

**Theorem 3.1.** *The extension problems for  $\mathbf{U}$ ,  $\mathbf{Q}$  and  $\mathbf{Q}_n$  are undecidable.*

*Proof.* For each prime  $p$  we construct a finite inverse automaton  $\mathcal{A}_p$  as follows. The state set consists of the elements  $q_0, \dots, q_{p-1}, r_0, \dots, r_{p-1}, s$ . There are edges labeled by  $a$  from  $q_i$  to  $q_{i+1}$  and  $r_i$  to  $r_{i+1}$  (the indices taken mod  $p$ ). In addition, there are two edges labeled by  $b$ : one from  $q_0$  to  $r_0$ , the other from  $q_1$  to  $s$ . All edges are reversible to get an inverse automaton: one can traverse them backward by application of the appropriate letter from  $\{a^{-1}, b^{-1}\}$ . See Figure 1 for the case  $p = 5$ .

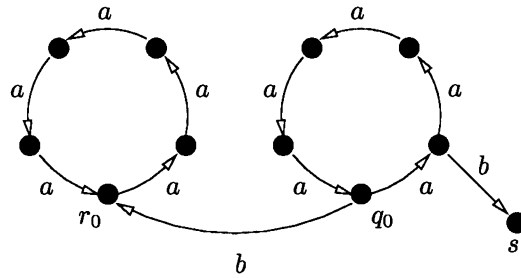


FIGURE 1. The inverse automaton  $\mathcal{A}_5$ .

We prove that if  $p \in A \cup C$ , then  $\mathcal{A}_p$  embeds in a permutation automaton over  $\mathbf{V}_q$  for some  $q$ , while if  $p \in D$ , then  $\mathcal{A}_p$  does not embed in a permutation automaton over  $\mathbf{U}$ .

Suppose that  $p \in A \cup C$ . Then there exists  $q \in A$  such that  $\mathbb{Z}/p\mathbb{Z} \in \mathbf{V}_q$ . Indeed, if  $p \in A$ , then we may take  $p = q$ ; if  $p \in C$ , then  $p = f(q)$  for some  $q \in A$  and so  $\mathbb{Z}/p\mathbb{Z} \in \mathbf{V}_q$ . Let  $C_p = \langle x \mid x^p = 1 \rangle$  be a cyclic group of order  $p$ , written multiplicatively, and  $V$  be the additive group of the group ring

$$\mathbb{Z}/q\mathbb{Z}C_p = \{ \lambda_0 + \lambda_1x + \dots + \lambda_{p-1}x^{p-1} \mid \lambda_i \in \mathbb{Z}/q\mathbb{Z} \}.$$

Let  $G = V \rtimes C_p$  be the semidirect product with respect to the natural left action of  $C_p$  on  $V$ . Then  $G$  is isomorphic to the wreath product  $\mathbb{Z}/q\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$  and so  $G \in \mathbf{V}_q$ . Consider the subgroup  $H = \langle a, b \rangle$  of  $G$  generated by  $a = (0, x)$  and  $b = (1, 1)$ . Then, for  $n = 0, \dots, p - 1$ , all the elements  $a^n, ba^n$  and  $ab$  are distinct from each other since  $a^n = (0, x^n)$ ,  $ba^n = (1, 1)(0, x)^n = (1, x^n)$  and  $ab = (0, x)(1, 1) = (x, x)$ ; moreover,  $a^p = (0, 1)$ , the identity of  $H$ . It follows that  $\mathcal{A}_p$  embeds in the Cayley graph of  $H$  with respect to  $\{a, b\}$ . This graph is a permutation automaton with transition group  $H \in \mathbf{V}_q$ .

Now let  $p \in D$ ; we show that  $\mathcal{A}_p$  does not embed in a permutation automaton with transition group in  $\mathbf{U}$ . Suppose, by contrast, that  $\mathcal{A}_p$  does embed in a permutation automaton  $\mathcal{P}$  with transition group  $G \in \mathbf{U}$ . We may assume that  $G$  is generated by  $a$  and  $b$ . Then, by Lemma 2.2,  $G = K \times H$  with  $H$  an Abelian  $p$ -group and the order of  $K$  co-prime with  $p$ . Suppose that  $a = (k, h)$ . Since  $a$  labels a circuit of length  $p$  in  $\mathcal{A}_p$ , and hence in  $\mathcal{P}$ , the order  $ord_G(a)$  of  $a$  in  $G$  must be a non-zero multiple of  $p$ ; therefore  $h \neq 1$ .

By Lemma 2.1, there exists an integer  $l$  such that  $k^l = 1$  and  $h^l = h$ . Consequently,  $a^l = (1, h)$  is central in  $G$  and therefore  $a^l$  commutes with  $b$  in  $G$ . On the other hand, from  $h^l = h$  it follows that  $l \equiv 1 \pmod{p^n}$ , where  $p^n = ord_H(h)$ , whence  $l \equiv 1 \pmod{p}$ . Therefore, when reading  $a^l b$  from  $q_0$  in  $\mathcal{A}_p$ , one ends up at  $s$  while  $q_0 b a^l = r_1$ . Since  $s \neq r_1$  this is a contradiction.  $\square$

According to [15, 30], to say that an inverse automaton  $\mathcal{A}$  embeds in a permutation automaton over a group  $G$  in a pseudovariety  $\mathbf{H}$  of groups is the same as saying that the transition inverse monoid  $I$  of  $\mathcal{A}$  is in the inverse monoid pseudovariety  $\mathbf{SI} * \mathbf{H}$  (that is the class of all inverse monoids which have an  $E$ -unitary cover over  $\mathbf{H}$ ). We have thus proved the following.

**Theorem 3.2.** *Each inverse monoid pseudovariety in the interval  $[\mathbf{SI} * \mathbf{Q}, \mathbf{SI} * \mathbf{U}]$  has undecidable membership problem.*

Taking into account that  $\mathbf{Q}$  is metabelian, this is in marked contrast to the results of [26] which imply that, for each decidable pseudovariety of Abelian groups  $\mathbf{H}$ , the extension problem for  $\mathbf{H}$  is decidable (and thus membership in  $\mathbf{SI} * \mathbf{H}$ , as well).

Let  $\mathcal{A}$  be a connected finite inverse automaton over an alphabet  $X$  and  $q$  a vertex of  $\mathcal{A}$ . Then the fundamental group  $\pi_1(\mathcal{A}, q)$  is a finitely generated subgroup of the free group on  $X$ . If, for a pseudovariety of groups  $\mathbf{H}$ , one can effectively determine membership in the pro- $\mathbf{H}$  closure of  $\pi_1(\mathcal{A}, q)$ , then one can decide whether  $\mathcal{A}$  embeds in a permutation automaton with transition group in  $\mathbf{H}$  [30, Theorem 5.12] (which extends the case of reduced automata considered in [15]). One easily computes  $\pi_1(\mathcal{A}_p, q_0) = \langle a^p, ba^p b^{-1} \rangle$ , leading to the following result.

**Corollary 3.3.** *Let  $F$  be a free group on at least two generators. Then there is no algorithm which, given as input a finite subset  $W$  of  $F$  and an element  $w$  of  $F$ , decides if  $w$  is in the pro- $\mathbf{U}$  [pro- $\mathbf{Q}$ , pro- $\mathbf{Q}_n$ ] closure  $\overline{\langle W \rangle}$ . In fact, no such algorithm exists even when  $W$  is restricted to consist of two (conjugate) elements.*

#### 4. APPLICATIONS TO UNDECIDABILITY OF PSEUDOVARITIES

We now prepare to prove several undecidability results for pseudovarieties of monoids. The reader is referred to [2, 8] for basic definitions from monoid theory. If  $\mathbf{V}$  is a pseudovariety of monoids [semigroups] and  $\mathbf{H}$  is a pseudovariety of groups, then  $\mathbf{V} \overset{\circ}{\circlearrowleft} \mathbf{H}$  is the pseudovariety generated by all monoids [semigroups]  $S$  for which there is a morphism  $\varphi : S \rightarrow G \in \mathbf{H}$  such that  $\varphi^{-1}(1) \in \mathbf{V}$ . On the other hand,  $\mathbf{V} * \mathbf{H}$  is the pseudovariety generated by all semidirect products of members in  $\mathbf{V}$  by members in  $\mathbf{H}$ . Hence  $\mathbf{V} * \mathbf{H} \subseteq \mathbf{V} \overset{\circ}{\circlearrowleft} \mathbf{H}$ . If  $\mathbf{V}$  is local in the sense of Tilson [35], then equality holds (cf. Henckell, Margolis, Pin and Rhodes [9]).

Recall that for a pseudovariety  $\mathbf{V}$  of monoids,  $\mathbf{LV}$  is the pseudovariety of all semigroups whose submonoids belong to  $\mathbf{V}$ . Clearly the membership problems for  $\mathbf{V}$  and  $\mathbf{LV}$  are equivalent. A result of Tilson [35] shows that  $\mathbf{V} \neq \mathbf{I}$  is local if and only if  $\mathbf{LV} = \mathbf{V} * \mathbf{LI}$  (here  $\mathbf{I}$  is the trivial pseudovariety). In general,  $\mathbf{V} * \mathbf{LI} \subseteq \mathbf{LV}$  [8, 35].

Let  $\mathbf{DA}$  be the pseudovariety of all monoids [semigroups] whose regular  $\mathcal{D}$ -classes are aperiodic semigroups. It is easy to verify that the inverse monoids in  $\mathbf{DA}$  are precisely the semilattices. We also mention that  $\mathbf{SI}$  and  $\mathbf{DA}$  are local (see Brzozowski and Simon [7] and Almeida [3]). In fact, if  $\mathbf{H}$  is a pseudovariety of groups, then  $\mathbf{SI} * \mathbf{H} = \mathbf{SI} \overset{\circ}{\circlearrowleft} \mathbf{H}$  even holds if both sides are interpreted as pseudovarieties of inverse monoids or inverse semigroups (cf. [14]). It follows that for an inverse monoid  $I$ ,  $I \in \mathbf{SI} * \mathbf{H}$  if and only if  $I \in \mathbf{DA} \overset{\circ}{\circlearrowleft} \mathbf{H} = \mathbf{DA} * \mathbf{H}$ . Denote by  $\mathbf{J}$  the pseudovariety of all  $\mathcal{J}$ -trivial monoids.

**Theorem 4.1.** *Every monoid pseudovariety in the interval  $[\bigvee_{p \in A} \mathbf{SI} * \mathbf{V}_p, \mathbf{DA} \overset{\circ}{\circlearrowleft} \mathbf{U}]$  has undecidable membership problem. In particular,  $\diamond \mathbf{U}$ ,  $\diamond_n \mathbf{U}$ , and  $\mathbf{PU}$  have undecidable membership problems.*

*Proof.* Let  $\mathbf{V}$  be in the interval. Denote by  $I_p$  the transition inverse monoid of  $\mathcal{A}_p$ . Then  $I_p \in \mathbf{V}$  if and only if  $p \in A \cup C$ . It is shown in [31] that  $\diamond \mathbf{H} = \mathbf{J} * \mathbf{H}$  for any pseudovariety of groups  $\mathbf{H}$  and hence  $\diamond \mathbf{U}$  is in the interval. On the other hand,  $\diamond_2 \mathbf{W} = \mathbf{SI} ** \mathbf{W}$  for any pseudovariety  $\mathbf{W}$  — see Rhodes and Tilson [24] for the definition of the two-sided semidirect product \*\*, Tilson [35] for the statement of the result, and Weil [36, Corollary 3.4] for a complete proof. Since, for any

pseudovariety of groups  $\mathbf{H}$ ,  $\mathbf{SI} ** \mathbf{H} = \mathbf{SI} * \mathbf{H}$  [24], we see that  $\diamond_n \mathbf{U}$  belongs to this interval for  $n \geq 2$ .

For the remaining assertion, we use the following two results of [31]: for any pseudovariety of groups  $\mathbf{H}$ , one has  $\mathbf{PH} \subseteq \mathbf{J} * \mathbf{H}$ ; see also Pin [18]; if  $\mathbf{H} = \mathbf{G}_p * \mathbf{H}$  for some prime  $p$ , then  $\mathbf{PH} = \mathbf{J} * \mathbf{H}$ . In particular, for  $p \in A$ ,  $\mathbf{G}_p * \mathbf{U}_p = \mathbf{U}_p$ , so  $\mathbf{PU}_p = \mathbf{J} * \mathbf{U}_p$ . It follows that  $\mathbf{PU}$  is in the interval considered.  $\square$

Amongst the pseudovarieties contained in the interval are  $\mathbf{L} * \mathbf{U} = \mathbf{L} \textcircled{m} \mathbf{U}$ ,  $\mathbf{R} * \mathbf{U} = \mathbf{R} \textcircled{m} \mathbf{U}$ ,  $\mathbf{J} * \mathbf{U}$  and  $\mathbf{J} \textcircled{m} \mathbf{U}$ ; here  $\mathbf{R}$  and  $\mathbf{L}$  denote the pseudovarieties of all  $\mathcal{R}$ -, respectively,  $\mathcal{L}$ -trivial monoids. The inequality  $\mathbf{J} * \mathbf{U} \neq \mathbf{J} \textcircled{m} \mathbf{U}$  has been established in [6]. The same results hold for  $\mathbf{U}$  replaced with  $\mathbf{Q}$  or  $\mathbf{Q}_n$ .

The reader is referred to [6, 9, 30] for the definitions of the  $\mathbf{H}$ -kernel and  $\mathbf{H}$ -pointlike pairs [sets]. Since the inverse monoid pseudovariety  $\mathbf{SI} * \mathbf{U}$  is undecidable, it follows that the  $\mathbf{U}$ -kernel of an inverse monoid is not computable. If  $I$  is an inverse monoid and  $m \in I$ , then  $m$  is in the  $\mathbf{U}$ -kernel of  $I$  if and only if  $\{1, m\}$  is  $\mathbf{U}$ -pointlike. Hence the  $\mathbf{U}$ -pointlike pairs are not decidable for inverse monoids. As far as we know, this is the first example of a decidable pseudovariety satisfying no non-trivial identities and having undecidable pointlike pairs (cf. [29]). We summarize as follows.

**Theorem 4.2.** *The  $\mathbf{U}$ -kernel and the  $\mathbf{U}$ -pointlike pairs [sets] of a monoid [an inverse monoid] are not computable. The same holds for  $\mathbf{Q}$  and  $\mathbf{Q}_n$ .*

Now we consider the situation for semigroup pseudovarieties.

**Theorem 4.3.** *Every semigroup pseudovariety in the interval*

$$\left[ \bigvee_{p \in A} \mathbf{SI} * \mathbf{V}_p, \mathbf{L}(\mathbf{DA} \textcircled{m} \mathbf{U}) \right]$$

*has undecidable membership problem. In particular,  $\mathbf{SI} * \mathbf{LU}$ ,  $\mathbf{DA} * \mathbf{LU}$ ,  $\mathbf{DA} \textcircled{m} \mathbf{LU}$ ,  $\diamond \mathbf{LU}$ ,  $\diamond_n \mathbf{LU}$ , and  $\mathbf{PLU}$  are undecidable.*

*Proof.* The first statement follows immediately from Theorem 4.1. Since any pseudovariety of groups  $\mathbf{H}$  is local [35], setting  $\mathbf{H} = \mathbf{U}$  gives

$$\mathbf{V} * \mathbf{LU} = \mathbf{V} * \mathbf{U} * \mathbf{LI} \subseteq \mathbf{L}(\mathbf{V} * \mathbf{U}).$$

It follows that  $\mathbf{SI} * \mathbf{LU}$  and  $\mathbf{DA} * \mathbf{LU}$  are in the interval. Next, from the proof of [16, Proposition 6.1] (where only a special case is explicitly stated) we get that, for any pseudovarieties  $\mathbf{V}$  and  $\mathbf{W}$  (where  $\mathbf{W}$  is a pseudovariety of monoids),  $\mathbf{V} \textcircled{m} \mathbf{LW} \subseteq \mathbf{L}(\mathbf{V} \textcircled{m} \mathbf{W})$ . Hence  $\mathbf{DA} \textcircled{m} \mathbf{LU}$  is in the interval.

For the remaining part, Pin shows in [20] that, for any pseudovariety  $\mathbf{W}$  of monoids,  $(\diamond \mathbf{W}) * \mathbf{LI} = \diamond(\mathbf{W} * \mathbf{LI})$ . Setting  $\mathbf{W} = \mathbf{U}$ , we see that

$$\diamond \mathbf{LU} = (\diamond \mathbf{U}) * \mathbf{LI} = \mathbf{J} * \mathbf{U} * \mathbf{LI} = \mathbf{J} * \mathbf{LU}$$

proving that  $\diamond \mathbf{LU}$  belongs to the interval. Since

$$\diamond_2 \mathbf{LU} = \mathbf{SI} ** \mathbf{LU} \supseteq \mathbf{SI} * \mathbf{LU},$$

$\diamond_n \mathbf{LU}$  belongs to the interval for  $n \geq 2$ .

For the power operator  $\mathbf{P}$ , it is shown in [16] that for any pseudovariety of groups  $\mathbf{H}$ ,  $\mathbf{PLH} \subseteq \diamond \mathbf{LH} = \mathbf{J} * \mathbf{LH}$ ; moreover, if  $\mathbf{G}_p * \mathbf{H} = \mathbf{H}$ , then  $\mathbf{PLH} = \diamond \mathbf{LH}$ . In particular, for  $p \in A$ ,  $\mathbf{PLU}_p = \diamond \mathbf{LU}_p = \mathbf{J} * \mathbf{LU}_p$ , so  $\mathbf{PLU}$  is in the interval considered.  $\square$

It was shown in [29] that if  $\mathbf{V}$  is a non-trivial pseudovariety of monoids, then the decidability of pointlike pairs [sets] for  $\mathbf{V}$  and  $\mathbf{V} * \mathbf{LI}$  are equivalent. Hence the decidability of the pointlike pairs [sets] of  $\mathbf{U}$  and  $\mathbf{LU}$  are equivalent. This gives the following result.

**Theorem 4.4.** *The  $\mathbf{LU}$ -pointlike pairs [sets] of a semigroup are undecidable.*

Note that we have shown that the semidirect, two-sided semidirect, Mal'cev, and Schützenberger products do not preserve decidability. As mentioned earlier, the semidirect (= Mal'cev = two-sided semidirect product) on the lattice of group pseudovarieties does preserve decidability.

## 5. JOINS

By a different construction we prove that various joins with  $\mathbf{U}$  and  $\mathbf{Q}$  are not decidable. Let  $C_{2,1} = \{1, a, a^2 = 0\}$  be the cyclic monoid with index 2 and period 1 and  $\mathbf{A}$  be the pseudovariety of aperiodic monoids [semigroups].

**Theorem 5.1.** *Each monoid pseudovariety in the interval  $[\langle C_{2,1} \rangle \vee \mathbf{Q}, \mathbf{A} \vee \mathbf{U}]$  has undecidable membership problem. In particular,  $\mathbf{Com} \vee \mathbf{U}$  has undecidable membership problem.*

*Proof.* Let  $p$  be a prime and  $C_p$  a cyclic group of order  $p$ ; put

$$S_p = C_p \cup (C_p \times C_p) \cup \{0\}$$

endowed with the following multiplication:  $(C_p \times C_p) \cup \{0\}$  forms a null semigroup and an ideal of  $S_p$ , and  $C_p$  is the group of units of  $S_p$  acting on  $C_p \times C_p$  via

$$x(y, z) = (xy, z) \text{ and } (x, y)z = (x, yz).$$

Thus,  $S_p$  is an ideal extension of the null semigroup  $C_p \times C_p \cup \{0\}$  by the cyclic group  $C_p$ . We show that if  $p \in A \cup C$ , then  $S_p \in \langle C_{2,1} \rangle \vee \bigvee_{q \in A} \mathbf{V}_q$  while if  $p \in D$ , then  $S_p \notin \mathbf{A} \vee \mathbf{U}$ .

Let  $p \in A \cup C$  and  $q$  be defined by  $q = p$  if  $p \in A$  and  $f(q) = p$  if  $p \in C$ ; then each co-extension of  $C_p$  by an elementary Abelian  $q$ -group is in  $\mathbf{V}_q$  (cf. [6]). Let  $C_p$  act on the left of the set  $C_p \times C_p$  by  ${}^x(y, z) = (xy, zx^{-1})$  and let  $V$  be the additive group of the  $\mathbb{Z}/q\mathbb{Z}$ -vector space with basis  $C_p \times C_p$ . The semidirect product  $V \rtimes C_p$  (with respect to the induced action) is in  $\mathbf{V}_q$ .

Consider the following subsets of  $C_{2,1} \times (V \rtimes C_p)$ :

$$U_p = \{(1, (0, u)) \mid u \in C_p\},$$

$$I_p = \{(a, ((v, w), u)) \mid u, v, w \in C_p\} \cup (\{0\} \times (V \rtimes C_p)).$$

It is easy to see that  $N_p = U_p \cup I_p$  is a submonoid of  $C_{2,1} \times (V \rtimes C_p)$  with group of units  $U_p$  and that  $I_p$  is an ideal. The reader can readily verify that the assignment

$$(1, (0, u)) \mapsto u, (a, ((v, w), u)) \mapsto (v, wu), \{0\} \times (V \rtimes C_p) \mapsto 0 \quad (u, v, w \in C_p)$$

is a well-defined surjective morphism  $\varphi : N_p \rightarrow S_p$  (cf. [5, Theorem 2.2]). Consequently  $S_p \in \langle C_{2,1} \rangle \vee \mathbf{Q}$ .

Suppose now that  $p \in D$  and assume that  $S_p \in \mathbf{A} \vee \mathbf{U}$ ; we shall arrive at a contradiction. Let  $M \in \mathbf{A}$  and  $K \in \mathbf{U}$  be such that  $S_p$  divides  $M \times K$ . The group  $K$  is of the form  $H \times G$  with  $G \in \mathbf{G}_{p,com}$  and  $|H|$  co-prime with  $p$ . By assumption there is a subsemigroup  $N$  of  $M \times H \times G$  and a surjective morphism  $\varphi : N \rightarrow S_p$ . Let  $1 \neq x \in C_p$ ,  $a = (m, h, g) \in \varphi^{-1}(x)$  and  $b \in \varphi^{-1}((1, 1))$ . Let

$t$  be a positive integer for which  $h^t = 1$  and  $x^t = x$  as per Lemma 2.1. For each  $k \geq 0$  we also have  $h^{t+tkp} = 1$  and  $x^{t+tkp} = x$ . Now choose  $k$  large enough so that  $m^{t+tkp}$  is an idempotent ( $M$  is aperiodic). Then we have  $x^{t+tkp} = x$  and  $a^{t+tkp} = (m^{t+tkp}, 1, g^{t+tkp})$ . Set  $c = a^{t+tkp}$ . Then  $\varphi(c) = x$  and  $c$  has central group component and idempotent aperiodic component. It follows that in  $M \times G \times H$  the equation  $c^2bc = bc^2$  holds. Applying  $\varphi$  then gives  $x^2(1, 1)x = x(1, 1)x^2$ . But  $(x^2, x) \neq (x, x^2)$ , so we have obtained a contradiction.

The remaining statement follows since  $\mathbf{G}_{com} \subseteq \mathbf{U}$  and  $\mathbf{Com} = \mathbf{ACom} \vee \mathbf{G}_{com}$  (see [2]) implies that  $\mathbf{Com} \vee \mathbf{U} = \mathbf{ACom} \vee \mathbf{U}$ , where  $\mathbf{ACom}$  is the pseudovariety of all aperiodic commutative monoids.  $\square$

The question as to the decidability of  $\mathbf{A} \vee \mathbf{G}$  is a long-standing open question of Schützenberger. Our result shows that the operator  $\mathbf{A} \vee \_$  need not preserve decidability when applied to group pseudovarieties.

Note that, by Theorem 5.1,  $\langle C_{2,1} \rangle \vee \mathbf{U}$  is undecidable. This is the first example (as far as we know) of the join of a one-generated pseudovariety (or even a locally finite pseudovariety) with a decidable pseudovariety being undecidable. This is in marked contrast to the case of group pseudovarieties. It is shown in [28] that the join of any locally finite pseudovariety of groups with a decidable pseudovariety of groups is again decidable. By the results in [25, 27, 4], the join of any locally finite pseudovariety of monoids [semigroups] whose free objects are computable with a pseudovariety having decidable pointlike pairs is decidable; moreover, in [25, 27] many pseudovarieties  $\mathbf{V} \in [\langle C_{2,1} \rangle, \mathbf{J}]$  are given such that joins of the form  $\mathbf{V} \vee \mathbf{H}$  with  $\mathbf{H}$  a group pseudovariety with decidable pointlike pairs are decidable. By Theorem 5.1,  $\mathbf{V} \vee \mathbf{U}$  is undecidable for such  $\mathbf{V}$ . Thus, in some sense, the results of [25, 27] are sharp.

We also have the following semigroup analog.

**Theorem 5.2.** *Each semigroup pseudovariety in the interval*

$$[\langle C_{2,1} \rangle \vee \mathbf{Q}, \mathbf{L}(\mathbf{A} \vee \mathbf{U})]$$

*has undecidable membership problem. In particular,  $\mathbf{A} \vee \mathbf{LU}$  has undecidable membership problem.*

*Proof.* The first statement is clear since  $S_p$  is a monoid; for the other statement one has to take into account that  $\mathbf{LV} \vee \mathbf{LW} \subseteq \mathbf{L}(\mathbf{V} \vee \mathbf{W})$  and that  $\mathbf{A} = \mathbf{LA}$ .  $\square$

#### REFERENCES

1. D. Albert, R. Baldinger and J. Rhodes, *Undecidability of the identity problem for finite semigroups*, J. Symbolic Logic **57** (1992), 179–192. MR **93f**:03030
2. J. Almeida, *Finite Semigroups and Universal Algebra*, World Scientific, Singapore, 1995. MR **96b**:20069
3. J. Almeida, *A syntactical proof of locality of DA*, Internat. J. Algebra Comput. **6** (1996), 165–177. MR **97b**:20096
4. J. Almeida, *Hyperdecidable pseudovarieties and the calculation of semidirect products*, Internat. J. Algebra Comput. **9** (1999), 241–261. MR **2001a**:20102
5. K. Auinger, *Semigroups with central idempotents*, pp. 25–33 in: Algorithmic Problems in Groups and Semigroups, J.-C. Birget, S. Margolis, J. Meakin, M. Sapir eds., Birkhäuser, Basel 2000. MR **2001c**:20125
6. K. Auinger and B. Steinberg, *The geometry of profinite graphs with applications to free groups and finite monoids*, preprint.

7. J. A. Brzozowski and I. Simon, *Characterizations of locally testable events*, Discrete Math. **4** (1973), 243–271. MR **47**:7948
8. S. Eilenberg, Automata, Languages and Machines, Academic Press, New York, Vol. A, 1974; Vol. B, 1976. MR **58**:26604a, MR **58**:26604b
9. K. Henckell, S. Margolis, J.-E. Pin, and J. Rhodes, *Ash's type II theorem, profinite topology and Mal'cev products, Part I*, Internat. J. Algebra Comput. **1** (1991), 411–436. MR **93h**:20064
10. B. Herwig and D. Lascar, *Extending partial automorphisms and the profinite topology on free groups*, Trans. Amer. Math. Soc. **352** (2000), 1985–2021. MR **2000j**:20036
11. G. Higman, B. H. Neumann and H. Neumann, *Embedding theorems for groups*, J. London Math. Soc. **26** (1949), 247–254. MR **11**:322d
12. E. Hrushovski, *Extending partial isomorphisms of graphs*, Combinatorica **12** (1992), 411–416. MR **93m**:05089
13. O. G. Kharlampovich and M. V. Sapir, *Algorithmic problems in varieties*, Internat. J. Algebra Comput. **5** (1995), 379–602. MR **96m**:20045
14. M. V. Lawson, Inverse Semigroups: The Theory of Partial Symmetries, World Scientific, Singapore, 1998. MR **2000g**:20123
15. S. W. Margolis, M. Sapir, and P. Weil, *Closed subgroups in pro-V topologies and the extension problem for inverse automata*, Internat. J. Algebra Comput. **11** (2001), 405–445. MR **2002g**:20097
16. S. W. Margolis and B. Steinberg, *Power semigroups and polynomial closure*, in: Proceedings of the Third International Colloquium on Words, Languages and Combinatorics, Kyoto, to appear.
17. D. B. McAlister, *Groups, semilattices and inverse semigroups*, Trans. Amer. Math. Soc. **68** (1974), 227–244. MR **50**:10128
18. J.-E. Pin, **BG** = **PG**, *a success story*, pp. 33–47 in: Semigroups, Formal Languages and Groups, J. B. Fountain, ed., Kluwer, Dordrecht, 1995. MR **99e**:20072
19. J.-E. Pin, Syntactic semigroups, pp. 679–746 in: Handbook of language theory, Vol. I, G. Rozenberg and A. Salomaa eds., Springer, 1997. MR **98i**:68205
20. J.-E. Pin, *Algebraic tools for the concatenation product*, preprint.
21. L. Ribes and P. A. Zalesskiĭ, *The pro-p topology of a free group and algorithmic problems in semigroups*, Internat. J. Algebra Comput. **4** (1994), 359–374. MR **96e**:20046
22. J. Rhodes, *Undecidability, automata, and pseudovarieties of finite semigroups*, Internat. J. Algebra. Comput. **9** (1999), 455–473. MR **2000j**:20112
23. J. Rhodes and B. Steinberg, *Pointlike sets, hyperdecidability and the identity problem for finite semigroups*, Internat. J. Algebra Comput. **9** (1999), 475–481. MR **2000k**:20075
24. J. Rhodes and B. Tilson, *The kernel of a monoid morphism*, J. Pure Appl. Algebra **62** (1989), 227–268. MR **92j**:18005
25. B. Steinberg, *On pointlike sets and joins of pseudovarieties*, Internat. J. Algebra Comput. **8** (1998), 203–231. MR **99g**:20104
26. B. Steinberg, *Monoid kernels and profinite topologies on the free Abelian group*, Bull. Austral. Math. Soc. **60** (1999), 391–402. MR **2000h**:20120
27. B. Steinberg, *On algorithmic problems for joins of pseudovarieties*, Semigroup Forum **62** (2001), 1–40. MR **2002e**:20124
28. B. Steinberg, *Inevitable graphs and profinite topologies: Some solutions to algorithmic problems in monoid and automata theory stemming from group theory*, Internat. J. Algebra Comput. **11** (2001), 25–71. MR **2002a**:68074
29. B. Steinberg, *A delay theorem for pointlikes*, Semigroup Forum **63** (2001), 281–304.
30. B. Steinberg, *Finite state automata: A geometric approach*, Trans. Amer. Math. Soc. **353** (2001), 3409–3464. MR **2002c**:20106
31. B. Steinberg, *Polynomial closure and topology*, Internat. J. Algebra Comput. **10** (2000), 603–624. MR **2001m**:20102
32. J. Stallings, *Topology of finite graphs*, Invent. Math. **71** (1983), 551–565. MR **85m**:05037a
33. J. B. Stephen, *Presentations of inverse monoids*, J. Pure Appl. Algebra **63** (1990), 81–112. MR **91g**:20083
34. H. Straubing and D. Thérien, *Regular Languages Defined by Generalized First-Order Formulas with a Bounded Number of Bound Variables*, pp. 551–562 in: Proceedings of the 18th Annual Symposium on Theoretical Aspects of Computer Science, Dresden, Germany, February 2001, Afonso Ferreira, Horst Reichel eds., Springer LNCS **2010**, Berlin, 2001.

35. B. Tilson, *Categories as algebra: An essential ingredient in the theory of monoids*, J. Pure Appl. Algebra **48** (1987), 83–198. MR **90e**:20061
36. P. Weil, *Closure of varieties of languages with counter*, J. Comp. Syst. Sci. **45** (1992), 316–339. MR **94g**:68065

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT WIEN, STRUDLHOFGASSE 4, A-1090 WIEN, AUSTRIA  
*E-mail address:* `karl.aunger@univie.ac.at`

SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, HERZBERG LABORATORIES,  
1125 COLONEL BY DRIVE, OTTAWA, ONTARIO, CANADA K1S 5B6  
*E-mail address:* `bsteinbg@math.carleton.ca`