Theoretical Computer Science 104 (1992) 161–183 Elsevier 161

Fundamental Study

On a conjecture concerning dot-depth two languages

H. Straubing*

Computer Science Department, Boston College, Chestnut Hill, MA 02167, USA

P. Weil**

Université Paris-VI, Tour 55-65, 4^{ième} étage, 4 place Jussieu, 75252 Paris Cedex 05, France

Communicated by D. Perrin Received April 1990 Revised February 1991

Abstract

Straubing, H. and P. Weil, On a conjecture concerning dot-depth two languages, Theoretical Computer Science 104 (1992) 161–183.

In this paper, we study the second level of the dot-depth hierarchy for star-free regular languages. We investigate a necessary condition stated by Straubing for a language to have dot-depth two, and prove that it is sufficient for languages whose syntactic monoid is inverse with three inverse generators. Also we disprove a conjecture according to which Straubing's condition would be equivalent to both dot-depth two and another condition expressed in terms of two-sided semidirect product.

Résumé

Straubing, H. and P. Weil, On a conjecture concerning dot-depth two languages, Theoretical Computer Science 104 (1992) 161–183.

Dans cet article, nous étudions le deuxième niveau de la hiérarchie de concaténation des langages rationnels sans étoile. Nous prouvons qu'une condition nécessaire d'appartenance à ce niveau, énoncée par Straubing, est suffisante pour les langages dont le monoïde syntaxique est inversif et a trois générateurs inversifs. De plus, nous infirmons une conjecture selon laquelle la condition de Straubing serait équivalente à la fois à l'appartenance au deuxième niveau et à une autre condition exprimée en termes de produit semidirect bilatéral.

* Research supported in part by NSF grants CCR-8700700 and CCR-8902369.

** Research supported in part by the PRC Mathématique et Informatique, Ministère de l'Industrie et de la Recherche (France).

0304-3975/92/\$05.00 ① 1992—Elsevier Science Publishers B.V. All rights reserved

Contents

1.	Introduction	162
2.	Basic definitions and previous results	163
	2.1. The dot-depth hierarchy.	163
	2.2. The algebra of finite categories.	164
	2.3. The associated category	166
	2.4. The characterization of dot-depth two	167
	2.5. The fundamental conjectures	168
3.	The dot-depth of inverse monoids.	169
	3.1. Inverse monoids	169
	3.2. Conjecture 2.4 for inverse monoids	171
4.	Conjecture 2.4 is true for inverse monoids with 3 inverse generators	172
5.	Some strict inclusions	176
	5.1. A refinement of Theorem 4.1	176
	5.2. Inverse monoids with at least 4 inverse generators	
	References	182

1. Introduction

This paper is part of a continuing investigation of the dot-depth hierarchy of recognizable languages, a topic in the theory of automata and formal languages, with close connections to logic, semigroup theory and computational complexity. We shall give the precise definition of dot-depth in Section 2. For the moment it is sufficient to say that the hierarchy is a strictly increasing sequence of families of recognizable languages, and that the union of this sequence is the family of all *aperiodic* recognizable languages – those whose syntactic monoids contain no nontrivial groups. The paper by Straubing [22] contains a thorough discussion of the topic and its connections with other areas of mathematics and computer science.

We are particularly interested in the problem of effectively determining the dotdepth of a given aperiodic language – that is, determining the first level of the hierarchy to which a given language belongs. This is trivial for level 0, and results of Simon [17] and Knast [12] show that one can effectively determine whether a given language has dot-depth 1. Straubing [22] gave an effective criterion for determining whether a given aperiodic language over a binary alphabet has dot-depth 2. Weil [26] showed that Straubing's condition, which can be formulated for languages over arbitrary alphabets, decides dot-depth 2 for languages whose syntactic monoids are inverse monoids with two inverse generators. (As these are languages over a four-letter alphabet, this fact does not follow directly from the original results of [22].)

It is known that the dot-depth of a given aperiodic language depends only on the structure of its syntactic monoid. The method used in [22] was to associate with each finite monoid M a category C(M). It was shown that a language L over a two-letter alphabet has dot-depth at most 2 if and only if the category C(M(L)) can be covered by a finite \mathcal{J} -trivial monoid. Here M(L) denotes the syntactic monoid of L. Precise definitions of the other terms used in this introduction will be given in Section 2.

162

Straubing conjectured that this condition decides dot-depth 2 for languages over an arbitrary finite alphabet. Indeed, a stronger conjecture was formulated: Let J ** DA denote the family of finite monoids that divide a two-sided semidirect product of a finite \mathscr{I} -trivial monoid and a monoid in which every regular \mathscr{I} -class is a rectangular band. Furthermore, let V_2 denote the variety of finite monoids generated by the syntactic monoids of languages of dot-depth 2, and CJ the class of finite monoids M such that C(M) divides a finite \mathscr{I} -trivial monoid. Then we know that

$$\mathbf{J} \ast \ast \mathbf{D} \mathbf{A} \subseteq \mathbf{V}_2 \subseteq \mathbf{C} \mathbf{J},$$

with equality holding in place of both inclusions for monoids generated by two elements. The precise conjecture was that both inclusions can be replaced by equalities in general.

There are three principal results in the present paper. First of all, we correct an error in the paper [22] – the category C(M) described therein is not well defined. The correct definition appears in an earlier version [21] of the same paper, which was published in the proceedings of a conference. In Section 2 we give this corrected definition, and indicate how the proof in [22] must be modified. As it turns out, the required modifications are relatively slight, and all the principal results of [22] continue to hold. Second, we show that the strong conjecture cited above is true for inverse monoids with three inverse generators. Finally, we prove that the conjecture is, in general, false. Indeed, we give an example of an inverse monoid M with four inverse generators such that $M \in CJ \setminus (J ** DA)$. Thus, at least one of the two inclusions given above is strict. The weaker conjectures $CJ = V_2$ and $V_2 = J ** DA$ are both open questions at present, although we do know that at least one of them is false.

2. Basic definitions and previous results

2.1. The dot-depth hierarchy

Let A be a finite alphabet. For each $k \ge 0$, we define a family $A^* \mathscr{V}_k$ of subsets of A^* as follows:

$$A^*\mathscr{V}_0 = \{\emptyset, A^*\}$$

and, for k > 0, $A^* \mathscr{V}_k$ is the boolean closure of the family of languages

 $L_0a_1L_1\ldots a_{r-1}L_r,$

where $r \ge 0$, $a_i \in A$ for all *i*, and $L_i \in A^* \mathscr{V}_{k-1}$ for all *i*.

Thus, $A^* \mathcal{V}_k \subseteq A^* \mathcal{V}_{k+1}$ for all $k \ge 0$. This hierarchy of families of languages is called the *dot-depth hierarchy*. The union of the hierarchy is the smallest family of languages in A^* containing the letters and closed under boolean operations and concatenation, that is, the family of *star-free languages* in A^* . The *dot-depth* of a star-free language L is the least k such that $L \in A^* \mathcal{V}_k$. For each $k \ge 0$ there is a variety \mathbf{V}_k of finite monoids (that is, a class of finite monoids closed under submonoids, quotients and finite direct products) such that for any finite alphabet $A, L \subseteq A^*$ belongs to $A^* \mathscr{V}_k$ if and only if M(L), the syntactic monoid of L, is in \mathbf{V}_k . In particular, the dot-depth of a star-free language depends only on the syntactic monoid of the language. It is known that \mathbf{V}_0 is the variety consisting of the trivial monoid alone, \mathbf{V}_1 is the variety of finite \mathscr{I} -trivial monoids [17], the union of the \mathbf{V}_k is the variety of finite aperiodic monoids [15] and for all $k \ge 0$, \mathbf{V}_k is properly contained in \mathbf{V}_{k+1} [4].

The dot-depth hierarchy, thus, gives a parametrization of the star-free languages that appears natural from the standpoint of both language theory and semigroup theory. The works of Thomas [23] and Barrington and Thérien [1] show that this parametrization also has natural interpretations in terms of first-order logic and boolean circuit complexity. The principal open question concerning the hierarchy is whether one can effectively calculate the dot-depth of a star-free language. In view of the semigroup-theoretic characterization, this is equivalent to deciding whether a given finite monoid belongs to V_k . At present, such decision criteria exist only for $k \leq 1$.

We should mention that the original definition of the dot-depth hierarchy [2] was for subsets of A^+ , and gave rise to a hierarchy of varieties of finite semigroups [6]. It follows from work of Knast [12] and Straubing [20] that the decision problems for the two hierarchies are equivalent.

2.2. The algebra of finite categories

The present treatment of finite categories as algebraic objects is due to Tilson [23]. Here we present just enough of the theory to state the principal conjectures and results.

A finite category C is given by a finite set of objects, denoted as Obj(C), and for all $a, b \in Obj(C)$, a finite set of arrows from a to b, denoted as $Hom_C(a, b)$. The sets $Hom_C(a, b)$ are pairwise disjoint for different ordered pairs (a, b) of objects. If $x \in Hom_C(a, b)$ and $y \in Hom_C(b, c)$ (that is, if x and y are consecutive arrows), then there is a product arrow xy in $Hom_C(a, c)$. This product is associative, and for each object a there is an identity arrow $1_a \in Hom(a, a)$ that is a left identity for all Hom(a, b) and a right identity for all Hom(b, a).

The central notion of this theory is that of one category *dividing* another. We say that a category *C divides* a category *D*, or that *D covers C*, and we write $C \prec D$, if there is a function $\varphi : Obj(C) \rightarrow Obj(D)$, and for each $x \in Hom_C(a, b)$ a nonempty subset O(x) of $Hom_D(a\varphi, b\varphi)$ such that

(i) if x and y are consecutive arrows and $x' \in O(x)$, $y' \in O(y)$, then $x'y' \in O(xy)$;

(ii) If x, y are distinct elements of $Hom_C(a, b)$, then $O(x) \cap O(y) = \emptyset$;

(iii) for all $a \in Obj(c)$, $1_{a\varphi} \in O(1_a)$.

A monoid can be viewed as a category with a single object. The definition above then generalizes the usual definition of monoid division (a monoid M divides a monoid N if M is a quotient of a submonoid of N). Division is a reflexive, transitive relation on categories. It is not, in constrast to division of monoids, antisymmetric on isomorphism classes of categories; that is, two nonisomorphic categories can divide one another. We define two categories to be *equivalent* if each divides the other.

A category C is said to be strongly connected if $Hom_C(a, b) \neq \emptyset$ for all $a, b \in Obj(C)$. Let J_1 denote the variety of finite idempotent and commutative monoids. Simon showed that a category C divides an element of J_1 if and only if each of the base monoids $Hom_C(a, a)$ is in J_1 . (Simon's original work [16, 5] makes no reference to categories, but the principal combinatorial lemma in this work is easily equivalent to the assertion about categories.)

The structure of the base monoids alone is not sufficient to determine whether a given category C divides a finite \mathscr{I} -trivial monoid. Knast [12] gives an effective criterion for this based on the structure of the two-object subcategories of C. More precisely, C divides a finite \mathscr{I} -trivial monoid if and only if there exists n > 0 such that for all $a, b \in Obj(C)$, and all $u, v \in Hom_C(a, b), x, y \in Hom_C(b, a)$,

$$(ux)^n uy (vy)^n = (ux)^n (vy)^n.$$

If this condition is satisfied, then taking a=b and $u=v=y=1_a$ shows that each monoid $Hom_C(a, a)$ satisfies the identity $x^n = x^{n+1}$. It follows that the above condition is satisfied with n no larger than the maximum of the cardinalities of the monoids $Hom_C(a, a)$. Thus, one can verify effectively if the condition holds in a given category.

Let A be a finite alphabet, M, N finite monoids, and $\varphi: A^* \to M$, $\psi: A^* \to N$ morphisms, with φ surjective. There results a *relational morphism* $\eta = \varphi^{-1} \psi: M \to N$. The *derived category* of this relational morphism has $A^*\psi$ as its set of objects. Arrows from $w\psi$ to $(wv)\psi$ will be defined as equivalence classes of triples

$$(w\psi, v, (wv)\psi),$$

where $v, w \in A^*$. Two arrows are multiplied according to the rule

 $(w\psi, u, (wu)\psi) \cdot ((wu)\psi, v, (wuv)\psi) = (w\psi, uv, (wuv)\psi).$

Two arrows $(w\psi, u_1, (wu_1)\psi)$, $(w\psi, u_2, (wu_2)\psi)$ are identified if for all w' such that $w'\psi = w\psi$, one has $(w'u_1)\varphi = (w'u_2)\varphi$. It is straightforward to verify that the multiplication of triples yields a well-defined associative multiplication on equivalence classes, and that the equivalence class of $(w\psi, 1, w\psi)$ is the identity at the object $w\psi$. The resulting category is denoted as D_{η} . We shall denote the equivalence class of a triple $(w\psi, v, (wv)\psi)$ by $[w\psi, v, (wv)\psi]$. The definition given here is equivalent to the one given in [24], where the notion of derived category was first defined. The principal result concerning the derived category is the following: Let V and W be varieties of finite monoids. The product variety V * W is the variety of finite monoids generated by all semidirect products S * T, where $S \in V$, $T \in W$. Then $M \in V * W$ if and only if there exists a relational morphism $\eta : M \to N$ with $N \in W$ such that D_{η} divides a monoid in V.

We can associate with the relational morphism $\eta: M \to N$ another category, called the *kernel* of η . Here the objects are pairs $(w_1\psi, w_2\psi)$, where $w_1, w_2 \in A^*$. A triple

 $((w\psi, (ux)\psi), u, ((wu)\psi, x\psi))$

represents an arrow from $(w\psi, (ux)\psi)$ to $((wu)\psi, x\psi)$. Two such triples, with middle coordinates u_1 and u_2 , are identified if and only if for all $w', x' \in A^*$ with $w\psi = w'\psi$, $x\psi = x'\psi$, one has $(w'u_1x)\varphi = (w'u_2x)\varphi$. Multiplication of triples is given by

 $((w\psi, (xyu)\psi), x, ((wx)\psi, (yu)\psi)) \cdot (((wx)\psi, (yu)\psi), y, ((wxy)\psi, u\psi)) =$

 $((w\psi, (xyu)\psi), xy, ((wxy)\psi, u\psi)).$

Once again, this induces a well-defined multiplication on equivalence classes, and results in a finite category K_{η} , which is called the kernel of η .

Let V and W be pseudovarieties of finite monoids. We define V ****** W to be the class of all finite monoids M for which there exists a relational morphism $\eta: M \to N$ with $N \in W$ and K_{η} dividing a member of V. It is easy to show that V ****** W is a pseudovariety. Indeed, there is a two-sided version of the semidirect product with respect to which the kernel plays the same role as the derived category plays with respect to the semidirect product. V ****** W can then be defined in terms of this two-sided semidirect product, in which case the above definition of V ****** W becomes a theorem. See [14]. We note that $K_{\eta} < D_{\eta}$, so that V ***** W \subseteq V ****** W.

2.3. The associated category

In [22] a category C(M) is defined for each monoid M as follows: Obj(C(M)) is the set of idempotents of M, and there is an arrow from e to f labelled by an element s of M if and only if e and s can be expressed as products of elements that are above f in the \mathscr{J} -ordering on M. Unfortunately, the existence of an arrow from e to f and an arrow from f to g does not imply the existence of an arrow from e to g. Thus this "definition" does not really define a category.

To obtain the decidability results of [22], we must go back to an earlier version [21] of this paper, and use the category defined there: Let M be a finite monoid and let $\varphi: A^* \to M$ be a surjective morphism from a free monoid into M. If $w \in A^*$, wa denotes the set of letters of w. The objects of the category $C(M, \varphi)$ are pairs (e, X) where $e \in M$ is idempotent, $X \subseteq A$, and there is a word $w \in A^*$ such that $w\varphi = e$ and $w\alpha = X$. There is an arrow ((e, X), w, (f, Y)) from (e, X) to (f, Y) labelled by $w \in A^*$ if and only if $X \cup w\alpha = Y$. Arrows $((e, X), w_1, (f, Y))$ and $((e, X), w_2, (f, Y))$ are identified if $e \cdot w_1 \varphi \cdot f = e \cdot w_2 \varphi \cdot f$. (Thus an arrow in this category is actually an equivalence class of triples.) The product of arrows is defined by

$$((e, X), v, (f, Y)) \cdot ((f, Y), w, (g, Z)) = ((e, X), vuw, (g, Z)),$$

where $u \in A^*$ is any word such that $u\varphi = f$ and $u\alpha = Y$. Now it can be verified that this is a well-defined associative multiplication on equivalence classes of triples, and that the

equivalence class of ((e, X), 1, (e, X)) is the identity arrow at (e, X). Thus, $C(M, \varphi)$ is a category.

We note two properties of the category $C(M, \varphi)$ with respect to division. First let $\varphi: A^* \to M$, $\psi: M \to N$ be surjective morphisms, with M, N finite. Then $C(N, \varphi \psi) \prec C(M, \varphi)$. The map on objects is defined by covering (n, X) with any $(u\varphi, X)$, where $u\alpha = X$ and $u\varphi \psi = n$. An arrow represented by ((n, X), v, (n', Y)) is covered by the set of all arrows represented by triples of the form ((m, X), w, (m', Y)), where (m, X) covers (n, X), (m', Y) covers (n', Y), and ((n, X), w, (n', Y)) is equivalent to ((n, X), v, (n', Y)). It is then straightforward to verify that the definition of category division is satisfied.

Second, let $\varphi: A^* \to M$, $\psi: B^* \to M$ be surjective morphisms. Then $C(M, \varphi)$ and $C(M, \psi)$ are equivalent. To see this, observe that there is a morphism $\eta: A^* \to B^*$ such that $\eta \psi = \varphi$. We can cover the object (m, X) of $C(M, \varphi)$ by

$$(m, \hat{X}) = \left(m, \bigcup_{a \in X} a\eta \alpha\right),$$

and the arrow represented by ((m, X), w, (m', Y)) with the arrow represented by $((m, \hat{X}), w\eta, (m', \hat{Y}))$. Again one verifies easily that this is a division. Division in the other direction is proved in an identical manner. This last result is particularly important, for while the category defined here requires that one specify a system of generators for M, the equivalence class of the category is independent of this choice of generators.

2.4. The characterization of dot-depth two

Let CJ denote the class of finite monoids M such that $C(M, \varphi)$ divides a \mathscr{J} -trivial monoid, where φ is a morphism from a free monoid onto M. By the remarks at the end of the preceding subsection, this property depends only on M and not on the particular morphism φ . The principal results of [22] can then be stated as follows.

Theorem 2.1. $V_2 \subseteq CJ$.

Theorem 2.2. If $M \in CJ$ is generated by two elements, then $M \in V_2$.

The proof of these results given in [22] uses the incorrect definition of the associated category. We indicate here the minor modifications that must be made in order to obtain correct proofs. In what follows, we shall make free use of the notation and terminology of [22] without giving the definitions.

The crucial step in the proof of Theorem 2.2 is showing that if M is a Schützenberger product of idempotent and commutative monoids then $M \in CJ$ ([22], Lemma 3.2). Let

$$\varphi: A^* \to M = \Diamond (M_1, \ldots, M_k),$$

be a surjective morphism and let

$$\psi: M \to M_1 \times \cdots \times M_k$$

be the projection morphism. Since $M_1 \times \cdots \times M_k \in \mathbf{J}_1$, $u\alpha = v\alpha$ implies $u\varphi\psi = v\varphi\psi$. Now observe that if (e, X) and (f, Y) belong to the same strongly connected subcategory of $C(M, \varphi)$, then X = Y. Thus, there exist $u, v \in A^*$ such that $u\alpha = v\alpha$, $u\varphi = e$, and $v\varphi = f$. Thus, $e\psi = f\psi$. The proof that $M \in \mathbf{CJ}$ now proceeds exactly as in [22].

The proof of Theorem 2.2 requires that we modify Lemma 5.4 of [22]. This lemma should now read:

Let $\varphi : \{a, b\}^* \to M$ be a surjective morphism, with $M \in \mathbb{CJ}$. Let $\gamma = \varphi^{-1} \cong$. Then the derived category D_{γ} divides a finite \mathscr{J} -trivial monoid.

(The congruence \cong is defined in [22].)

The proof then proceeds as that of the original: It is sufficient to verify that each strongly connected component of D_{γ} divides a finite \mathscr{I} -trivial monoid, and it is therefore enough to consider the subcategory of D_{γ} whose objects are all the $w \cong$ such that w has more than 2T blocks. One must now show that this subcategory D divides $C(M, \varphi)$. The map on the objects is defined by: Let w = uv be the standard factorization, and e the associated idempotent. Then $w \cong$ is covered by $(e, \{a, b\})$. Let w_1, w_2 be words with at least 2T blocks, with standard factorizations u_1v_1, u_2v_2 and associated idempotents e_1, e_2 , respectively. The arrow $[w_1 \cong, x, w_2 \cong]$ is covered by the set of all equivalence classes of triples $((e_1, \{a, b\}), z, (e_2, \{a, b\}))$ such that $z\varphi \in e_1 Me_2$, and for all $w \cong w_1$ with standard factorization $uv, (wx)\varphi = (uzv_2)\varphi$. The proof that this is indeed a division now proceeds exactly as in [22].

2.5. The fundamental conjectures

Let **DA** denote the variety of finite monoids in which every regular \mathscr{J} -class is a rectangular band. It is not difficult to show the following proposition.

Proposition 2.3. $J ** DA \subseteq V_2 \subseteq CJ$.

A consequence of the proof given in [22] is that for monoids generated by two elements, these three classes coincide. It was, thus, conjectured that the three classes coincide in general.

Old Conjecture 2.4. $J **DA = V_2 = CJ$.

As we shall soon show, this conjecture is false. It remains an open question, however, whether Theorem 2.2 holds in general.

Conjecture 2.5. $CJ = V_2$.

3. The dot-depth of inverse monoids

In the next sections we are going to prove that Conjecture 2.4 holds if M is an inverse monoid with 3 inverse generators. In preparation for this proof, we shall prove in the present section that for inverse monoids Conjecture 2.4 has a particularly simple form. Let us first review a few classical facts about inverse monoids.

3.1. Inverse monoids

Recall that a monoid M is said to be *inverse* if and only if, for each $m \in M$, there exists a unique $m' \in M$ such that mm'm = m and m'mm' = m'. Then m' is called the *inverse of* m and is denoted by m^{-1} . The following facts are well known [10].

Proposition 3.1. Let M be a monoid and $m, m' \in M$.

(1) If M is inverse, then $(m^{-1})^{-1} = m$ and $(mm')^{-1} = m'^{-1}m^{-1}$.

(2) M is inverse if and only if M is regular and the idempotents commute in M.

(3) If M is inverse, there exists a unique idempotent e(f) that is \mathscr{R} - $(\mathscr{L}$ -) equivalent to m, and $e = mm^{-1}$ ($f = m^{-1}m$).

(4) If M is a monoid of partial one-to-one transformations on a set Q and if, for each transformation m from Q_1 onto Q_2 in $M(Q_1, Q_2 \subseteq Q)$, $m^{-1}: Q_2 \rightarrow Q_1$ is also in M, then M is an inverse monoid. In that case, the idempotents of M are exactly the partial identities in M.

The class of examples of inverse monoids mentioned in Proposition 3.1(4) above is very general, as is shown by the classical Preston–Vagner Theorem, which states that every (finite) inverse monoid is a submonoid of the monoid of one-to-one partial transformations on a (finite) set Q.

In fact, from a variety-theoretic point of view, the study of inverse monoids is equivalent to the study of certain automata. Let us first turn to a few definitions and conventions regarding the presentation of inverse monoids. Let A be an alphabet and $\overline{A} = \{\overline{a} \mid a \in A\}$. We define an involution on $(A \cup \overline{A})^*$ by setting, for all $u \in (A \cup \overline{A})^*$ and $a \in A$, $\overline{1} = 1$, $\overline{ua} = \overline{au}$ and $\overline{ua} = a\overline{u}$. So, if M is an inverse monoid and $\varphi : (A \cup \overline{A})^* \to M$ is a monoid morphism such that $\overline{a}\varphi = (a\varphi)^{-1}$ for all $a \in A$, then, for all $u \in (A \cup \overline{A})^*$, $\overline{u}\varphi = (u\varphi)^{-1}$. If φ is onto, we shall say that $A\varphi$ is a set of *inverse generators* for M. Note that M is generated by $(A \cup \overline{A})\varphi$ in the usual sense.

We shall call a connected deterministic automaton \mathscr{A} over the alphabet $A \cup \overline{A}$ an *inverse automaton* over A if each letter induces a partial one-to-one transition function on the state set and if, for all $a \in A$, \overline{a} induces the reciprocal transformation of the one induced by a. Then, for all $u \in (A \cup \overline{A})^*$, the transition induced by u is a partial one-to-one function and its reciprocal function is the transition induced by \overline{u} . By Proposition 3.1, the transition monoid of \mathscr{A} is inverse. When drawing an inverse automaton over A, we shall avoid drawing the edges labelled by barred letters. The following result is proved in [13].

Proposition 3.2. Let \mathscr{A} be an inverse automaton. Then \mathscr{A} is the minimal automaton of the language it recognizes.

By Proposition 3.1(4), the transition monoid of an inverse automaton is inverse. Proposition 3.3 below provides us with a weak converse.

Proposition 3.3. Let $\mu: A^* \to M$ be a morphism onto an inverse monoid. Then there exists a family $(\mathscr{A}_i)_{i \in I}$ of inverse automata over A, with transition monoids M_i , and there exists a submonoid N of $\prod_{i \in I} M_i$ such that M is isomorphic to N, and the projections of N into each M_i are onto. If M is finite, then I can be chosen to be finite, as well as the \mathscr{A}_i .

Proof. Let R be an \mathscr{R} -class of M, and let \mathscr{A}_R be the automaton with state set R and edges shown in Fig. 1, where r and $r(a\mu)$ lie in R. Then \mathscr{A}_R is an inverse automaton. Indeed, by definition of \mathscr{R} , it is trivially connected. Now, let $u \in A^*$ be the word such that $u\mu = (a\mu)^{-1}$. We must show that $r(a\mu)(u\mu) = r$. Since $r \mathscr{R} r(a\mu)$, we have $rr^{-1} = r(au)\mu r^{-1}$. So

$$r(au) \mu = rr^{-1}r(au) \mu = r(au) \mu r^{-1}r(au) \mu$$
.

But $r^{-1}r$ and $(au)\mu$ are idempotents of M. So

 $r(au)\mu = r(au)\mu r^{-1}r = rr^{-1}r = r.$

Let $\mu_R: A^* \to M_R$ be the transition morphism of \mathscr{A}_R . To conclude the proof, it suffices to show that, for each $u, v \in A^*$, $u\mu = v\mu$ if and only if $u\mu_R = v\mu_R$ for each \mathscr{R} -class R of M. By definition of \mathscr{A}_R , it is immediate that if $u\mu = v\mu$, then u and v induce the same transition in \mathscr{A}_R . Let us now assume that u and v induce the same transformations in all the \mathscr{A}_R 's. In particular, since $u\mu \mathscr{R} u\mu(u\mu)^{-1}$ and $v\mu \mathscr{R} vk(v\mu)^{-1}$, we have $(u\mu(u\mu)^{-1})v\mu = (u\mu(u\mu)^{-1})u\mu = u\mu$ and $(v\mu(v\mu)^{-1})u\mu = (v\mu(v\mu)^{-1})v\mu$. So $u\mu \leq \mathscr{L} v\mu \leq \mathscr{L} u\mu$, i.e. $u\mu \mathscr{L} v\mu$. This implies $(u\mu)^{-1}u\mu = (v\mu)^{-1}v\mu$. But, by the first part of this proof, if u' and v' are words such that $u'\mu = (u\mu)^{-1}$ and $v'\mu = (v\mu)^{-1}$, then $(u\mu_R)^{-1} = u'\mu$ and $(v\mu_R)^{-1} = v'\mu$ for each R. So the transformations induced by u'and v' also coincide in each \mathscr{A}_R . Thus, $(u\mu)^{-1} = (u\mu)^{-1}u\mu(u'\mu) = (u\mu)^{-1}u\mu(v'\mu)$ $= (v\mu)^{-1}v\mu(v\mu)^{-1} = (v\mu)^{-1}$ and, hence, $u\mu = v\mu$. \Box

The monoids M_R above are sometimes called the *right Schützenberger representations of M*. For a complete study of the automata \mathcal{A}_R and their use in the solution of word problems, see Stephen's work [18, 19].



Fig. 1.

3.2. Conjecture 2.4 for inverse monoids

Let us first consider the categories of the form $C(M, \varphi)$ when M is an inverse monoid.

Proposition 3.4. Let M be an inverse monoid. Then $M \in CJ$ if and only if for each idempotent e of M, $eM_e e \in J_1$.

Proof. Let $\varphi: (A \cup \overline{A})^* \to M$ be an onto morphism such that $\overline{a}\varphi = (a\varphi)^{-1}$ for all a in A. It is easy to check that the base monoid of $C(M, \varphi)$ at object $e(e \in E(M))$ is exactly the submonoid $eM_e e$ of M. So, if $C(M, \varphi)$ divides a \mathscr{J} -trivial monoid, then each $eM_e e$ is \mathscr{J} -trivial. Now, by definition, if $m \in M_e$, then $m^{-1} \in M_e$, so that M_e is an inverse semigroup, and $eM_e e$ is an inverse monoid. Thus, $eM_e e$, being both inverse and \mathscr{J} -trivial, lies in \mathbf{J}_1 .

Conversely, let us assume that $eM_e e \in \mathbf{J}_1$ for each idempotent e of M. Then, by Simon's result mentioned in Section 2.2 above, $C(M, \varphi)$ divides a \mathcal{J} -trivial monoid and, hence, $M \in \mathbf{CJ}$. \Box

Let W be the M-variety of all monoids M such that $eM_e e \in J_1$ for each idempotent e of M. Then the restrictions of Conjecture 2.4 to the case of inverse monoids are given by the following conjecture.

Conjecture 3.5. Let M be an inverse monoid. Then $M \in V_2$ if and only if $M \in W$, if and only if $M \in J ** DA$.

We now turn to a detailed study of the inverse monoids in W.

By Proposition 3.3, each inverse monoid M is a subdirect product of a family of inverse monoids M_i $(1 \le i \le n)$, each of which is the transition monoid of some inverse automaton. It is then clear that M lies in V_2 (W) if and only if each of the M_i 's does. Note also that if M has k inverse generators, then so does each M_i . Thus, it is enough to work on monoids that are the transition monoids of inverse automata.

So we need to characterize the W-inverse automata, that is, the inverse automata whose transition monoid is in W. Let \mathscr{A} be an inverse automaton over the alphabet A, with state set Q, M its transition monoid, and μ the canonical projection from $(A \cup \overline{A})^*$ onto M. For each $w \in (A \cup \overline{A})^*$, we let $\omega \alpha (\omega \beta)$ be the set of letters a of $A \cup \overline{A}$ (A) such that a (a or \overline{a}) occurs in w. This defines onto morphisms $\alpha : (A \cup \overline{A})^* \rightarrow 2^{A \cup \overline{A}}$ and $\beta : (A \cup \overline{A})^* \rightarrow 2^A$. Note that β factors through α and that $w\beta = \overline{w}\beta$ for each word $w \in (A \cup \overline{A})^*$.

Lemma 3.6. The following conditions are equivalent.

(1) $M \in \mathbf{W}$.

(2) If w∈(A ∪ A)* and both q.w and q'.w are defined in A (q, q'∈Q), and if there exists u∈(A ∪ A) such that uβ ⊆ ωβ and q.u=q', then q=q'.

Proof. If $M \in \mathbf{W}$ and both q.w and q'.w exist, then $e = (w\bar{w})\mu$ is an idempotent and $q.w\bar{w} = q, q'.w\bar{w} = q'$. Further, for each letter a of $w\beta$, $e \leq \mathcal{J} a\mu$ and $e \leq \mathcal{J} \bar{a}\mu$, that is, $a\mu$, $\bar{a}\mu \in M_e$. So, if $u\beta \subseteq w\beta$, $u\mu \in M_e$. If u is such that q.u = q', then $q.(w\bar{w}uw\bar{w}) = q'$ and $(w\bar{w}uw\bar{w})\mu = e(u\mu)e \in eM_ee$. Thus, if $M \in \mathbf{W}$, then $e(u\mu)e \in E(M)$. By Proposition 3.1, this implies that $w\bar{w}uw\bar{w}$ induces a partial identity of Q, so that q = q'.

Conversely, assume that \mathscr{A} satisfies (2) and let $e \in E(M)$. Also let $m \in M_e$. Then $m = m_1 \dots m_n$ for some m_1, \dots, m_n such that $e \leq_{\mathscr{I}} m_i$ $(1 \leq i \leq n)$. For each *i*, there exist u_i , v_i , $w_i \in (A \cup \overline{A})^*$ such that $e = (u_i v_i w_i) \mu$ and $m_i = v_i \mu$. Therefore, $e = v\mu$ and $m = w\mu$, where $v = v_1 \dots v_n$ and $w = u_1 v_1 w_1 \dots u_n v_n w_n$. Let *q* be a state such that q.(wvw) is defined in \mathscr{A} . Then, since *e* is idempotent, q.w = q and q'.w = q', where q' = q.v. Since $v\beta \subseteq w\beta$, we have q = q' and, hence, q.(wvw) = q. So *eme* is a partial identity of *Q*, that is, *eme* is an idempotent of *M*. Finally, the idempotents of *M* commute since *M* is inverse, so that $eM_e e \in J_1$. \Box

If $B \subseteq A$ and $q \in Q$, it makes sense to consider the *B*-connected component \mathscr{B} of q in \mathscr{A} . This component \mathscr{B} consists of all paths containing q and labelled by words in $(B \cup \overline{B})^*$. Let $Q_{\mathscr{B}}$ be the state set of \mathscr{B} and let $\mu_{\mathscr{A}}$ be the transition morphism of \mathscr{B} . Since $\mu_{\mathscr{A}}$ factors through the restriction of μ to $(B \cup \overline{B})^*$, $M_{\mathscr{A}}$ divides M. In particular, if \mathscr{A} is a W-inverse automaton, then so is \mathscr{B} .

Lemma 3.6 implies the following property.

Corollary 3.7. Let \mathscr{A} be a W-inverse automaton. For all $q \in Q$ and $u \in (A \cup \overline{A})^*$, $q \cdot u^2$ exists if and only if $q \cdot u = q$. In particular, if $m \in M$ and $m^2 \neq 0$, then $m^2 = m$.

Proof. If q.u = q, it is clear that $q.u^2$ exists, and is equal to q. Conversely, let us assume that $q.u^2$ exists, and let \mathscr{B} be the $u\beta$ -connected component of q in \mathscr{A} . Then \mathscr{B} is a W-inverse automaton and both q.u and (q.u).u exist in \mathscr{B} . By Lemma 3.6, this implies q = q.u. \Box

Another consequence of Lemma 3.6, which is immediate, is the following.

Corollary 3.8. Let \mathscr{A} be a W-inverse automaton. Let $u \in (A \cup \overline{A})^*$ and let \mathscr{B} be a $u\beta$ connected component of \mathscr{A} . If $u\mu_{\mathscr{A}} \neq 0$, then $u\mu_{\mathscr{A}}$ has rank 1, that is, there exists a unique
state q of $Q_{\mathscr{A}}$ such that q.u exists.

4. Conjecture 2.4 is true for inverse monoids with 3 inverse generators

Let A_1 be the variety of finite idempotent monoids, that is, the variety defined by the identity $x^2 = x$. In this section we shall prove the following theorem.

Theorem 4.1. Let M be an inverse monoid with 3 inverse generators. The following are equivalent.

- (1) $M \in \mathbf{J}_1 * \mathbf{A}_1$.
- (2) $M \in \mathbf{V}_2$.
- (3) $M \in \mathbf{W}$.

The implications $(1) \Rightarrow (2)$ and $(2) \Rightarrow (3)$ are true in general by the results of Section 2 and the inclusion $A_1 \subseteq DA$. So we need to show that, if M is an inverse monoid with 3 inverse generators that lies in W, then $M \in J_1 * A_1$.

Note that $J_1 * A_1 \subseteq J * A_1 \subseteq V_2$. So Theorem 4.1 proves that, if M is an inverse monoid with 3 inverse generators that lies in W, then it is equivalent for M to be in V_2 (W) and in J * DA, thus proving Conjectures 2.4, 2.5 and 3.5 in this particular case.

Let us mention that parts of this theorem were proved before. In the case of an inverse monoid M with a single inverse generator, it is a consequence of a result by Brzozowski and Fich [3] that $M \in \mathbf{W}$ if and only if $M \in \mathbf{J}_1 * \mathbf{L}$. This implies the equivalence (2) \Leftrightarrow (3). Also, it is a consequence of a result by Straubing [21, 22] that, for such a monoid M, $M \in \mathbf{V}_2$ if and only if $M \in \mathbf{J} * \mathbf{L}$. The equivalence (2) \Leftrightarrow (3) was also proved by Weil [26] in the case of an inverse monoid with 2 inverse generators. The mechanism of the proof in [26] was very different from the one presented here.

Before proving Theorem 4.1, let us review some facts about free bands. Let A be a finite alphabet and let $\gamma: (A \cup A)^* \to FB(A \cup \overline{A})$ be the free band over $A \cup \overline{A}$. It is known that $FB(A \cup \overline{A})$ is finite and its word problem was solved in [9,8]. Let FIB(A)(the *free involutorial band* over A) be the quotient of $FB(A \cup \overline{A})$ by the congruence generated by the pairs of the form $((w\overline{w}w)\gamma, w\gamma)$ ($w \in (A \cup \overline{A})^*$) and let π be the canonical projection of $(A \cup \overline{A})^*$ onto FIB(A).

Since $FB(A \cup \overline{A})$ is finite, so is FIB(A). We shall be interested in the solution of its word problem. For each $w \in (A \cup \overline{A})^*$ that is not the empty word, we let w(0) (w(1)) be the longest prefix (suffix) of w whose β -image is not $w\beta$. Let also w(0) (w(1)) be the letter that occurs in w immediately to the right of w(0) (to the left of w(1)).

For instance, if $w = ab\bar{b}abc\bar{b}c\bar{a}c\bar{a}$, then $w(0) = ab\bar{b}ab$, w(0) = c, $w(1) = \bar{b}$ and $w(1) = c\bar{a}c\bar{a}ca$.

Proposition 4.2. Let $w, w' \in (A \cup \overline{A})^*$. If $w\pi = 1$, then w = 1. If $w, w' \neq 1$, then $w\pi = w'\pi$ if and only if $w\beta = w'\beta$, $w(0)\pi = w'(0)\pi$, w(0) = w'(0), $w(1)\pi = w'(1)\pi$ and w(1) = w'(1).

This solves the word problem for FIB(A) by induction on $|w\beta|$. In particular, we have the following corollary.

Corollary 4.3. Let $w \in (A \cup \overline{A})^*$ and $w \neq 1$. Then $w\pi$ is characterized by the 4-tuple [w(0), w(0), w(1), w(1)], and $w\pi = (w(0)w(0)w(1)w(1))\pi$.

In order to prove Theorem 4.1, we need to show that, if M is an inverse monoid with 3 inverse generators that lies in W, then $M \in J_1 * A_1$. We have seen that it suffices to show the result when M is the transition monoid of some inverse automaton. So let \mathscr{A} be a W-inverse automaton, and let M be its transition monoid. We use the notation of Section 3.

Lemma 4.4. If $u \in (A \cup \overline{A})^*$ and $u\beta = \{a\}$, then there exists a unique v in $\{a, a\overline{a}, \overline{a}, \overline{a}a\}$ such that $u\pi = v\pi$. Furthermore, for each q in Q, if q.u exists, then q.v exists and q.u = q.v.

Proof. By Corollary 4.3, $u\pi$ is characterized by a 4-tuple of the form [1, x, y, 1], where $x, y \in \{a, \bar{a}\}$, and $u\pi = (xy)\pi$. We let v = x if x = y, v = xy otherwise. Then, since *FIB(A)* is a band, $u\pi = v\pi$. Also note that, by definition of u(0) and u(1) and by Corollary 3.7, u = vu' = u''v for some $u', u'' \in (A \cup \bar{A})^*$. Now let $q \in Q$ such that q.u exists. Then q.v exists and, by Corollary 3.8, q' = q.u is the only state in the $\{a\}$ -connected component of q in \mathscr{A} such that $q'.\bar{v}$ exists. Thus, q.v = q' = q.u. \Box

The main combinatorial tool of the proof of Theorem 4.1 is the following proposition.

Proposition 4.5. If $|u\beta| \leq 3$ and $u\pi = u'\pi$, and if \mathcal{B} is a $u\beta$ -connected component of \mathcal{A} such that $u\mu_{\mathcal{A}} \neq 0$ and $u'\mu_{\mathcal{A}} \neq 0$, then $u\mu_{\mathcal{A}} = u'\mu_{\mathcal{A}}$.

Proof. Recall that, by Corollary 3.8, $\mu_{\mathscr{A}}$ and $u'\mu_{\mathscr{A}}$ both have rank 1 if they are not 0. So it is enough to show that $\mu_{\mathscr{A}}$ and $u'\mu_{\mathscr{A}}$ have the same domain and the same range.

If $u\beta = \emptyset$, then u = 1 = u' and the result is trivial.

If $u\beta = \{a\}$, by Lemma 4.4, there exists a prefix v of u such that, for all $q \in Q$, if q.u(q.u') exists, then q.u = q.v (q.u' = q.v). By Corollary 3.8, there exists at most one state q in $Q_{\mathcal{A}}$ such that q.v exists. So, if $u\mu_{\mathcal{A}} \neq 0$ and $u'\mu_{\mathcal{A}} \neq 0$, we have $u\mu_{\mathcal{A}} = v\mu_{\mathcal{A}} = u'\mu_{\mathcal{A}}$.

If $|u\beta| = 2$, then $u(0)\beta = u'(0)\beta$ and $u(1)\beta = u'(1)\beta$ are singletons. Let $y = \underline{u}(0) = \underline{u}'(0)$ and $z = \underline{u}(1) = \underline{u}'(1)$. In particular, $(u(0)y)\beta$, $(u'(0)y)\beta$, $(zu(1))\beta$, $(zu'(1))\beta$ and $u'\beta$ are all equal to $u\beta$ so that, by Corollary 3.8, $u\mu_{\mathscr{B}}$, $u'\mu_{\mathscr{B}}$, $(u(0)y)\mu_{\mathscr{B}}$, $(u'(0)y)\mu_{\mathscr{B}}$, $(zu(1))\mu_{\mathscr{B}}$ and $(zu'(1))\mu_{\mathscr{A}}$ all have rank 1. So we have

$$q_1.u(0) y = q_2, \qquad q_3.zu(1) = q_4, \qquad q_1.u = q_4,$$

$$q'_1.u'(0) y = q'_2, \qquad q'_3.zu'(1) = q'_4, \qquad q'_1.u' = q'_4,$$

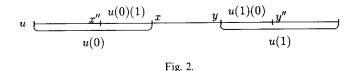
for elements $q_1, q'_1, q_2, q'_2, q_3, q'_3, q_4, q'_4$ uniquely determined in $Q_{\mathscr{B}}$. Now let $v_0(v_1)$ be the word associated with u(0) and u'(0) (u(1) and u'(1)) by Lemma 4.4. Then we have

$$q_1 \cdot v_0 y = q_2, \qquad q_3 \cdot z v_1 = q_4, q'_1 \cdot v_0 y = q'_2, \qquad q'_3 \cdot z v_1 = q'_4.$$

By Corollary 3.8, this implies $q_1 = q'_1$ and $q_4 = q'_4$, so that $u\mu_{\mathscr{B}}$ and $u'\mu_{\mathscr{B}}$ coincide with the transformation of $Q_{\mathscr{B}}$ that maps q_1 on q_4 .

Finally, let us consider the case where $|u\beta|=3$. Let $x=\underline{u}(0)=\underline{u}'(0)$ and $y=\underline{u}(1)=\underline{u}'(1)$. Recall that $u(0)\pi=u'(0)\pi$, $u(1)\pi=u'(1)\pi$ and $|u(0)\beta|=|u(1)\beta|=2$. Then let $x''=\underline{u}(0)(1)=\underline{u}'(0)(1)$, $y''=\underline{u}(1)(0)=\underline{u}'(1)(0)$ and x'(y') be the unique element $u(0)(1)\beta(u(1)(0)\beta)$ (see Fig. 2). Finally, let $v_{01}(v_{10})$ be the word associated with u(0)(1) and u'(0)(1)(u(1)(0) and u'(1)(0)) by Lemma 4.4.

On a conjecture concerning dot-depth two languages



If $u\mu_{\mathscr{A}} \neq 0$ and $u'\mu_{\mathscr{A}} \neq 0$, then $u\mu_{\mathscr{A}}$, $u'\mu_{\mathscr{A}}$, $(x''u(0)(1)x)\mu_{\mathscr{A}}$, $(x''u'(0)(1)x)\mu_{\mathscr{A}}$, $(yu(1)(0)y'')\mu_{\mathscr{A}}$ and $(yu'(1)(0)y'')\mu_{\mathscr{A}}$ all have rank 1 by Corollary 3.8. So we have

$$q_1 \cdot x'' u(0)(1) x = q_2, \qquad q_3 \cdot y u(1)(0) y'' = q_4,$$

$$q_1 \cdot x'' u'(0)(1) x = q_2, \qquad q_3 \cdot y u'(1)(0) y'' = q_4',$$

for elements q_1 , q'_1 , q_2 , q'_2 , q_3 , q'_3 , q_4 and q'_4 uniquely determined in $Q_{\mathscr{R}}$. By Lemma 4.4, this implies

$$q_1 \cdot x'' v_{01} x = q_2, \qquad q_3 \cdot y v_{10} y'' = q_4, q_1' \cdot x'' v_{01} x = q_2', \qquad q_3' \cdot y v_{10} y'' = q_4'$$

and, hence, by Corollary 3.8, $q_2 = q'_2$ and $q_3 = q'_3$.

Then let \mathscr{C} be the $(x'x'')\beta$ -connected component of $q_2.\bar{x}$. Then $u(0)\mu_{\mathscr{C}} \neq 0$ and $u'(0)\mu_{\mathscr{C}} \neq 0$, so that $u(0)\mu_{\mathscr{C}}$ and $u'(0)\mu_{\mathscr{C}}$ both have rank 1 and are equal, by the $(|u\beta|=2)$ -case above. Thus $u\mu_{\mathscr{A}}$ and $u'\mu_{\mathscr{A}}$ have the same domain. Also, let \mathscr{D} be the $(y'y'')\beta$ -connected component of $q_3.y$. Then $u(1)\mu_{\mathscr{D}} \neq 0$ and $u'(1)\mu_{\mathscr{D}} \neq 0$ and, hence, as above, $u(1)\mu_{\mathscr{D}}$ and $u'(1)\mu_{\mathscr{D}}$ both have rank 1 and are equal. Thus, $u\mu_{\mathscr{A}}$ and $u'\mu_{\mathscr{A}}$ have the same range, which proves that $u\mu_{\mathscr{A}} = u'\mu_{\mathscr{A}}$. \Box

Proof of Theorem 4.1. Let $\tau = \mu^{-1}\pi$. Then, τ is a relational morphism, and the diagram shown in Fig. 3 commutes.

By Section 2.2, in order to prove that $M \in \mathbf{J}_1 * \mathbf{A}_1$, it is enough to show that D_{τ} divides an element of \mathbf{J}_1 , and by Simon's result, this will be done if we prove that each base monoid of D_{τ} lies in \mathbf{J}_1 . It is not difficult to see that each of these base monoids of D_{τ} divides M and, hence, has commuting idempotents. So it suffices to prove that each base monoid of D_{τ} is idempotent, i.e. that, if $w, w' \in (A \cup \overline{A})^*$ and $(ww')\pi = w\pi$, then $(ww'^2)\mu = (ww')\mu$.

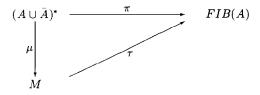


Fig. 3.

Since we are assuming that $|A| \leq 3$, we may use Proposition 4.5. Let \mathscr{B} be any $w\beta$ -connected component. First, it is clear that if $w\mu_{\mathscr{B}} = 0$, then $(ww')\mu_{\mathscr{B}} = 0$. Now, if $w\mu_{\mathscr{A}} \neq 0$ and $(ww')\mu_{\mathscr{A}} \neq 0$, then $w\mu_{\mathscr{A}} = (ww')\mu_{\mathscr{A}}$ by Proposition 4.5. So $(ww')\mu$ is a restriction of $w\mu$, that is, for each $q \in Q$, if q.ww' exists, then q.ww' = q.w. So if q.ww' exists, then $q.ww'^2$ exists and $q.ww'^2 = q.ww'$. Thus, since the existence of $q.ww'^2$ implies the existence of q.ww', we have proved that $(ww')\mu = (ww'^2)\mu$.

5. Some strict inclusions

We shall make the statement of Theorem 4.1 more precise in the case of a 2-letter alphabet. Then we shall give examples of inverse monoids that illustrate some strict inclusions. In particular, we shall construct an inverse monoid with 4 inverse generators, that is in W and not in J ** DA. This will prove that Theorem 4.1 cannot be extended to the 4-generator case, and also that the strong conjecture is false or, equivalently, that one of the containments $J ** DA \subseteq V_2$ and $V_2 \subseteq CJ$ is strict.

5.1. A refinement of Theorem 4.1

Let \mathbf{L}_1 (\mathbf{R}_1) be the M-variety of \mathscr{L} - (\mathscr{R} -) trivial idempotent monoids. Over each finite alphabet A, \mathbf{A}_1 (\mathbf{R}_1 , \mathbf{L}_1 , $\mathbf{R}_1 \vee \mathbf{L}_1$) has a finite free object $\pi_B: A^* \to FB(A)$ ($\pi_R: A^* \to FRB(A)$, $\pi_L: A^* \to FLB(A)$, $\pi_{RL}: A^* \to FRLB(A)$) [9]. Note that \mathbf{R}_1 and \mathbf{L}_1 are the smallest idempotent M-varieties strictly containing \mathbf{J}_1 [27]. The solutions of the word problems for $FB(A \cup \overline{A})$, $FRB(A \cup \overline{A})$, $FLB(A \cup \overline{A})$ and $FRLB(A \cup \overline{A})$ are similar to Proposition 4.2, but we need to modify our notations slightly.

In this section, for each $w \in (A \cup \overline{A})^*$, we shall denote by w(0)(w(1)) the longest prefix (suffix) of w whose α -image is not $w\alpha$, and by w(0)(w(1)) the letter of $A \cup \overline{A}$ that occurs in w immediately to the right of w(0) (to the left of w(1)). The difference from the definitions in Section 4 is that, here, no link whatsoever is established between the letters a and \overline{a} , while in Section 4, a and \overline{a} played equivalent roles in the determination of w(0) and w(1). Then we have [11] the following lemma.

Lemma 5.1. Let u and u' be in $(A \cup \overline{A})^*$.

(1) $u\pi_B = u'\pi_B$ if and only if $u\alpha = u'\alpha$, $u(0)\pi_B = u'(0)\pi_B$, $\underline{u}(0) = \underline{u}'(0)$, $\underline{u}(1) = \underline{u}'(1)$ and $u(1)\pi_B = u'(1)\pi_B$.

(2) $u\pi_R = u'\pi_R$ if and only if $u\alpha = u'\alpha$, $u(0)\pi_R = u'(0)\pi_R$ and $\underline{u}(0) = \underline{u}'(0)$.

(3) $u\pi_L = u'\pi_L$ if and only if $u\alpha = u'\alpha$, $u(1)\pi_L = u'(1)\pi_L$ and $\underline{u}(1) = \underline{u}'(1)$.

(4) $u\pi_{RL} = u'\pi_{RL}$ if and only if $u\pi_R = u'\pi_R$ and $u\pi_L = u'\pi_L$.

One can modify Lemma 4.4 and the proof of Proposition 4.5 in the $(|u\beta|=2)$ -case by replacing π with π_{RL} , thus showing the following theorem.

Theorem 5.2. Let M be an inverse monoid with 2 inverse generators. The following are equivalent.

- (1) $M \in \mathbf{J}_1 * (\mathbf{R}_1 \vee \mathbf{L}_1).$ (2) $M \in \mathbf{V}_2.$
- (3) $M \in \mathbf{W}$.

We now turn to the construction of a few examples of inverse monoids. By Theorem 5.2, if M has 2 inverse generators and $M \in W$, then $M \in J_1 * (\mathbf{R}_1 \vee \mathbf{L}_1)$. Example 5.5 will be of a 2-generated inverse monoid in V_2 that is neither in $\mathbf{A}_1 * * \mathbf{R}_1$ nor in $\mathbf{A}_1 * * \mathbf{L}_1$ (and, hence, neither in $\mathbf{A}_1 * \mathbf{R}_1$ nor in $\mathbf{A}_1 * \mathbf{L}_1$). Also concerning Theorem 5.2, we shall give in Example 5.6 an example of a 3-generated inverse monoid in \mathbf{W} that is not in $\mathbf{A}_1 * (\mathbf{R}_1 \vee \mathbf{L}_1)$ (and, hence, not in $\mathbf{A}_1 * (\mathbf{R}_1 \vee \mathbf{L}_1)$).

For both these examples, we are going to need the following two results.

Lemma 5.3. Let $\varphi: S \to T$ be an onto relational morphism, and let $\psi: F \to T$ be an onto morphism (see Fig. 4). Let $\tau = \varphi \psi^{-1}$. Then D_{τ} divides D_{φ} and K_{τ} divides K_{φ} .

Proof. The construction of the division $\delta: D_{\tau} \prec D_{\varphi}$ is as follows. The object map $\delta: Obj(D_{\tau}) = F^1 \rightarrow Obj(D_{\varphi}) = T^1$ is given by $f\delta = f\psi$ for each $f \in F$. For each f_1 , $f_2 \in F^1$, the arrow-set relation δ from $Hom_{D_{\tau}}(f_1, f_2)$ into $Hom_{D_{\varphi}}(f_1\psi, f_2\psi)$ is given by $(f_1, [s, f])\delta = (f_1\psi, [s, f\psi])$ for each $s \in S$ and $f \in s\tau$ such that $f_1 f = f_2$. The division $\delta': K_{\tau} \prec K_{\varphi}$ is constructed similarly. \Box

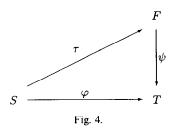
Corollary 5.4. Let V and W be M-varieties, and assume that V has a finite free object $\pi: B^* \to F$ over some finite alphabet B. Let $\mu: B^* \to M$ be an onto morphism and let $\tau = \mu^{-1}\pi$. Then the following are equivalent.

(1) $M \in \mathbf{W} * \mathbf{V} (\mathbf{W} * * \mathbf{V})$.

(2) There exists a relational morphism $\varphi: M \to F$ such that $D_{\varphi}(K_{\varphi})$ divides a monoid in **W**.

(3) $D_{\tau}(K_{\tau})$ divides a monoid in **W**.

Proof. (3) \Rightarrow (2) is trivial and (2) \Rightarrow (1) is a consequence of the results mentioned in Section 2.2.



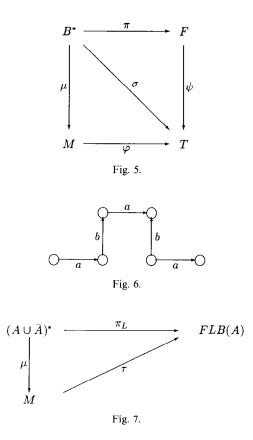
Now let us assume that $M \in \mathbf{W} * \mathbf{V}$ ($\mathbf{W} * * \mathbf{V}$). Then, there exists a relational morphism $\varphi: M \to T$ such that $T \in \mathbf{V}$ and $D_{\varphi}(K_{\varphi})$ divides an element of \mathbf{W} . For each $b \in B$, let us choose $b\sigma$ in $b\mu\varphi$. This defines (see Fig. 5) a morphism σ from B^* into T such that $\sigma = \mu\varphi$; hence, $\mu^{-1}\sigma \subseteq \varphi$. Thus, $\mu^{-1}\sigma$ is a restriction of φ , $B^*\mu^{-1}\sigma = B^*\sigma \in \mathbf{V}$ and $D_{\mu^{-1}\sigma}(K_{\mu^{-1}\sigma})$ is a subcategory of $D_{\varphi}(K_{\varphi})$, so that $D_{\mu^{-1}\sigma} \prec D_{\varphi}(K_{\mu^{-1}\sigma} \prec K_{\varphi})$. So we may assume that σ is onto and $\varphi = \mu^{-1}\sigma$. Since $T \in \mathbf{V}$, there exists an onto morphism $\psi: F \to T$ such that $\sigma = \pi\psi$.

Then, we have $\tau = \mu^{-1} \pi = \varphi \sigma^{-1} \pi = \varphi \psi^{-1}$ since all the morphisms are onto. By Lemma 5.3, this implies $D_{\tau} \prec D_{\varphi} (K_{\tau} \prec K_{\varphi})$; hence, $D_{\tau} (K_{\tau})$ divides a monoid in W. \Box

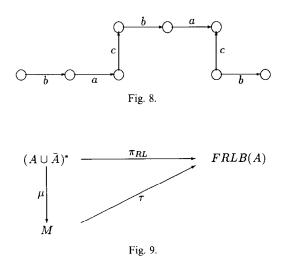
Example 5.5. Let $\mu: (A \cup \overline{A})^* \to M$ be the transition monoid of the inverse automaton shown in Fig. 6. It is easy to see that $M \in \mathbf{W}$, by Lemma 3.6. Let $\tau = \mu^{-1} \pi_L$ (Fig. 7). Let w_1, w and w_2 be the following words:

 $w_1 = ab\bar{b}b, \qquad w = a\bar{b}b, \qquad w_2 = \bar{b}b\bar{b}a,$

By Lemma 5.1, we have $(w_1 w)\pi_L = w_1\pi_L$ and $(ww_2)\pi_L = w_2\pi_L$. So $s = (w_1\pi_L, [w\mu, w\pi_L], w_2\pi_L)$ is in $Hom_{K_{\tau}}((w_1\pi_L, w_2\pi_L))$. But $(w_1ww_2)\mu \neq 0$ and $(w_1w^2w_2)\mu = 0$, so that $s \neq s^2$. Thus, K_{τ} does not divide an idempotent monoid and, hence, $M \notin A_1 * * L_1$.



On a conjecture concerning dot-depth two languages



Similarly, we can prove that $M \notin \mathbf{A}_1 * * \mathbf{R}_1$. The proof is the same, where we replace π_L by π_R , w_1 by $\bar{a}b\bar{b}b$, w by $\bar{b}b\bar{a}$ and w_2 by $\bar{b}b\bar{b}\bar{a}$. \Box

Example 5.6. Let $\mu: (A \cup \overline{A})^* \to M$ be the transition monoid of the inverse automaton shown in Fig. 8. It is easy to check, using Lemma 3.6, that $M \in \mathbf{W}_2$. Let $\tau = \mu^{-1} \pi_{RL}$ (Fig. 9). Let w_1 , w and w_2 be the following words:

 $w_1 = b\bar{b}ba\bar{a}ac\bar{c}, \qquad w = c\bar{c}\bar{a}acb\bar{b}ba\bar{a}a\bar{c}c\bar{c}, \qquad w_2 = c\bar{c}c\bar{a}a\bar{c}b\bar{b}.$

By Lemma 5.1, we have $(w_1 w)\pi_{RL} = w_1\pi_{RL}$ and $(ww_2)\pi_{RL} = w_2\pi_{RL}$. So $s = (w_1\pi_{RL}, [w\mu, w\pi_{RL}], w_2\pi_{RL})$ is in $Hom_{K_{\tau}}((w_1\pi_{RL}, w_2\pi_{RL}))$. But $(w_1ww_2)\mu \neq 0$ and $(w_1w^2w_2)\mu = 0$, so that $s \neq s^2$. Thus, K_{τ} does not divide an idempotent monoid and, hence, $M \notin \mathbf{A}_1 * * (\mathbf{R}_1 \vee \mathbf{L}_1)$. \Box

5.2. Inverse monoids with at least 4 inverse generators

In this section, we shall exhibit an inverse automaton over a 4-letter alphabet whose transition monoid is in W but not in J ** DA, thus proving that Conjecture 2.4 does not hold in general. The proof of this fact requires the following results concerning the M-variety DA, due to Fich and Brzozowski [7].

Let A be a finite alphabet. For each $w \in A^*$ and $n \ge 1$, we let $w\mu_n$ be the set of all subwords of u of length at most n:

 $w\mu_n = \{a_1 \dots a_k \mid k \leq n, a_i \in A, \exists u_0, \dots, u_n \in A^*, w = u_0 a_1 u_1 \dots a_k u_k\}.$

In particular, $w\mu_1 = w\alpha$ is the alphabet of w. We say that w is *n*-full if $w\mu_n = \bigcup_{i=0}^n (w\alpha)^i$, that is, if the set of subwords of w of length n is as large as possible (with respect to the size of the alphabet of w).

Following Fich and Brzozowski [6], we define \equiv_n to be the least congruence satisfying:

For all $u, v, w \in A^*$ such that $v\alpha \subseteq u\alpha = w\alpha$ and u and w are *n*-full, we have $uvw \equiv_n uw$.

Then, we have [6] the following theorem.

Theorem 5.7. Let $\mu: A^* \to M$ be an onto morphism. Then the following are equivalent. (1) $M \in \mathbf{DA}$.

(2) $eM_e e = e$ for each idempotent e of M.

(3) $u \equiv_n v$ implies $u\mu = v\mu$ for some $n \ge 1$.

Then, similar to Corollary 5.4, we can prove the following corollary.

Corollary 5.8. Let V be an M-variety and let $\mu: A^* \to M$. Let also π_n be the canonical projection from A^* onto A^*/\equiv_n and let $\tau_n = \mu^{-1}\pi_n$. Then the following are equivalent.

(1) $M \in \mathbf{V} * \mathbf{DA}$ (V ** DA).

(2) There exists a relational morphism $\varphi: M \to A^*/\equiv_n$ such that $D_{\varphi}(K_{\varphi})$ divides an element of V for some n.

(3) $D_{\tau_n}(K_{\tau_n})$ divides an element of V for some n.

Proof. The proof is very similar to the proof of Corollary 5.4. Implications $(3) \Rightarrow (2)$ and $(2) \Rightarrow (1)$ are immediate.

Then let us consider M in $\mathbf{V} * \mathbf{DA}$ ($\mathbf{V} * * \mathbf{DA}$). We know that there exists a relational morphism $\varphi: M \to T$ such that $T \in \mathbf{DA}$ and $D_{\varphi}(K_{\varphi})$ divides a monoid in \mathbf{V} . As in the proof of Corollary 5.4, we may assume that there exists an onto morphism $\sigma: A^* \to T$ such that $\varphi = \mu^{-1}\sigma$. Then, by Theorem 5.7, there exists an onto morphism $\psi: A^*/\equiv_n \to T$ such that $\sigma = \pi_n \psi$ for some n (see Fig. 10).

Then, we have $\tau_n = \mu^{-1} \pi_n = \varphi \sigma^{-1} \pi_n = \varphi \psi^{-1}$ since all the morphisms are onto. By Lemma 5.3, this implies $D_{\tau_n} \ll D_{\varphi} (K_{\tau_n} \ll K_{\varphi})$ and, hence, $D_{\tau_n} (K_{\tau_n})$ divides an element of **V**. \Box

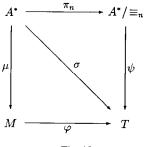


Fig. 10.

180

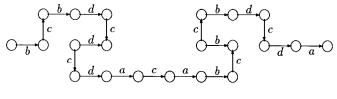


Fig. 11.

We are now ready to construct our counterexample to the extension of Theorem 4.1 to the 4-generator case and to the strong conjecture.

Example 5.9. Let $A = \{a, b, c, d\}$ and let $\mu: (A \cup \overline{A})^* \to M$ be the transition monoid, over A, of the inverse automaton shown in Fig. 11.

Again, using Lemma 3.6, it is easy to see that $M \in W$. For all $n \ge 1$, let

$$u'_{n} = (bc\bar{c}\bar{b})^{n}bcb(\bar{b}\bar{c}cb)^{n},$$

$$v'_{n} = (bc\bar{c}\bar{b})^{n}bc\bar{b}cb(\bar{b}\bar{c}cb)^{n}.$$

Since $(bcc\bar{b})^n$ and $(\bar{b}cc\bar{b})^n$ are *n*-full, we have

$$u'_n \equiv {}_n (bc\bar{c}\bar{b})^n (b\bar{c}cb)^n \equiv {}_n v'_n.$$

Let also

 $u_n'' = (dc\bar{c}\bar{d})^n dcd(\bar{d}\bar{c}cd)^n,$ $v_n'' = (dc\bar{c}\bar{d})^n dc\bar{d}cd(\bar{d}\bar{c}cd)^n.$

Similarly, $u_n'' \equiv_n v_n''$. In particular, the following words,

$$r_{n} = (u'_{n}v''_{n}a\bar{a}\bar{v}''_{n}\bar{u}'_{n})^{n},$$

$$r'_{n} = (\bar{u}'_{n}u'_{n}v''_{n}a\bar{a}\bar{v}''_{n})^{n},$$

$$s_{n} = (v'_{n}u''_{n}a\bar{a}u''_{n}\bar{v}'_{n})^{n},$$

$$s'_{n} = (\bar{v}'_{n}v'_{n}u''_{n}a\bar{a}\bar{u}''_{n})^{n},$$

are *n*-full, use all the letters of $(A \cup \overline{A})^*$, and satisfy

$$r_n \equiv_n s_n, \qquad r'_n \equiv_n s'_n$$

since it is clear that, for any two words z and t, $z \equiv_n t$ if and only if $\overline{z} \equiv_n \overline{t}$. Now let the words w_n , u_n , x_n , v_n and y_n be defined as follows:

$$w_n = r_n r_n,$$

$$u_n = r_n u'_n r'_n,$$

$$x_n = r_n u'_n v''_n a ca v'_n s'_n,$$

$$v_n = \bar{u}_n w_n,$$

$$y_n = \bar{x}_n w_n.$$

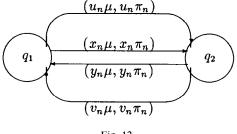


Fig. 12.

Then, we have $u_n \equiv {}_n r_n r'_n \equiv {}_n x_n$ and $v_n \equiv {}_n \bar{r}'_n r_n \equiv {}_n y_n$; hence, the following $\equiv {}_n$ -equivalences hold:

$$w_n u_n \equiv {}_n w_n x_n \equiv {}_n r_n r'_n,$$

$$w_n u_n v_n \equiv {}_n w_n x_n y_n \equiv {}_n r_n r_n = w_n,$$

$$v_n w_n \equiv {}_n y_n w_n \equiv {}_n \overline{r'}_n r_n,$$

$$u_n v_n w_n \equiv {}_n x_n y_n w_n \equiv {}_n r_n r_n = w_n.$$

Let $q_1 = (w_n \pi_n, (x_n w_n) \pi_n)$ and $q_2 = ((w_n x_n) \pi_n, w_n \pi_n)$. The above \equiv_n -equivalences mean that we have the picture shown in Fig. 12 in K_{τ_n} .

Note, however, that for all $k \ge 1$

$$(w_n(x_ny_n)^k(u_nv_n)^kw_n)\mu = (w_nx_ny_nu_nv_nw_n)\mu \neq 0,$$

while

$$(w_n(x_ny_n)^k x_nv_n(u_nv_n)^k w_n)\mu = (w_nx_ny_nx_nv_nu_nv_nw_n)\mu = 0$$

since $w_n x_n y_n x_n v_n u_n v_n w_n = w_n x_n y_n x_n \overline{u}_n w_n u_n v_n w_n$ and $(x_n \overline{u}_n) \mu = 0$.

By Knast's result (see Section 2.2), this proves that K_{τ_n} does not divide a \mathscr{J} -trivial monoid and, hence, by Corollary 5.8, that $M \notin \mathbf{J} * * \mathbf{D} \mathbf{A}$. \Box

References

- D. Barrington and D. Thérien, Finite monoids and the fine structure of NC¹, J. Assoc. Comp. Mach. 35 (1988) 941–952.
- [2] J. Brzozowski and R. Cohen, Dot-depth of star-free events, J. Comput. System Sci. 5 (1971) 1-16.
- [3] J. Brzozowski and F. Fich, On generalized locally testable languages, Discrete Math. 50 (1984) 153-169.
- [4] J. Brzozowski and R. Knast, The dot-depth hierarchy of star-free events is infinite, J. Comput. System Sci. 16 (1978) 37-55.
- [5] J. Brzozowski and I. Simon, Characterization of locally testable events, Discrete Math. 4 (1973) 243-271.
- [6] S. Eilenberg, Automata, Languages and Machines, Vol. B (Academic Press, New York, 1976).
- [7] F. Fich and J. Brzozowski, A characterization of a dot-depth two analogue of generalized definite languages, in: *Proc. 6th ICALP*, Lecture Notes in Computer Science, Vol. 71 (Springer, Berlin, 1979) 230-244.

- [8] J. Gerhardt, The lattice of equational classes of idempotent semigroups, J. Algebra 15 (1970) 195-224.
- [9] J. Green and D. Rees, On semigroups in which $x^r = x$, Proc. Cambridge Phil. Soc. 48 (1952) 35-40.
- [10] J. Howie, An Introduction to Semigroup Theory (Academic Press, London, 1976).
- [11] N. Kimura, The structure of idempotent semigroups, I, Pacific J. Math. 8 (1958) 227-244.
- [12] R. Knast, A semigroup characterization of semigroups of dot-depth one languages, RAIRO Inform. Théor. Appl. 17 (1983) 321-330.
- [13] Ch. Reutenauer, Une topologie du monoïde libre, Semigroup Forum 18 (1979) 33-50.
- [14] J. Rhodes and B. Tilson, The kernel of monoid morphisms, J. Pure Appl. Algebra 62 (1989) 227–268.
- [15] M.-P. Schützenberger, On finite monoids having only trivial subgroups, Inform. and Control 8 (1965) 190–194.
- [16] I. Simon, Hierarchies of events of dot-depth one, Ph.D. Thesis, University of Waterloo, 1972.
- [17] I. Simon, Piecewise testable events, in: Proc. 2nd G.I. Conf., Lecture Notes in Computer Science, Vol. 33 (Springer, Berlin, 1975) 214–222.
- [18] J. Stephen, Applications of automata theory to presentations of monoids and inverse monoids, Ph.D. Thesis, University of Nebraska, Lincoln, 1987.
- [19] J. Stephen, Presentations of inverse monoids, J. Pure Appl. Algebra 63 (1990) 81-112.
- [20] H. Straubing, Finite semigroup varieties of the form V * D, J. Pure Appl. Algebra 36 (1985) 53-94.
- [21] H. Straubing, Semigroups and languages of dot-depth two, in: Proc. 13th ICALP, Lecture Notes in Computer Science, Vol. 226 (Springer, Berlin, 1986) 416–423.
- [22] H. Straubing, Semigroups and languages of dot-depth two, Theoret. Comput. Sci. 58 (1988) 361–378.
- [23] W. Thomas, Classifying regular events in symbolic logic, J. Comput. System Sci. 25 (1982) 360-376.
- [24] B. Tilson, Categories as algebras: an essential ingredient in the theory of monoids, J. Pure Appl. Algebra 48 (1987) 83-198.
- [25] P. Weil, Inverse monoids and the dot-depth hierarchy, Ph.D. Thesis, University of Nebraska, Lincoln, 1988.
- [26] P. Weil, Inverse monoids of dot-depth two, Theoret. Comput. Sci. 66 (1989) 233-245.
- [27] S. Wismath, The lattices of varieties and pseudovarieties of band monoids, Semigroup Forum 33 (1986) 187–198.