Theoretical Computer Science 58 (1988) 361-378
North-Holland

SEMIGROUPS AND LANGUAGES OF DOT-DEPTH TWO

Howard STRAUBING*
Department of Computer Science, Boston College, Chestnut Hill, MA 02167, U.S.A.

Abstract. This paper is a contribution to the problem of effectively determining the dot-depth of a star-free language, a problem concerning formal languages that has close connections to semigroup theory and mathematical logic. I conjecture an effective criterion, based on the syntactic monoid of the language, for determining whether a given language has dot-depth two, and prove the conjecture in the case of languages over an alphabet of two letters. The condition is formulated in terms of a novel use of categories in semigroup theory, recently developed by Tilson.

1. The dot-depth hierarchy

This paper presumes that the reader is familiar with the theory of the syntactic monoid of a recognizable language. For the fundamentals of this theory, as well as definitions of all terms not defined here, see [6] or [11].

Let A be a finite alphabet. The *star-free languages* over A are those subsets of A^* (the free monoid on A) that can be obtained, starting from the letters of A, by applying the boolean operations and concatenation. More precisely, the star-free languages over A constitute the smallest family $\boldsymbol{F}$ of languages such that

(i) $\{a\} \in \boldsymbol{F}$ for all $a \in A$;

(ii) $A^* - L$, $L \cup L'$, $LL' \in \boldsymbol{F}$ for all L, $L' \in \boldsymbol{F}$.

The star-free languages thus form a subfamily of the family of regular, or recognizable, languages over A. It is sometimes convenient to consider the family of star-free languages in A^+ (the free semigroup on A); this consists of the star-free languages in A^* that do not contain the empty word 1. According to a theorem of Schützenberger [19], a language L in A^* is star-free if and only if its syntactic monoid $M(L)$ is finite and aperiodic—that is, $M(L)$ contains no nontrivial groups. (The analogous result holds for the star-free languages in A^+: $L \subseteq A^+$ is star-free if and only if its syntactic semigroup $S(L)$ is finite and aperiodic.)

The *dot-depth hierarchy*, introduced by Cohen and Brzozowski [2] (see also [6, Chapter IX]), is a hierarchy of families of languages whose union is the family of star-free languages. The position that a language occupies in this hierarchy can be viewed as a measure of its complexity. For reasons that will be explained below, this hierarchy is defined for languages in A^+ rather than A^*. Let $A^+\boldsymbol{B}_0$ be the family consisting of the finite and cofinite subsets of A^+. For $k \geq 0$, let $A^+\boldsymbol{B}_{k+1}$ be the boolean closure of the family of languages of the form $L_1 \ldots L_r$, $r \geq 1$, where $L_i \in A^+\boldsymbol{B}_k$ for $i = 1, \ldots, r$. $L \subseteq A^+$ is star-free if and only if $L \in A^+\boldsymbol{B}_k$ for some $k \geq 0$. The dot-depth of L is the smallest such k.

* Research supported by National Science Foundation Grant CCR8700700.

For the most part I will be considering a closely related hierarchy, this one in A^*. Let $A^*\mathbf{V}_0 = \{\emptyset, A^*\}$. For $k \geq 0$, let $A^*\mathbf{V}_{k+1}$ be the boolean closure of the family of languages of the form $L_0 a_1 L_1 a_2 \ldots L_r$, $r \geq 0$, where $L_i \in A^*\mathbf{V}_k$ for $i = 0, \ldots, r$ and $a_i \in A$ for $i = 1, \ldots, r$. The following list of facts summarizes the important properties of the two hierarchies that have so far appeared in the literature.

(1.1) *The hierarchy is strict.* If $|A| > 1$ then both hierarchies are infinite; that is, $A^+\mathbf{B}_k \subsetneq A^+\mathbf{B}_{k+1}$ and $A^*\mathbf{V}_k \subsetneq A^*\mathbf{V}_{k+1}$ for $k \geq 0$ (see [3, 22, 30]).

(1.2) *The hierarchy is algebraically determined.* Each $\mathbf{B}_k$ is a *+-variety of languages* [6, Chapter IX]. That is, for each $k \geq 0$ there exists a pseudovariety $\mathbf{B}_k$ of finite semigroups such that, for any $L \subseteq A^+$, $L \in A^+\mathbf{B}_k$ if and only if $S(L) \in \mathbf{B}_k$. Similarly, each $\mathbf{V}_k$ is a *-variety of languages: for each $k \geq 0$ there is a pseudovariety $\mathbf{V}_k$ of finite monoids such that for $L \subseteq A^*$, $L \in A^*\mathbf{V}_k$ if and only if $M(L) \in \mathbf{V}_k$ [23], [26]. The corresponding statement for the syntactic monoids of members of $A^+\mathbf{B}_k$ is false; this is why the $\mathbf{B}$-hierarchy is defined in terms of the syntactic semigroup rather than the syntactic monoid.

(1.3) *Low levels of the V-hierarchy.* The pseudovariety $\mathbf{V}_0$ consists of the trivial monoid alone. The pseudovariety $\mathbf{V}_1$ consists of all finite monoids having one-element $\mathbf{J}$-classes. Such a monoid is said to be $\mathbf{J}$-trivial [20, 25].

(1.4) *Low levels of the B-hierarchy.* The pseudovariety $\mathbf{B}_0$ consists of the finite nilpotent semigroups. The pseudovariety $\mathbf{B}_1$ consists of all finite semigroups S that satisfy the following condition [9]: There exists an $n > 0$ such that, for all $e, f, s, t, u, v \in S$ with e and f idempotent,

$$(esft)^n esfve(ufve)^n = (esft)^n e(ufve)^n.$$

Furthermore, if $k \geq 1$, each $\mathbf{B}_k$ is equal to the product variety $\mathbf{V}_k * \mathbf{D}$, where $\mathbf{D}$ is the pseudovariety of definite semigroups. (In particular, $\mathbf{V}_k$ consists of all the monoids in $\mathbf{B}_k$). From this standpoint, the $\mathbf{V}$-hierarchy appears to be the more fundamental of the two, although, when defined in terms of languages, the $\mathbf{B}$-hierarchy is somewhat simpler. It follows from this that if $k \geq 2$ and there is an algorithm for determining whether a given finite monoid belongs to $\mathbf{V}_k$, then there exists an algorithm for determining whether a given finite semigroup belongs to $\mathbf{B}_k$ [23].

(1.5) *Connection with formal logic.* It was shown by Büchi [5] that a language is recognizable if and only if it can be described by a sentence in a certain second-order logical language (the weak monadic second-order theory of linear order). The logical language has first-order variables, which denote positions in a word; second-order variables, which denote sets of positions; binary predicates "=" and "<" (so that "$x < y$" is interpreted as "position x is to the left of position y"); a unary predicate P_a for each $a \in A$ (so that "$P_a(x)$" is interpreted as "the letter in position x is a") and a relation "$\in$" between first- and second-order variables with the usual interpretation. McNaughton showed [13, 10] that the star-free languages are exactly those that can be described by the first-order sentences in this language. It was shown by Thomas that the levels of the dot-depth hierarchy correspond to the degree of

alternation of quantifiers required in the first-order sentences used to describe star-free languages [29, 14]. More precisely, $L \in \boldsymbol{V}_k$ if and only if L can be described by a boolean combination of Σ_k sentences. It is interesting to note that Thomas originally proved his result for the $\boldsymbol{B}$-hierarchy. This required the adjunction of a number of new predicates and constants to the logical language in order to get the result to turn out right. When the $\boldsymbol{V}$-hierarchy is used instead, the result takes on the simple form stated here. Thus, from the logical as well as the semigroup-theoretic standpoint, the $\boldsymbol{V}$-hierarchy appears to be the more fundamental of the two.

(1.6) *Connection with circuit complexity.* The computational capabilities of families of bounded-depth boolean circuits with unbounded fan-in have been studied in connection with the complexity of parallel algorithms, sequential complexity classes relativized to oracles, and theoretical investigations of programmable logic arrays [8, 21]. Recent work of Barrington and Thérien [1] has demonstrated a connection between circuit complexity and semigroup theory. They define "nonuniform deterministic finite automata" (NUDFA) over a finite monoid—a kind of nonsequential computation in a finite monoid—and show that

(a) a set of bit strings $L \subseteq \{0, 1\}^*$ is recognized by a polynomial-size, constant-depth family of boolean circuits if and only if it is recognized by a family of polynomial-size NUDFA over an aperiodic monoid; and

(b) L is recognized by a polynomial-size, depth-k family of boolean circuits, with $k \geqslant 2$ if and only if it is recognized by a family of polynomial-size NUDFA over a monoid in $\boldsymbol{V}_k$. In particular, Sipser's result [21] distinguishing the capabilities of depth-k and depth-$(k+1)$ circuit families provides still another proof that the dot-depth hierarchy is strict.

An outstanding open problem is whether one can effectively determine the dot-depth of a given star-free language. By (1.2), this is equivalent to determining whether a given finite semigroup belongs to the pseudovariety $\boldsymbol{B}_k$. The result cited in (1.4) gives a solution to the problem in case $k = 1$. (If the condition in (1.4) holds, then S must be aperiodic, so $s^p = s^{p+1}$ for all $s \in S$, where $p = |S|$. Thus the condition holds with n replaced by $|S|$, and this can be verified effectively from the multiplication table of S.) The cases $k > 1$ are open. According to (1.4), the problem now reduces to determining whether a given finite monoid belongs to $\boldsymbol{V}_k$. According to (1.5), this is closely related to the problem of determining whether a given sentence in the first-order theory of linear order is equivalent to a boolean combination of Σ_k sentences. In this paper I conjecture a solution to the problem for the case $k = 2$. It will be shown that the proposed condition is necessary in all cases, and sufficient for monoids generated by two elements. The condition itself is formulated in terms of a novel use of categories in the study of semigroups, due largely to Tilson [32], which will be described in the next section.

These results first appeared, in a slightly different form, in [24]. The present paper contains complete proofs of the theorems announced there, and a detailed discussion of the status of the general conjecture.

2. Categories as algebraic objects; statement of the main results

Let C be a category. I denote by $\mathrm{Obj}(C)$ the set of objects of C; by $\mathrm{Hom}_C(a, b)$ (or $\mathrm{Hom}(a, b)$ when C is understood) the set of morphisms, or arrows, in C from a to b, where $a, b \in \mathrm{Obj}(C)$; and by $\mathrm{Hom}(C)$ the set of all arrows of C. C can be viewed as a generalized monoid, where the arrows of C correspond to the elements of the monoid, and where the product of two such elements x and y is defined if and only if x and y are consecutive; i.e., $x \in \mathrm{Hom}(a, b)$ and $y \in \mathrm{Hom}(b, c)$ for some $a, b, c \in \mathrm{Obj}(C)$. From this point of view a monoid is a category having only one object.

We shall only be concerned with finite categories—those C for which $\mathrm{Hom}(C)$ is finite. For the purposes of this paper, the crucial notion is that of a monoid M *covering* a category C. We say that M *covers* C, or C *divides* M, *and write* $C \prec M$, if for each arrow x of C there is a nonempty subset M_x of M such that

(i) (*multiplicativity*) if x and y are consecutive arrows (so that xy is defined) and $x' \in M_x$, $y' \in M_y$, then $x'y' \in M_{xy}$;

(ii) (*injectivity*) if $x \neq y$ are coterminal arrows (so that $x, y \in \mathrm{Hom}(a, b)$ for some $a, b \in \mathrm{Obj}(C)$), then $M_x \cap M_y = \emptyset$;

(iii) if 1_a is the identity at $a \in \mathrm{Obj}(C)$, then 1_M (the identity of M) is in M_{1_a}.

Intuitively, M covers C if one can multiply two arrows in C by checking the endpoints of the arrows and performing a multiplication in M. If $C = N$ is a monoid, then $N \prec M$ if and only if N is a quotient of a submonoid of M—thus this definition generalizes the usual notion of division of monoids. There is a more general notion of one category dividing another: $C \prec D$ if there is a function $\phi : \mathrm{Obj}(C) \to \mathrm{Obj}(D)$, and for each $x \in \mathrm{Hom}_C(a, b)$ a nonempty subset M_x of $\mathrm{Hom}_D(a\phi, b\phi)$ such that (i) and (ii) above hold, and such that if $x = 1_a$, then $1_{a\phi} \in M_x$. Division of categories is a transitive relation.

It turns out that the heart of Knast's paper [9] demonstrating the decidability of dot-depth one is the proof of a criterion for determining whether a finite cateogry can be covered by a J-trivial monoid:

Proposition 2.1. *Let C be a finite category. There is a J-trivial monoid M such that $C \prec M$ if and only if there exists $n > 0$ such that if $a, b \in \mathrm{Obj}(C)$; $x, u \in \mathrm{Hom}(a, b)$; $y, v \in \mathrm{Hom}(b, a)$, then*

$$(xy)^n xv(uv)^n = (xy)^n (uv)^n.$$

Knast's proof of this fact is stated in terms of graph congruences, and is quite difficult. A simpler proof is in [27]. Observe that if an integer n satisfying the condition in the proposition exists, then $u^{n+1} = u^n$ for all arrows u that begin and end at the sme vertex. It follows that $u^{r+1} = u^r$ for all such arrows, where $r = |\mathrm{Hom}(C)|$. Thus the condition holds with $n = |\mathrm{Hom}(C)|$, and consequently one can verify effectively, given the multiplication in the category, whether a given finite category can be covered by a finite J-trivial monoid.

Let M be a finite monoid, and let $E(M)$ be the set of idempotents of M. If $e \in E(M)$ then P_e denotes the set $\{m \in M \mid e = xmy \text{ for some } y \in M\}$—that is P_e is the set of elements of M that are above e in the $\mathbf{J}$-order on M. M_e denotes the submonoid of M generated by P_e. I define a category $C = C(M)$ as follows: $\mathrm{Obj}(C) = E(M)$, and the elements of $\mathrm{Hom}_C(e, f)$ are equivalence classes of triples (e, s, f), where $e, s \in M_f$ and where two such triples (e, s_1, f) and (e, s_2, f) are equivalent if and only if $es_1 f = es_2 f$. The equivalence class of (e, s, f) is denoted $[e, s, f]$. Multiplication of triples is defined by

$$[e, s, f][f, t, g] = [e, sft, g].$$

It is easy to verify that this multiplication is well-defined and associative. Furthermore, $[e, 1, e]$ is the identity at e. Thus C is indeed a category. Observe that a list of the objects and arrows of $C(M)$, and the multiplication table for the arrows, can be effectively produced from the multiplication table of M.

The principal results of this paper are the following theorems.

Theorem 2.2. *If $M \in \mathbf{V}_2$, then $C(M)$ divides a finite $\mathbf{J}$-trivial monoid.*

Theorem 2.3. *If M is generated by two elements and $C(M)$ divides a finite $\mathbf{J}$-trivial monoid, then $M \in \mathbf{V}_2$.*

Theorems 2.2 and 2.3, together with Proposition 2.1, give an effective procedure for determining whether a language over a two-letter alphabet has dot-depth at most two. The proofs of these theorems will be given in Sections 3–5.

In [24] I conjectured that the two-generated condition in Theorem 2.3 can be dropped, thus providing an effective procedure for determining whether any given language has dot-depth two or less. I now believe that this cannot be done without some modification of the definition of $C(M)$. Section 6 is devoted to conjectured extensions of Theorems 2.2 and 2.3.

3. Proof of Theorem 2.2

The proof makes use of the generalized Schützenberger product of finite monoids. This is defined as follows: Let $M_1, \ldots, M_n$ be monoids. Consider the set of upper triangular $n \times n$ matrices in which the (i, j)-entry is a subset of $M_i \times \cdots \times M_j$. If $\mu = (m_i, \ldots, m_j) \in M_i \times \cdots \times M_j$ and $\mu' = (m'_j, \ldots, m'_k) \in M_j \times \cdots \times M_k$, then I define $\mu\mu' = (m_i, \ldots, m_{j-1}, m_j m'_j, m'_{j+1}, \ldots, m'_k)$. This product is extended to subsets of $M_i \times \cdots \times M_j$ and $M_j \times \cdots \times M_k$ in the usual fashion; addition is given by set union. It is easy to see that the set of all such matrices forms a monoid. The generalized Schützenberger product $\diamond(M_1, \ldots, M_n)$ is the submonoid consisting

of those matrices all of whose diagonal entries are one-element sets. If $\mu \in \Diamond(M_1, \ldots, M_n)$ and $(\{m_1\}, \ldots, \{m_n\})$ is the diagonal of μ, then I define $\mu\psi = (m_1, \ldots, m_n)$. Thus ψ is a morphism from $\Diamond(M_1, \ldots, M_n)$ onto $M_1 \times \cdots \times M_n$. The reader is referred to [22] for the important properties of this construction.

Let $\boldsymbol{V}$ be a pseudovariety of finite monoids. We define $\Diamond \boldsymbol{V}$ to be the family of all finite monoids that divide some generalized Schützenberger product $\Diamond(M_1, \ldots, M_n)$, where $M_i \in \boldsymbol{V}$ for $i = 1, \ldots, n$. Since

$$\Diamond(M_1, \ldots, M_k) \times \Diamond(N_1, \ldots, N_r) \subseteq \Diamond(M_1, \ldots, M_k, N_1, \ldots, N_r),$$

$\Diamond \boldsymbol{V}$ is itself a pseudovariety. It has been shown [16] that

$$\boldsymbol{V}_2 = \Diamond \boldsymbol{J} = \Diamond \boldsymbol{J}_1 = \Diamond \mathbf{DA},$$

where $\boldsymbol{J}$ is the pseudovariety of all finite $\boldsymbol{J}$-trivial monoids, $\boldsymbol{J}_1$ is the pseudovariety of idempotent and commutative monoids, and $\mathbf{DA}$ is the pseudovariety consisting of all finite monoids in which every regular $\boldsymbol{J}$-class is a rectangular band.

Let $M_1, \ldots, M_k$ be finite monoids, and let $\psi : \Diamond(M_1, \ldots, M_k) \to M_1 \times \cdots \times M_k$ be the projection morphism.

Lemma 3.1. *Let $e \in M_1 \times \cdots \times M_k$ be idempotent. Then $e\psi^{-1} \in B_1$.*

Proof. Let $e = (e_1, \ldots, e_k) \in M_1 \times \cdots \times M_k$ and let $u, v, w, x, y, z \in e\psi^{-1}$, with u, v idempotent. According to (1.4), it must be shown that, for some n,

$$[(uwvx)^n uwvzu(yvzu)^n]_{ij} = [(uwvx)^n u(yvzu)^n]_{ij}$$

whenever $1 \leq i, j \leq k$. The proof mimics that of [22, Theorem 1.4], where a slightly weaker result is proved. One first shows, as in that paper, that if $n \geq 2k$ and $s \in e\psi^{-1}$, then $s^n = s^{n+1}$. Now every entry v_{rs} of v with $r \leq s$ can be written as a sum of terms $v_{ri_1} v_{i_1 i_2} \ldots v_{i_p s}$, each of which contains a factor of the form v_{tt} (this is a consequence of the idempotence of v). Since $v_{tt} = e_t = v_{tt} x_{tt} u_{tt} y_{tt} v_{tt}$, every term in the expansion of

$$[(uwvz)^n uwvzu(yvzu)^n]_{ij}$$

is a sum of terms in the expansion of

$$[(uwvz)^n uwvxuyvzu(yvzu)^n]_{ij}$$
$$= [(uwvz)^{n+1} u(yvzu)^{n+1}]_{ij} = [(uwvz)^n u(yvzu)^n]_{ij},$$

so

$$[(uwvz)^n uwvzu(yvzu)^n]_{ij} \subseteq [(uwvz)^n u(yvzu)^n]_{ij}.$$

Conversely, u_{rs} can also be written as a sum of terms, each of which contains a factor of the form u_{tt}. As $u_{tt} = e_t = u_{tt} w_{tt} v_{tt} z_{tt} u_{tt}$, one obtains

$$[(uwvz)^n u(yvzu)^n)]_{ij} \subseteq [(uwvx)^n uwvzu(yvzu)^n]_{ij},$$

so

$$[(uwvz)^n u(yvzu)^n]_{ij} = [(uwvx)^n uwvzu(yvzu)^n]_{ij},$$

as claimed. □

Lemma 3.2. *Let $M = \Diamond(M_1, \ldots, M_k)$, where $M_1, \ldots, M_k \in \boldsymbol{J}_1$. Then $C(M)$ divides a finite $\boldsymbol{J}$-trivial monoid.*

Proof. Let

$$A_1 = [e, s_1, f], \qquad A_2 = [e, s_2, f],$$
$$B_1 = [f, t_1, e], \qquad B_2 = [f, t_2, e]$$

be arrows in $C(M)$. Then

$$(A_1B_1)^n A_1B_2(A_2B_2)^n = [e, (s_1ft_1e)^n s_1ft_2e(s_2ft_2e)^n, e],$$

and

$$(A_1B_1)^n(A_2B_2)^n = [e, (s_1ft_1e)^n(s_2ft_2e)^n, e].$$

Let $x_1 = es_1f$, $x_2 = es_2f$, $y_1 = ft_1e$, and $y_2 = ft_2e$. Observe that, in general, if M is a monoid and β a morphism from M into an idempotent and commutative monoid N, then, whenever $x \in M_e$, $x\beta$ is above $e\beta$ in the semilattice N. In the present instance, $e \in M_f$ and $f \in M_e$. Thus if $\psi : \Diamond(M_1, \ldots, M_k) \to M_1 \times \cdots \times M_k$ is the projection morphism, $e\psi = f\psi = esf\psi$ for any $[e, s, f] \in \mathrm{Hom}(C(M))$. Thus e, f, x_1, x_2, $y_1, y_2 \in (e\psi)\psi^{-1}$, so, by Lemma 3.1, there exists an n such that

$$e(s_1ft_1e)^n s_1ft_2e(s_2ft_2e)^n$$
$$= e(x_1fy_1)^n e(x_2fy_2e)^n = e(s_1ft_1e)^n(s_2ft_2e)^n.$$

Thus,

$$(A_1B_1)^n A_1B_2(A_2B_2)^n = (A_1B_1)^n(A_2B_2)^n.$$

By Proposition 2.1, $C(M)$ is covered by a finite $\boldsymbol{J}$-trivial monoid. □

The proof of Theorem 2.2 can now be completed. If $M \in \boldsymbol{V}_2 = \boldsymbol{J}_1$, then M divides a generalized Schützenberger product N of idempotent and commutative monoids. It is easy to verify that $C(M) < C(N)$, and the result follows from Lemma 3.2 and the transitivity of category division. □

4. The congruence $\cong$ and its properties

Let A be an alphabet with two letters; $A = \{a, b\}$. No distinction will be made between a congruence on A^* and the morphism from A^* onto the quotient monoid by this congruence. Thus, if φ is a morphism defined on A^*, I write $w\varphi = w'\varphi$ or $w\varphi w'$ to mean the same thing. Similarly, if $\cong$ is a congruence on A^*, then $w\cong$ denotes the congruence class of w.

Given a surjective morphism $\varphi: A^* \to M$, where M is a finite aperiodic monoid, I will construct a congruence $\cong$ on A^* having certain properties relative to the morphism φ. These properties will then be used in the next section to prove Theorem 2.3.

Every $w \in A^*$ has a unique factorization $w = w_k \dots w_1$, where $k \geq 0$; $|w_i| > 0$ for each i; each w_i consists either entirely of a's or entirely of b's; and adjacent factors do not contain the same letter. The words w_i will be called the *blocks* of w, and the factorization given above will be called the *block factorization* of w. Let $T = |M|$. Since M is aperiodic, $m^T = m^{T+1}$ for all $m \in M$. Two words $w_1, w_2 \in a^* \cup b^*$ are said to be of *equivalent threshold* T if w_1 and w_2 have the same set of letters, and either $|w_1| = |w_2|$ or $|w_1|, |w_2| \geq T$. I write $w_1 \equiv w_2$ to denote this. Observe that $w_1 \equiv w_2$ implies $w_1\varphi = w_2\varphi$.

I define an equivalence relation $\cong$ on A^* as follows: Let $v, w \in A^*$, and let

$$v = v_k \dots v_1, \qquad w = w_p \dots w_1$$

be their block factorizations. Then $v \cong w$ if and only if k and p are both less than, or both greater than or equal to, $2T$ and $v_i \equiv w_i$ for $i = 1, \dots, \min(k, 2T)$. The remainder of this section is devoted to establishing certain properties of the equivalence relation $\cong$.

Lemma 4.1. *$\cong$ is a congruence of finite index on A^*.*

Proof. The $\cong$-class of a word $w \in A^*$ is determined by the k-tuple whose ith component is the $\equiv$-class of w_i, where k is the number of blocks of w if w has no more than $2T$ blocks, and where $k = 2T+1$ otherwise. Since $\cong$ has finite index, it follows that $\cong$ has finite index as well. Furthermore, it is easy to verify that if $v \cong w$, then $va \cong wa$, $vb \cong wb$, $av \cong aw$, and $bv \cong bw$. Thus $\cong$ is a congruence. □

A monoid is said to be $\boldsymbol{L}$-trivial if each of its $\boldsymbol{L}$-class has one element; that is, if distinct elements generate distinct principal left ideals. The family $\boldsymbol{L}$ of all finite $\boldsymbol{L}$-trivial monoids forms a pseudovariety of finite monoids. Observe that $\boldsymbol{J} \subseteq \boldsymbol{L} \subseteq \mathbf{DA}$, so that $\Diamond \boldsymbol{L} = \boldsymbol{V}_2$.

Lemma 4.2. *$A^*/\cong \in \boldsymbol{L}$.*

Proof. One easily verifies that for $u, v, w \in A^*$, $uvw \cong w$ implies $vw \cong w$, from which the result follows. □

Lemma 4.3. *Let $w \in A^*$, let $w = w_k \dots w_1$ be the block factorization of w, and let $k > 2T$. Then there is an idempotent $e \in M$ such that*

(i) *$w = uv$ where $v = w_j \dots w_1$ for some $j < 2T$, and $(w_T \dots w_{j+1})\varphi e = (w_T \dots w_{j+1})\varphi$;*

(ii) *$M_e = M$.*

Proof. Let $z_i = w_{2i}w_{2i-1}$ for $i = 1, \ldots, T$. If the products $z_T\varphi$, $(z_T z_{T-1})\varphi, \ldots,$ $(z_T \ldots z_1)\varphi$ are all distinct, then all the elements of M appear among them, and thus there is an idempotent $e = (z_T \ldots z_r)\varphi$ among them. Since $z_T \ldots z_r$ contains both a and b, $M_e = M$. Thus the result follows with

$$u = w_k \ldots w_{2T+1} z_T \ldots z_r, \qquad v = z_{r-1} \ldots z_1,$$

and $j = 2(r-1)$. If the products are not all distinct, then $(z_T \ldots z_r)\varphi = (z_T \ldots z_s)\varphi$ for some $s < r$. Since some power $e = [(z_{r-1} \ldots z_s]\varphi]^p$ is idempotent, the result follows as above. □

Now consider an arbitrary linear ordering on the set of idempotents of M. Let $w \in A^*$ be a word with more than $2T$ blocks. Choose a factorization $w = uv$ satisfying the conditions of the preceding lemma with j as large as possible, and choose e to be the least idempotent that satisfies the conditions of the lemma for this particular choice of j. Then $w = uv$ will be called the *standard factorization* of w, and e the *associated idempotent* of w.

Lemma 4.4. *Let $w \cong w'$, and suppose w and w' both have more than $2T$ blocks. Let $w = uv$, $w' = u'v'$ be the standard factorizations, and let e and e' be the associated idempotents. Then*

(i) *v and v' have the same number of blocks*;
(ii) $v\varphi = v'\varphi$;
(iii) $e = e'$;
(iv) $uv' \cong u'v \cong w \cong w'$.

Proof. (i), (ii), and (iii) result from the fact that if $x, y \in a^* \cup b^*$ are $\equiv$-equivalent, then $x\varphi = y\varphi$. (iv) is then immediate from the definition of the congruence. □

5. Proof of Theorem 2.3

Before proceeding to the proof I will establish a characterization, in terms of congruences, of the operation that passes from a pseudovariety $\boldsymbol{V}$ to the pseudovariety $\Diamond \boldsymbol{V}$; and a characterization of categories that divide finite monoids belonging to a given pseudovariety $\boldsymbol{V}$.

Let B be a finite alphabet, let β be a congruence on B^*, and let $k \geqslant 0$. An equivalence relation $[\beta, k]$ on B^* is defined as follows: If $w_1, w_2 \in B$; then $w_1 \subset_{[\beta,k]} w_2$, if, for each factorization,

$$w_1 = v_0 a_1 v_1 \ldots a_r v_r$$

with $r \geqslant k$; $v_i \in B^*$ for $i = 0, \ldots, r$, and $a_i \in B$ for $i = 1, \ldots, r$; there exists a factorization

$$w_2 = u_0 a_1 u_1 \ldots a_r u_r$$

such that $u_i \beta v_i$ for $i = 0, \ldots, r$. $w_1[\beta, k]w_2$ if and only if both $w_1 \subset_{[\beta,k]} w_2$ and $w_2 \subset_{[\beta,k]} w_1$. Thérien [26] showed that $[\beta, k]$ is a congruence on B^*, and that $[\beta, k]$ has finite index if β does. Observe that $[\beta, 0] = \beta$ and that $[\beta, k+1]$ refines $[\beta, k]$ for $k \geqslant 0$.

Lemma 5.1. *Let $\mathbf{V}$ be a pseudovariety of finite monoids and let M be a finite monoid. $M \in \Diamond \mathbf{V}$ if and only if, for every morphism $\varphi : B^* \to M$ where B is a finite alphabet, there exists a congruence β on B^* and an integer $k \geqslant 0$ such that $B^*/\beta \in \mathbf{V}$ and $[\beta, k]$ refines φ.*

Proof. I first note two properties of the generalized Schützenberger product:

(i) If $L_0, \ldots, L_k \subseteq B^*$ are languages and $b_1, \ldots, b_k \in B$, then

$$M(L_0 b_1 L_1 \ldots b_k L_k) \prec \Diamond(M(L_0), \ldots, M(L_k)).$$

The proof is a slight variation of that of a proposition in [22], in which the letters b_i are not present. One defines a map $\eta : B^* \to \Diamond(M(L_0), \ldots, M(L_k))$ by setting $(w\eta)_{ij}$ to be the set of all $(j-i+1)$-tuples $(w_i\eta_i, \ldots, w_j\eta_j)$, where $\eta_t : B^* \to M(L_t)$ is the syntactic morphism, and $w = w_i b_{i+1} w_{i+1} \ldots b_j w_j$. (Here the rows and columns of the matrices that make up the Schützenberger product are indexed by the integers $0, \ldots, k$.) It can then be shown that η is a morphism, and that $L_0 b_1 L_1 \ldots b_k L_k = X\eta^{-1}$ for some $X \subseteq \Diamond(M(L_0), \ldots, M(L_k))$, so $M(L_0 b_1 L_1 \ldots b_k L_k) \prec \Diamond(M(L_0), \ldots, M(L_k))$.

(ii) Let $\eta : B^* \to \Diamond(M_0, \ldots, M_k)$ be a morphism. Then, for any $m \in \Diamond(M_0, \ldots, M_k)$, $m\eta^{-1}$ is a boolean combination of sets of the form $L_0 b_1 L_1 \ldots b_k L_k$, where $M(L_i) \prec M_i$ for $i = 0, \ldots, k$ and $b_i \in B$ for $i = 1, \ldots, k$. This fact is proved in [15].

Now suppose that M satisfies the second condition in the statement of the lemma. Let $\varphi : B^* \to M$ be a surjective morphism, and let $[\beta, k]$ be a congruence that refines φ, with $B^*/\beta \in \mathbf{V}$. It is easy to see that each $[\beta, k]$-class is a boolean combination of sets of the form $L_0 b_1 L_1 \ldots b_k L_k$, where each L_i is a β-class; and that, for any $m \in M$, $m\varphi^{-1}$ is a union of $[\beta, k]$-classes. Since the syntactic monoid of each β-class belongs to $\mathbf{V}$ and since M divides the direct product of the syntactic monoids of the languages $m\varphi^{-1}$ where the product ranges over all $m \in M$ (see [22]), it follows from fact (i) that $M \in \Diamond \mathbf{V}$.

Conversely, suppose $M \in \Diamond \mathbf{V}$ and let $\varphi : B^* \to M$ be a morphism. Then φ factors through a morphism $\psi : B^* \to \Diamond(M_0, \ldots, M_k)$, where $M_i \in$ for $i = 0, \ldots, k$. By fact (ii), each $m\psi^{-1}$ is a boolean combination of languages of the form $L_0 b_1 L_1 \ldots b_k L_k$, where $M(L_i) \prec M_i$ for $i = 0, \ldots, k$. Let β be the intersection of the syntactic congruences of all the L_i that arise in this fashion. Then $B^*/\beta \in \mathbf{V}$. Furthermore, if $w_1[\beta, k]w_2$ and $w_1 \in L = L_0 b_1 L_1 \ldots b_k L_k$, then $w_2 \in L$. Thus $[\beta, k]$ refines ψ, so $[\beta, k]$ refines φ. □

Let ω be the universal congruence on B^*; that is, $w_1 \omega w_2$ for all $w_1, w_2 \in B^*$. In the notation used here, Simon's theorem on $\mathbf{J}$-trivial monoids states that a finite

monoid M is $\mathbf{J}$-trivial if and only if for every morphism $\varphi: B^* \to M$ there exists a $k \geqslant 0$ such that $[\omega, k]$ refines φ. By the preceding lemma, this is equivalent to the assertion $\mathbf{J} = \Diamond\mathbf{1}$, where $\mathbf{1}$ denotes the pseudovariety consisting of the trivial monoid alone.

Let C be a finite category and let G be a set of arrows of C. G *generates* C if every arrow of C is a product of arrows in G. I say that an arrow in C is *represented* by a word in G^* if the arrow is obtained by multiplying, in C, the successive letters in the word. In addition, I stipulate that any identity arrow of C is represented by the empty word of G^*.

Lemma 5.2. *Let $\mathbf{V}$ be a pseudovariety of finite monoids, C a category, and G a set of arrows that generates C. Then the following are equivalent*:

(i) *There exists a finite monoid M such that $C < M$ and $M \in \mathbf{V}$.*

(ii) *There exists a congruence β on G^* such that $G^*/\beta \in \mathbf{V}$. Further, if x, y are coterminal arrows of C represented by $u, v \in G^*$ respectively and if $u\beta v$, then $x = y$.*

Proof. (i)$\Rightarrow$(ii): For each $g \in G$, let $g\beta$ be any element of M that covers g. This defines a morphism $\beta: G^* \to M$, and thus $G^*/\beta \in \mathbf{V}$. If x, y are coterminal arrows of C represented respectively by u and v, then, by the definition of category division, $u\beta$ covers x and $v\beta$ covers y; thus if $u\beta = v\beta$, then $x = y$.

(ii)$\Rightarrow$(i); Let $M = G^*/\beta$. By assumption, $M \in \mathbf{V}$. For each arrow x of C let $M_x = \{u\beta \mid u \text{ represents } x\}$. If x and y are consecutive arrows represented respectively by u and v, then uv represents xy, so $u\beta \cdot v\beta = (uv)\beta \in M_{xy}$. If x and y are coterminal arrows covered by the same element of M, then they are represented by β-equivalent elements of G^*, so, by assumption, $x = y$. Since the empty word represents every identity arrow in C, each identity arrow is covered by the identity of M. Thus $C < M$. □

If M and N are finite monoids and $\varphi: B^* \to M$, $\eta: B^* \to N$ are morphisms with φ surjective, there results a *relational morphism* $\gamma = \varphi\eta^{-1}: M \to N$ (see [31]). The *derived category* [32] of γ, denoted D_γ, is defined as follows: $\mathrm{Obj}(D_\gamma) = \{w\eta \mid w \in B^*\}$. The arrows of D_γ are equivalence classes of triples $(w\eta, v, (wv)\eta)$, where $v, w \in B^*$, and where two triples $(w\eta, v_i, (wv_i)\eta)$, $i = 1, 2$, are equivalent if and only if, for all $w' \in B^*$ with $w'\eta = w\eta$, one has $(w'v_1)\varphi = (w'v_2)\varphi$. As before, the equivalence class of $(w\eta, v, (wv)\eta)$ is denoted $[w\eta, v, (wv)\eta]$. Consecutive triples $(w\eta, v_1, (wv)\eta)$ and $((wv_1)\eta, v_2, (wv_1v_2)\eta)$ are multiplied by setting their product to be $(w\eta, v_1v_2, (wv_1v_2)\eta)$. It is easy to see that this product is associative and compatible with the equivalence relation, and that $[w\eta, 1, w\eta]$ is the identity at $w\eta$. Thus D_γ is a category. Observe that D_γ is generated by the set of arrows $G = \{[w\eta, b, (wb)\eta] \mid b \in B\}$.

Proposition 5.3. *Let φ, η, γ be as above. If D_γ divides a finite $\mathbf{J}$-trivial monoid, then φ is refined by $[\eta, k]$ for some k.*

Proof. By Proposition 5.2 and Simon's theorem, there exist a $k \geqslant 0$ such that if two coterminal paths in D_γ, viewed as words in G^*, are congruent modulo $[\omega, k]$, then they represent the same arrow. Now let $w, w' \in B^*$, and suppose $w[\eta, k]w'$. Let $w = b_1 \ldots b_r$ and $w' = b'_1 \ldots b'_s$, where each b_i and b'_j is in B. Consider the paths $X = c_1 \ldots c_r$, $Y = c'_1 \ldots c'_s$, where

$$c_i = [(b_1 \ldots b_{i-1})\eta, b_i, (b_1, \ldots, b_i)\eta]$$

and

$$c'_i = [(b'_1 \ldots b'_{i-1})\eta, b'_i, (b'_i, \ldots, b'_i)\eta].$$

X and Y are words in G^* that represent the arrows $x = [1, w, w\eta]$ and $y = [1, w', w'\eta]$ respectively. Since $w\eta = w'\eta$, x and y are coterminal. Let $c_{i_1} \ldots c_{i_p}$ be a subword (that is, a subsequence) of X with $p \leqslant k$. Then w has a factorization $w = w_0 b_{i_1} w_1 \ldots b_{i_p} w_p$, where $w_0 = b_1 \ldots b_{i_1 - 1}$, $w_0 b_{i_1} w_1 = b_1 \ldots b_{i_2 - 1}$, etc. Since $w[\eta, k]w'$, w' has a factorization $w' = w'_0 b_{i_1} \ldots b_{i_p} w'_p$, where $w_j \eta w'_j$ for $j = 0, \ldots, p$. Thus Y contains the subword $d_1 \ldots d_p$, where

$$\begin{aligned} d_j &= [(w'_0 b_{i_1} \ldots w'_{i_j - 1})\eta, b_{i_j}, (w'_0 b_{i_1} \ldots w'_{i_j - 1} b_{ij})\eta] \\ &= [(w_0 b_{i_1} \ldots w_{i_j - 1})\eta, b_{ij}, (w_0 b_{i_1} \ldots w_{i_j - 1} b_{i_j})\eta] = c_{i_j}. \end{aligned}$$

So $c_{i_1} \ldots c_{i_p}$ is a subword of Y. In the same way one shows that every subword of Y of length no more than k is a subword of X. Thus $x = y$, so $w\varphi = w'\varphi$, hence $[\eta, k]$ refines φ, as claimed. □

Proposition 5.4. *Let $A = \{a, b\}$, let $\varphi : B^* \to M$ be a surjective morphism with M finite and suppose $C(M)$ divides a finite $\mathbf{J}$-trivial monoid. Let $\gamma = \varphi^{-1} \cong$ (where $\cong$ is as defined in Section 4). Then D_γ divides a finite $\mathbf{J}$-trivial monoid.*

Proof. By the "Bonded Component Theorem" of [32] it suffices to verify that each strongly-connected subcategory of D_γ divides a finite $\mathbf{J}$-trivial monoid.

First, observe that if $C(M)$ divides a finite $\mathbf{J}$-trivial monoid, then each *base monoid* $\mathrm{Hom}_{C(M)}(e, e) = eM_e e$ is a divisor of $C(M)$, hence itself a $\mathbf{J}$-trivial monoid. In particular, since very group in M belongs to one of these base monoids, M is aperiodic.

If $w_1 \in A^*$ has more than $2T$ blocks, where $T = |M|$, and w_2 has no more than $2T$ blocks, then $w_1 \cong$ and $w_2 \cong$ cannot belong to the same strongly connected component of D_γ. Furthermore, suppose w_1 and w_2 have no more than $2T$ blocks and that their $\cong$-classes belong to the same strongly connected component. Then $w_1 \cong w_2$, and the only arrows in the component are of the form $[w_1 \cong, a^r, w_1 \cong]$, $r \geqslant 0$ (if the rightmost block of w_1 contains at least T a's), or $[w_1 \cong, b^r, w_1 \cong]$, $r \geqslant 0$ (if the rightmost block

of w_1 contains at least T b's), or $[w_1 \cong, 1, w_1 \cong]$ (if the rightmost block of w_1 has length less than T). Thus if $w \in A^*$ contains fewer than $2T$ blocks, the strongly connected component of $w \cong$ is a one-object category isomorphic to a cyclic aperiodic monoid, and any such monoid is J-trivial.

All the remaining strongly connected components are contained in the subcategory D of D_γ whose set of objects consists of all $w \cong$ such that w has more than $2T$ blocks, and whose arrows are all the arrows in D_γ between these objects. It is then sufficient to show that D divides a finite J-trivial monoid.

Suppose then that $w \in A^*$ has more than $2T$ blocks. Let $w = uv$ be the standard factorization, and $e \in M$ the associated idempotent, as defined in Section 4. By Lemma 4.3, $M_e = M$, and by Lemma 4.4, the map ψ taking $w \cong$ to e is a well-defined map from Obj(D) to Obj($C(M)$). Let $t = [w_1 \cong, x, w_2 \cong]$ be an arrow of D, let $w_1 = u_1 v_1$, $w_2 = u_2 v_2$ be the standard factorizations, and let e_1, e_2 be the associated idempotents. The set M_t of arrows of $C(M)$ that cover t is defined to be the set of all $[e_1, m, e_2]$ such that

(i) $m \in e_1 M e_2$;

(ii) for any $w \cong w_1$ with standard factorization $w = uv$, $(wx)\varphi = u\varphi \cdot m \cdot v_2\varphi$.

To complete the proof it must be verified that this covering relation satisfies the conditions of the definition of category division.

I first show that $M_t \neq \emptyset$. Let $w_1 x = u'v'$ be the standard factorization. By Lemma 4.4, $u'\varphi e_2 = u'\varphi$ and $v_2\varphi = v'\varphi$. It follows from the manner in which e_1 was chosen that u_1 is an initial segment of u', and thus $w_1 x = u_1 q v'$ for some $q \in A^*$. Let $m = e_1 \cdot q\varphi \cdot e_2$. Now, let $w \cong w_1$ with standard factorization $w = uv$. By Lemma 4.4, $u_1 v_1 \cong uv_1$, so $u_1 v_1 x \cong uv_1 x = uqv'$. It follows from Lemma 4.4 and the fact that the standard factorization of a word falls on the boundary between blocks, that $(uq) \cdot v'$ is the standard factorization of $uv_1 x$, and thus $(uq)\varphi \cdot e_2 = (uq)\varphi$. Since $v\varphi = v_1\varphi$ (again by Lemma 4.4), it follows that

$$(wx)\varphi = (uvx)\varphi = (uv_1 x)\varphi = u\varphi \cdot e_1 \cdot q\varphi \cdot e_2 \cdot v'\varphi = u\varphi \cdot m \cdot v'\varphi = u\varphi \cdot m \cdot v_2\varphi.$$

Thus $[e_1, m, e_2] \in M_t$.

I now show that the covering relation is injective. Let $s_1 = [e_1, m_1, e_2] \in M_{t_1}$, $s_2 = [e_1, m_2, e_2] \in M_{t_2}$, where $t_i = [w_1 \cong, x_i, w_2 \cong]$, and suppose $s_1 = s_2$. Then $m_1 = e_1 m_1 e_2 = e_1 m_2 e_2 = m_2$. Thus, with the notations as before, for any $w \cong w_1$,

$$(wx_1)\varphi = u\varphi \cdot m_1 \cdot v_2\varphi = u\varphi \cdot m_2 \cdot v_2\varphi = (wx_2)\varphi,$$

so $t_1 = t_2$.

To show that the covering relation is multiplicative, let

$$t_1 = [w_1 \cong, x_1, w_2 \cong], \qquad t_2 = [w_2 \cong, x_2, w_3 \cong],$$

and let $s_i = [e_i, m_i, e_{i+1}] \in M_{t_i}$. Then $s_1 s_2 = [e_1, m_1 m_2, e_2]$, and $t_1 t_2 = [w_1 \cong, x_1 x_2, w_2 \cong]$. Let $w \cong w_1$. With the notations as before, $(wx_1 x_2)\varphi = u\varphi \cdot m_1 \cdot v_2\varphi \cdot x_2\varphi$. It is then possible to choose, as in the proof that M_t is nonempty,

a word q so that $(uq)\varphi e_2 = (uq)\varphi$, $m_1 = e_1 \cdot \varphi \cdot e_2$, and $uqv_2 \cong wx_1$. Thus,

$$u\varphi \cdot m_1 \cdot x_2\varphi = u\varphi \cdot q\varphi \cdot m_2 \cdot v_3\varphi = u\varphi \cdot m_1 \cdot m_2 \cdot v_3\varphi,$$

which shows $s_1 s_2 \in M_{t_1 t_2}$.

Finally, for any $w\cong \in \mathrm{Obj}(D)$, the identity at $w \cong$ is $[w \cong, 1, w \cong]$, which is covered by $t = [e, e, e]$ where e is the associated idempotent of w. Thus t is the identity at $e \in \mathrm{Obj}(C(M))$, completing the proof that $D \prec C(M)$. □

To conclude the proof of Theorem 2.3, let $\varphi : A^* \to M$ be a surjective morphism and suppose $C(M)$ divides a finite J-trivial monoid N. As noted in the proof of Proposition 5.4, M is aperiodic. By Propositions 5.3 and 5.4, $[\cong, k]$ refines φ for some k, so by Lemmas 4.2 and 5.1, $M = A^*/\varphi \in \Diamond \boldsymbol{L} = \boldsymbol{V}_2$. □

6. Prospects for a general solution

Let $\boldsymbol{V}$ be a pseudovariety of finite monoids, let $C_{\boldsymbol{V}}$ be the collecton of all finite monoids M such that $C(M)$ divides a member of $\boldsymbol{V}$, and let $\boldsymbol{M}_2$ be the collection of all finite monoids generated by two elements. Proposition 5.4 shows that if $M \in C_{\boldsymbol{J}} \cap \boldsymbol{M}_2$, then there is a relational morphism γ from M into a finite $\boldsymbol{L}$-trivial monoid such that D_γ divides a finite $\boldsymbol{J}$-trivial monoid. It follows from results in [32], connecting the derived category and the wreath product, that M belongs to the product variety $\boldsymbol{J} * \boldsymbol{L}$. Thus,

$$C_{\boldsymbol{J}} \cap \boldsymbol{M}_2 \subseteq \boldsymbol{J} * \boldsymbol{L}.$$

Proposition 5.3 shows, in essence, that

$$\boldsymbol{J} * \boldsymbol{V} \subseteq \Diamond \boldsymbol{V}$$

for any pseudovariety $\boldsymbol{V}$, and Theorem 2.2 states that $\Diamond \boldsymbol{J} \subseteq C_{\boldsymbol{J}}$. Thus

$$C_{\boldsymbol{J}} \cap \boldsymbol{M}_2 = (\boldsymbol{J} * \boldsymbol{L}) \cap \boldsymbol{M}_2 = \boldsymbol{V}_2 \cap \boldsymbol{M}_2.$$

Of course, one would like to show that $C_{\boldsymbol{J}} \subseteq \boldsymbol{J} * \boldsymbol{L}$ holds in general, thus providing a solution to the decision problem for dot-depth two and a decomposition of $\boldsymbol{V}_2$ as a product variety. Unfortunately, there are serious obstacles to a generalization in precisely this form. The definitions of $C(M)$ and the derived category are asymmetrical, which is a bit unsettling in light of the fact that $\boldsymbol{V}_2$ is closed under reversal. In order to use the derived category effectively in the arguments in Section 5, it was necessary to show that if two words were $\cong$-equivalent, then the right-hand factors in their standard factorizations had the same image in M; and this in turn depended enormously on the fact that the alphabet A had only two letters. I now believe that $C_{\boldsymbol{J}} \subseteq \boldsymbol{J} * \boldsymbol{L}$ is false in general.

A possible solution to the dilemma is the use of a symmetrical generalization of the derived category and the product of pseudovarieties. Rhodes and Tilson [18]

have studied the "block product", or two-sided semidirect product $\boldsymbol{V} \square \boldsymbol{W}$ of two pseudovarieties of finite monoids. In this connection they associate with every relational morphism $\gamma: M \to N$ a cateogry K_γ, called the *kernel* of γ, with the following property: A monoid M belongs to the block product $\boldsymbol{V} \square \boldsymbol{W}$ if and only if there is a relational morphism $\gamma: M \to N \in \boldsymbol{W}$ such that K_γ divides a member of $\boldsymbol{V}$. In general, $K_\gamma \prec D_\gamma$, so the block product of two pseudovarieties contains their product (see [18] for the precise definitions). In order to prove that a monoid M belongs to $\Diamond \boldsymbol{V}$, it is sufficient to show that M belongs to the block product $\boldsymbol{J} \square \boldsymbol{LI}^{-1}\boldsymbol{V}$. Here $\boldsymbol{LI}^{-1}\boldsymbol{V}$ denotes the pseudovariety consisting of all finite monoids M for which there exists a relational morphism $\eta: M \to T \in \boldsymbol{V}$ such that, for each idempotent $e \in M$, $e\eta^{-1}$ is a nilpotent extension of a rectangular band. It follows from a result of Pin, Straubing and Thérien [17] characterizing the languages in $\boldsymbol{LI}^{-1}\boldsymbol{V}$, and an argument much like that of Proposition 5.3, that $\boldsymbol{J} \square \boldsymbol{LI}^{-1}\boldsymbol{V} \subseteq \Diamond \boldsymbol{V}$. In particular, it is known that $\boldsymbol{LI}^{-1}\boldsymbol{J}_1 = \mathbf{DA}$, a pseudovariety that was defined in Section 3.

This suggests that one ought to define a more symmetrical category $C'(M)$ having the following property: There is a monoid $N \in \mathbf{DA}$ and a relational morphism $\gamma: M \to N$ such that if $C'(M)$ divides a finite $\boldsymbol{J}$-trivial monoid, then K_γ divides a finite $\boldsymbol{J}$-trivial monoid. This property is entirely analogous to Proposition 5.4, with $\mathbf{DA}$ replacing $\boldsymbol{L}$, and the kernel replacing the derived category. A good candidate for $C'(M)$ is the category formed by taking the direct product of $C(M)$ with its dual $\overline{C(M)}$, where the objects of $\overline{C(M)}$ are the idempotents of M, and the arrows are equivalence classes of triples (e, s, f), where $s, f \in P_e$. We conjecture that $C'(M)$, or something very much like it, has the property just mentioned. It would then follow that $M \in \boldsymbol{V}_2$ if and only if $C'(M)$ divides a finite $\boldsymbol{J}$-trivial monoid, and as long as $C'(M)$ is effectively constructible (as in the candidate discussed here), this yields an effective procedure for determining whether a given monoid M belongs to $\boldsymbol{V}_2$.

There is some hope of extending this sort of reasoning to treat higher levels of the hierarchy. Indeed, one can write down a list of "axioms", which, if satisfied, yield a solution to the general problem. This is done in the proposition below. Of the four axioms listed, (i)-(iii) appear to be quite general, so the principal difficulty is likely to be in finding a category $C'(M)$ and a congruence $\cong$ that satisfy (iv) below.

Proposition 6.1. *Suppose that for each finite monoid M there is a category $C'(M)$ having the following properties.*

(i) *$C'(M)$ is effectively constructible from the multiplication table of M.*

(ii) *If $\boldsymbol{V}$ and $\boldsymbol{W}$ are pseudovarieties such that $M \in \boldsymbol{V}$ implies $C'(M)$ divides a member of $\boldsymbol{W}$, then $M \in \Diamond \boldsymbol{V}$ implies $C'(M)$ divides a member of $\Diamond \boldsymbol{W}$.*

(iii) *$C'(M)$ divides the trivial monoid if and only if $M \in \boldsymbol{U}$, where $\boldsymbol{U}$ is a pseudovariety between $\mathbf{J}_1$ and $\mathbf{DA}$.*

(iv) *If A is a finite alphabet, and $\varphi: A^* \to M$ a morphism with M aperiodic, then there is a congruence $\cong$ on A^* such that $A^*/\varphi \in \mathbf{DA}$ and every bonded component of $K_{\varphi^{-1}\cong}$ divides $C'(M)$.*

Then for all $k \geqslant 2$, $\boldsymbol{V}_k = \boldsymbol{J} \square \boldsymbol{LI}^{-1}\boldsymbol{V}_{k-1}$ *and* $M \in \boldsymbol{V}_k$ *if and only if* $C'(M)$ *divides a member of* $\boldsymbol{V}_{k-1}$. *In particular, it is decidable whether a given finite monoid belongs to* $\boldsymbol{V}_k$.

Sketch of proof. It follows from (ii) and (iii) that $M \in \boldsymbol{V}_2 = \Diamond \boldsymbol{U}$ implies that $C'(M)$ divides a member of $\boldsymbol{J} = \boldsymbol{V}_2$ and from (iv) that if $C'(M)$ divides a member of $\boldsymbol{J}$, then $M \in \boldsymbol{J} \square \mathbf{DA} \subseteq \Diamond \mathbf{DA} = \boldsymbol{V}_2$. This gives the characterization in the case $k = 2$.

Now suppose that the conclusion holds for some $\boldsymbol{V}_{k-1}$ where $k > 2$. If $M \in \boldsymbol{V}_k = \Diamond \boldsymbol{V}_{k-1}$, then, by (ii) and the inductive hypothesis, $C'(M)$ divides a member of $\Diamond \boldsymbol{V}_{k-2} = \boldsymbol{V}_{k-1}$. Conversely if $C'(M)$ divides a member of $\boldsymbol{V}_{k-1}$, then

$$\begin{aligned} M &\in \boldsymbol{V}_{k-1} \square \mathbf{DA} \\ &= (\boldsymbol{J} \square \boldsymbol{LI}^{-1}\boldsymbol{V}_{k-2}) \square \mathbf{DA} \\ &\subseteq \boldsymbol{J} \square \boldsymbol{LI}^{-1}(\boldsymbol{V}_{k-2} \square \mathbf{DA}) \\ &\subseteq \boldsymbol{J} \square \boldsymbol{LI}^{-1}\boldsymbol{V}_{k-2} \\ &\subseteq \Diamond \boldsymbol{V}_{k-1} = \boldsymbol{V}_k. \end{aligned}$$

The first line above follows from property (iv), the second from the inductive hypothesis, the third from a partial associativity result concerning the block product proved in [18]. The fourth line, in which $\boldsymbol{LI}^{-1}$ is taken outside the parentheses, can be proved by a simple computation using known properties of the block product. The fifth line follows by noting that the inductive argument has also proved

$$\boldsymbol{V}_{k-1} \square \mathbf{DA} = \boldsymbol{V}_k.$$

The final line is the result of observations made earlier in this section.

Decidability in the case $k = 2$ follows from Proposition 2.1. To prove the decidability in higher cases it suffices to have an effective criterion for determining whether a finite category divides a member of $\boldsymbol{V}_k$ when $k > 1$. But if $k > 1$, $\boldsymbol{V}_k$ contains the six-element aperiodic monoid consisting of the identity, a zero, and a 2×2 regular $\boldsymbol{J}$-class with exactly two idempotents. In this instance one can show (see [32]) that a category C divides a member of $\boldsymbol{V}_k$ if and only if a certain monoid, effectively constructible from C, is in $\boldsymbol{V}_k$. The decidability of $\boldsymbol{V}_k$ then follows by induction. □

7. Historical note

The connection between finite categories and monoids is implicit in the work of McNaughton [12] and Brzozowski and Simon [4] on locally testable sets. "Graph congruences" were used by Eilenberg [6, Chapter VIII], and later by Knast [9] in the study of some problems concerning recognizable languages. The finite categories studied here are in fact quotients of a free category by these graph congruences. The beginnings of a general theory of graph congruences were developed by Thérien

and Weiss [28], and some of their results were incorporated into the fundamental work of Tilson [32], in which it is explicitly recognized that the structures involved are indeed categories. The definitions of category division and the derived category of a relational morphism come from Tilson's paper.

Constructions related to the category $C(M)$, as well as the notations P_e and M_e, appear in a paper of Brzozowski and Fich [7], who study monoids M that satisfy conditions of the form $eM_ee \in \boldsymbol{V}$ for various pseudovarieties $\boldsymbol{V}$. The monoids eM_ee are, of course, the base monoids of the category $C(M)$. These authors, in a result quite similar to Theorem 2.3, show $eM_ee \in \boldsymbol{J}_1$ for all $e \in E(M)$ if and only if $M \in \boldsymbol{J}_1 * \boldsymbol{L}$, provided M is generated by two elements. In fact, a category divides a member of $\boldsymbol{J}_1$ if and only if its base monoids are in $\boldsymbol{J}_1$, so this theorem is the precise analogue of Theorem 2.3 with $\boldsymbol{J}$ replaced by $\boldsymbol{J}_1$.

The proof of Proposition 5.4 is an adaptation of the proof of the "Delay Theorem" of [32], which also appears, stated in different language, in [23]. Again, the ultimate source for arguments of this kind is the work on locally testable languages in [4, 12].

Acknowledgment

I am grateful to John Rhodes and Bret Tilson for sharing with me their work on categories and block products while it was still in its formative stage, and to Stuart Margolis, Jean-Eric Pin and Denis Thérien for informative discussions.

References

[1] D. Barrington and D. Thérien, Finite monoids and the fine structure of NC^1 in: *Proc. 19th ACM STOC*, New York (1987) 101-109.

[2] J.A. Brzozowski and R. Cohen, Dot-depth of star-free events, *J. Comput. System Sci.* **5** (1971) 1-16.

[3] J.A. Brzozowski and R. Knast, The dot-depth hierarchy of star-free events is infinite, *J. Comput. System Sci.* **16** (1978) 37-55.

[4] J.A. Brzozowski and I. Simon, Characterizations of locally testable events, *Discrete Math.* **4** (1973) 243-271.

[5] J.R. Büchi, Weak second-order arithmetic and finite automata, *Z. Math. Logik Grundlagen Math.* **6** (1960) 66-92.

[6] S. Eilenberg, *Automata, Languages and Machines, Vol. B* (Academic Press, New York, 1976).

[7] F. Fich and J.A. Brzozowski, A characterization of a dot-depth two analogue of generalized definite languages, in: *Proc. 6th ICALP*, Graz, Austria, Lecture Notes in Computer Science **71** (Springer, Berlin, 1979) 230-244.

[8] M. Fust, J. Saxe and M. Sipser, Parity, circuits and the polynomial-time hierarchy, *Math. Systems Theory* **18** (1984) 13-27.

[9] R. Knast, A semigroup characterization of dot-depth one languages, *RAIRO Inform. Théor.* (1984).

[10] R. Ladner, Application of model-theoretic games to discrete linear orders and finite automata, *Inform. and Control* **33** (1977) 281-303.

[11] G. Lallement, *Semigroups and Combinatorial Applications* (Wiley, New York, 1979).

[12] R. McNaughton, Algebraic decision procedures for local testability, *Math. Systems Theory* **8** (1974) 60-76.

[13] R. McNaughton and S. Papert, *Counter-Free Automata* (MIT Press, Cambridge, MA, 1971).
[14] D. Perrin and J.E. Pin, First-order logic and star-free events, *J. Comput. System Sci.* **32** (1986) 393-406.
[15] J.E. Pin, Variétés de semigroupes et variétés de langages, Thèse d'Etat, Université de Paris VI, 1981.
[16] J.E. Pin and H. Straubing, Monoids of upper triangular matrices, *Colloquia Math. Soc. J. Bolyai* **39** (1985) 259-272.
[17] J.E. Pin, H. Straubing, and D. Thérien, Locally trivial categories and unambiguous concatenation, *J. Pure Appl. Algebra*, to appear.
[18] J. Rhodes and B. Tilson, The kernel of monoid morphisms: a reversal-invariant decomposition theory, Preprint, Center for Pure and Applied Mathematics, University of California, Berkeley, CA, 1987.
[19] M.P. Schützenberger, On finite monoids having only trivial subgroups, *Inform. Control* **8** (1965) 190-194.
[20] I. Simon, Piecewise testable events, in: *Proc. 2nd GI Conf.*, Lecture Notes in Computer Science **33** (Springer, Berlin, 1975).
[21] M. Sipser, Borel sets and circuit complexity, in: *Proc. 24th IEEE FOCS* (1983) 61-69.
[22] H. Straubing, A generalization of the Schützenberger product of finite monoids, *Theoret. Comput. Sci.* **13** (1981) 137-150.
[23] H. Straubing, Finite semigroup varieties of the form $\boldsymbol{V} * \boldsymbol{D}$, *J. Pure Appl. Algebra* **36** (1985) 53-94.
[24] H. Straubing, Semigroups and languages of dot-depth two, in: *Proc. 13th ICALP*, Rennes, France, Lecture Notes in Computer Science **226** (Springer, Berlin, 1986) 416-423.
[25] H. Straubing and D. Thérien, Partially ordered finite monoids and a theorem of I. Simon, Tech. Rept. SOCS-85.10, McGill University, 1985.
[26] D. Thérien, Classification of finite monoids: the language approach, *Theoret. Comput. Sci.* **14** (1981) 195-208.
[27] D. Thérien, Catégories et langages de dot-depth un, Preprint, Tech. Rept. SOCS-85-22, McGill University, 1985.
[28] D. Thérien and A. Weiss, Graph congruences and wreath products, *J. Pure Appl. Algebra* **36** (1985) 205-215.
[29] W. Thomas, Classifying regular events in symbolic logic, *J. Comput. System Sci.* **25** (1982) 360-376.
[30] W. Thomas, An application of the Ehrenfeucht-Fraïssé game in formal language theory, *Bull. Soc. Math. France* **16** (1984) 11-21.
[31] B. Tilson, [6, Chapters 11 and 12].
[32] B. Tilson, Categories as algebra, *J. Pure Appl. Algebra* **48** (1987) 83-198.