INFORMATION AND COMPUTATION 113, 1–25 (1994)

Membership Testing in Threshold One Transformation Monoids

M. BEAUDRY*

Département de Mathématiques et d'Informatique,
Université de Sherbrooke, Sherbrooke, Québec J1K 2R1, Canada

The membership problem in transformation monoids is the natural extension to the well-studied membership problem in permutation groups. We consider the restriction of the problem to the varieties of threshold one monoids, those monoids in which every element f satisfies $f^{p+1} = f$, for some integer p. We find that each of the complexity classes AC^0, NC, and P can be associated with a variety of threshold one monoids which, within the hypothesis that $NC \neq P$ and $P \neq NP$, is the unique largest variety of monoids where the membership problem can be done with this complexity. We extend our study to other cases of threshold one monoids, for which we obtain NP-completeness results. We also consider the problem which consists in deciding whether the transformation monoid of an automaton belongs to a specific variety: we show that we can do in AC^0 the characterization of monoids in three of the varieties most significant to our study of the membership problem.

1. INTRODUCTION

The *membership problem* in transformation monoids can be defined as follows:

> Given a finite set X and a set A of total mappings from X to X, plus another mapping f, decide whether f can be expressed as a composition of the elements of A.

In its general form, this problem is *PSPACE*-complete, as shown by Kozen (1977). Study of its restriction to permutation groups has been extensive, motivated by applications to other problems on permutation groups and to graph isomorphism; it was eventually shown to belong to the parallel complexity class *NC* (Sims, 1970; Furst *et al.*, 1980; McKenzie and Cook, 1987; Luks and McKenzie, 1988; Luks, 1986; Babai *et al.*, 1987). Recent work has examined the restriction of the membership problem to the case of the

* Work supported by NSERC Grant OGP0089786 and FCAR Grants 92-NC-0608 and 91-ER-0642.

0890-5401/94 $6.00

aperiodic, or group-free, monoids (Beaudry, 1988; Beaudry *et al.*, 1989); this research showed that, depending on the monoid, complexity rises from AC^0 to P-complete, to NP-complete, then to $PSPACE$-complete, with a number of cases where the status of the problem is NP-hard, but otherwise unresolved.

Beaudry *et al.* (1989) also introduced the use of the classification of monoids into *varieties*, imported from the theory of abstract monoids, as a natural and consistent way of defining restrictions to the membership problem; they pointed out that all the cases mentioned above are actually defined in this manner. Furthermore, they showed that restrictions defined in terms of varieties are robust: natural manipulations such as solving two instances simultaneously, or working on a submonoid of the original instance, amount to working on a monoid which belongs to the same variety as the original ones. Varieties can be defined in many different ways; one of them consists in fixing one or both of two parameters called the *threshold* and the *period*. The threshold and period of a monoid are t and q, respectively, iff these values are the smallest integers $t \geqslant 0$ and $q \geqslant 1$ such that every element f of the monoid satisfies $f^{t+q} = f^t$. For example, the variety of all threshold zero monoids is the variety of all groups. Also, a monoid is group-free if, and only if, it has period 1.

If we denote by (X, A, f) an instance of the membership problem, we say that such an instance belongs to the restriction of the problem to variety $\mathbf{V}$, denoted by MEMB($\mathbf{V}$), if it is known in advance that the monoid generated by A belongs to $\mathbf{V}$. Study of the aperiodic cases showed that, as soon as $\mathbf{V}$ contains a monoid of threshold two or more, MEMB($\mathbf{V}$) is NP-hard. This leaves the monoids of threshold zero or one as the only case where the membership problem can possibly be in P, and sets the program for the research reported on in this article: to look at the threshold one monoids, and see how "combining" groups with aperiodic threshold one (*idempotent*) monoids influences the complexity of the membership problem.

Our results show that, whenever a monoid is a "simple" combination of groups and idempotents, an instance of the membership problem in this monoid can be split, with little computational effort, into an instance in a permutation group and an instance in an idempotent monoid; the overall complexity is determined by the harder of the two subproblems. We also prove that any more intricate "combination" leads to NP-hardness. Putting these results together, and assuming that $NC \neq P$ and $P \neq NP$, we come up with a complete description of the "borderline" between AC^0, NC, P, and NP. It takes the form of a striking pattern: all varieties in which the membership problem is in AC^0 are contained in a variety called $\mathbf{J}_1$, i.e., a unique "maximal" variety for this complexity class, and similarly for the restrictions feasible in NC and in P. Hence, we identify *the largest varieties*

of monoids where membership can be tested in AC^0, in NC, and in P, respectively. Our main results read therefore as follows; varieties mentioned in this statement are defined in Section 3.

MAIN THEOREM. *Let* $\mathbf{V}$ *be a variety of monoids.*

If $\mathbf{V} \subseteq \mathbf{J}_1$, *then* MEMB($\mathbf{V}$) $\in AC^0$;
else if $\mathbf{V} \subseteq \mathbf{J}_1 \vee \mathbf{G}$, *then* MEMB($\mathbf{V}$) $\in NC$;
else if $\mathbf{V} \subseteq \mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$, *then* MEMB($\mathbf{V}$) *is P-complete*;
else $\mathbf{V} \not\subseteq \mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$, *and* MEMB($\mathbf{V}$) *is NP-hard.*

We also study restrictions of the membership problem to varieties beyond $\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$, namely $\mathbf{A}_1 \vee \mathbf{G}$, $\mathbf{GR}_1$, and $\mathbf{GL}_1$. We show that the problem in these cases is *NP*-complete (Theorems 4.7 and 4.10); these results suggest that the membership problem may be *NP*-complete in the case of arbitrary threshold one monoids.

Since it assumes to be known in advance that the monoid generated by A belongs to variety $\mathbf{V}$, our definition of MEMB($\mathbf{V}$) effectively separates membership testing from the *characterization problem*, which consists in deciding whether a transformation monoid specified by generators belongs to a given variety of monoids. This problem can be seen as a "data validation" step, where it is verified whether a particular algorithm for the membership problem is applicable to the instance at hand. The characterization of transformation monoids has a complexity varying from easy (e.g., testing whether a monoid is commutative, AC^0), up to very hard e.g., deciding whether a monoid contains a nontrivial group, *NP*-hard, see Stern, 1986). We address this problem in some specific varieties of threshold one monoids.

In Section 2, we describe the background and notations used throughout the article. Section 3 introduces the varieties discussed in this paper. The main theorem and related results are demonstrated in Section 4. Our discussion the characterization problem is the topic of Section 5. Finally, Section 6 comments on the results and mentions some open questions.

2. NOTATION AND BACKGROUND

In this article, we use notions from the theory of computational complexity and from the theory of monoids and finite automata. While the reader is assumed to be familiar with the former, we provide some background on the latter, taken from Lallement (1979) and Pin (1984).

We define an automaton as a pair (X, A), where X is a set of *states* and A a set of mappings from X to X (*generators*); both sets are finite. We

denote by $\langle A \rangle$ the transformation monoid of (X, A), i.e., the set of all mappings from X to X (*transformations*) which can be obtained by composition of elements of A; if the set of generators is given by extension (e.g., $A = \{a, b\}$), we then use the notation $\langle A \rangle = \langle a, b \rangle$. We denote the identity transformation by 1; whenever none of the nontrivial generators is a permutation, the identity cannot be obtained from them and must be an element of A, in order for $\langle A \rangle$ to be a monoid. We denote by xg the image of a state $x \in X$ by a transformation g and, if $E \subseteq X$, we define $Eg = \{xg : x \in E\}$. Furthermore, in some cases we use the representation of an automaton as a directed graph, with the states as nodes, and from each node an outgoing edge for every generator. Of particular interest to us is the notion of a strongly connected component, SCC for short (the usual definition in a directed graph; formally, we regard them as subsets of X).

We associate to a transformation $f \in \langle A \rangle$ its *maximal alphabet*, the set of all those generators which can appear is an expression for f; that is,

$$\mathscr{A}(f) = \{a \in A : f = uav \text{ for some } u, v \in \langle A \rangle\}.$$

Green's relations are relations of equivalence defined inside a monoid (here fM denotes the set $\{fx : x \in M\}$):

$$\begin{aligned} f \mathscr{J} g &\Leftrightarrow MfM = MgM; \\ f \mathscr{L} g &\Leftrightarrow Mf = Mg; \\ f \mathscr{R} g &\Leftrightarrow fM = gM; \\ f \mathscr{H} g &\Leftrightarrow f \mathscr{R} g \wedge f \mathscr{L} g. \end{aligned}$$

Varieties are defined as those classes of finite monoids which are closed under finite direct product, homomorphism, and taking of submonoids. Monoids in a variety all satisfy some set of properties, which in many cases can be expressed as equations (*defining identities*). Varieties form a lattice under proper set inclusion.

We work in this article on the variety $\mathbf{DS}_1$ of all finite *threshold one monoids*, those in which, for every element f, there exists a $p > 0$ such that $f^{p+1} = f$. With $M \in \mathbf{DS}_1$, there is an integer $p > 0$ such that $f^{p+1} = f$ for all $f \in M$; we then speak of M as being a "threshold one monoid of period p." Note that, in our terminology, p does not have to be minimal. The following properties are used throughout the article.

PROPOSITION 2.1 (Green and Rees, 1952). *For all elements f, g in a threshold one monoid of period p, the following hold*:

$$
\begin{aligned}
&(1) && (f^p)^2 = f^p;\\
&(2) && \mathscr{A}(g)\subseteq\mathscr{A}(f) \Rightarrow fgf\,\mathscr{H}\,f;\\
&(3) && \forall k>0,\quad f^k\,\mathscr{H}\,f;\\
&(4) && f\,\mathscr{H}\,g \Leftrightarrow f^p=g^p;\\
&(5) && f\,\mathscr{J}\,g \Leftrightarrow \mathscr{A}(f)=\mathscr{A}(g).
\end{aligned}
$$

Green and Rees also demonstrated that for every element f in a threshold one monoid, the equivalence class of f under $\mathscr{H}$ (H-class of f) is a group, so that the monoid actually is a disjoint union of groups. Observe also that a transformation f of X is of threshold one if, and only if, it is a permutation of Xf; that is, iff $Xf^2 = Xf$.

The *dual* of the transformation monoid of (X, A) is isomorphic to the transformation monoid of $(2^X, A^{-1})$, where 2^X is the power set of X, and where we define $A^{-1} = \{a^{-1} : a \in A\}$, with $Ea^{-1} = \{x \in X : xa \in E\}$ for every $E \subseteq X$. We have $f \in \langle A \rangle$ iff $f^{-1} \in \langle A^{-1} \rangle$. The notion of dual also exists for varieties; the defining identities for the dual of a variety are obtained by rewriting the original equations in reverse order.

A monoid M belongs to variety $\mathbf{V} \vee \mathbf{W}$ if there exist monoids $S \in \mathbf{V}$ and $T \in \mathbf{W}$, and a homomorphism ϕ, such that $\forall f \in M,\ \exists r \in S, \exists u \in T : f = \phi(r, u)$. This relation between M, S, and T is denoted by $M \prec S \times T$. Also, given a monoid G, the variety generated by G, denoted by $\langle G \rangle$, is the set of all monoids M such that $M \prec G \times G \times \cdots \times G$.

Computational complexities are evaluated in the classical models for sequential and parallel computation (Hopcroft and Ullman, 1979; Garey and Johnson, 1979; Cook, 1985). We use the chain of complexity classes

$$AC^0 \subset NC^1 \subseteq L \subseteq \cdots \subseteq NC \subseteq P \subseteq NP \subseteq PSPACE$$

as a reference. The article contains two reductions for hardness results, one deterministic log-time, and one deterministic log-space; the former type was defined by Buss (1987). We assume for the automata any reasonable encoding which allows basic operations, such as comparison or composition of two transformations of X, or computation of the image of a state $x \in X$, to be feasible in AC^0.

3. Varieties of Threshold One Monoids

In this section, we describe those varieties of threshold one monoids relevant to our study of the membership problem. We work within the variety $\mathbf{DS}_1$, which consists of all finite threshold one monoids. Included in $\mathbf{DS}_1$ are the variety $\mathbf{G}$ of all groups and the variety $\mathbf{A}_1$ of all aperiodic threshold one

monoids (*idempotent*; defining identity $f^2 = f$). We also consider varieties which do not fall in either of these classes. With very few exceptions, these varieties contain the whole of **G**. In order to define them, we start from varieties of idempotent monoids, and we "combine" them with the variety of all groups. To do so, we use the lattice of the varieties of idempotent monoids; its description, to be found in Wismath (1986), is a translation in terms of monoids of the works of Fennemore (1971) and Gerhard (1970) on the varieties of idempotent semigroups.

To a variety **V** of idempotent monoids, we "add" the whole variety **G** in order to build what we call an "extension" of **V**. "Adding" can take various meanings, depending on how intricately groups and idempotent monoids are combined together. For instance, the join $\mathbf{V} \vee \mathbf{G}$ can be regarded as the "minimal extension" of **V**, in the sense that this is the smallest variety containing both **V** and **G**. We also define what we call a "maximal extension" of **V**, denoted by **GV**, which is the largest variety of threshold one monoids in which all idempotent monoids belong to **V**. Formally: **GV** is a variety, and $\mathbf{GV} \subseteq \mathbf{DS}_1$, and $\mathbf{GV} \cap \mathbf{A}_1 \subseteq \mathbf{V}$, and $\forall \mathbf{W} \subseteq \mathbf{DS}_1$, $\mathbf{W} \cap \mathbf{A}_1 \subseteq \mathbf{V} \Rightarrow \mathbf{W} \subseteq \mathbf{GV}$. Proving that every variety **V** of idempotent monoids has a maximal extension lies outside the scope of this article. However, we show that in those cases useful to our purposes, such a maximal extension indeed exists (Proposition 3.2).

Minimal extensions have been studied by Petrich (1975), who showed in particular that the lattice of subvarieties of $\mathbf{A}_1 \vee \mathbf{G}$ is isomorphic to $\mathscr{L}(\mathbf{A}_1) \times \mathscr{L}(\mathbf{G})$, where $\mathscr{L}(\mathbf{A}_1)$ and $\mathscr{L}(\mathbf{G})$ are the lattices of subvarieties of $\mathbf{A}_1$ and of **G**, respectively. Petrich also proved the following.

PROPOSITION 3.1. *The following conditions on M, a threshold one monoid of period p, are equivalent*:

(1) $M \in \mathbf{A}_1 \vee \mathbf{G}$;

(2) $\forall f, g \in M$: $fg = fgf^p g^p = f^p g^p fg$;

(3) $\forall f, a_1, \ldots, a_r \in M$: $f = a_1 \cdots a_r \Leftrightarrow f^p = a_1^p \cdots a_r^p$.

The third condition implies that the set of the idempotent elements of M is itself a monoid, generated by $A^p = \{a^p : a \in A\}$. We denote this set by $\langle A^p \rangle$.

The varieties of threshold one monoids we shall concentrate on are derived from variety $\mathbf{R}_1$, defined by identities $f^2 = f$ and $fgf = fg$, from its dual $\mathbf{L}_1$, from their join $\mathbf{R}_1 \vee \mathbf{L}_1$, and from their intersection $\mathbf{J}_1$, which is the variety of the commutative idempotent monoids. These varieties played a central role in the study of the membership problem in aperiodic monoids. In this article, we are particularly interested in the minimal extensions $\mathbf{J}_1 \vee \mathbf{G}$, $\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$, and $\mathbf{A}_1 \vee \mathbf{G}$. We also introduce three varieties,

namely $\mathbf{GR}_1$, $\mathbf{GL}_1$, and $\mathbf{GJ}_1$, defined with identities which generalize those of $\mathbf{R}_1$, $\mathbf{L}_1$, and $\mathbf{J}_1$, respectively.

DEFINITION. If M is a threshold one monoid of period p, then it belongs to $\mathbf{GR}_1$ iff $\forall f, g \in M : fgf^p = fg$. It belongs to $\mathbf{GL}_1$ iff $\forall f, g \in M : f^p gf = gf$; it belongs to $\mathbf{GJ}_1$ *iff* $\forall f, g \in M : gf^p = f^p g$.

Variety $\mathbf{GJ}_1$ is actually the meet of varieties $\mathbf{GR}_1$ and $\mathbf{GL}_1$, since the conjunction of conditions $fgf^p = fg$ and $f^p gf = gf$ is equivalent to $gf^p = f^p g$. Our notation for these varieties suggests that they are maximal extensions; we show that this is indeed the case.

PROPOSITION 3.2. *Varieties* $\mathbf{GR}_1$, $\mathbf{GL}_1$, *and* $\mathbf{GJ}_1$ *are the maximal extensions of* $\mathbf{R}_1$, $\mathbf{L}_1$, *and* $\mathbf{J}_1$, *respectively.*

Proof. We prove the statement for $\mathbf{GR}_1$; the argument for the other two varieties is similar. The first three conditions for $\mathbf{GR}_1$ to be a maximal extension are immediate. We prove the fourth by contraposition. Let $M \notin \mathbf{GR}_1$ be a monoid of period p: there are elements f and g in M such that $fgf^p \neq fg$. We first show that f and g must also satisfy $(f^p g^p f^p)^p \neq (f^p g^p)^p$. To see this, we assume that $(f^p g^p f^p)^p = (f^p g^p)^p$ holds for all $f, g \in M$. Combining this with the observation that, for every $u, v \in M$,

$$u \mathrel{\mathscr{J}} v \Rightarrow u^p \mathrel{\mathscr{J}} v^p \Rightarrow \mathscr{A}(u^p) = \mathscr{A}(v^p) \Rightarrow u^p v^p u^p \mathrel{\mathscr{H}} u^p \Rightarrow (u^p v^p u^p)^p = u^p,$$

which comes from the definition of Green's relations and Proposition 2.1, we obtain $u \mathrel{\mathscr{J}} v \Rightarrow (u^p v^p)^p = u^p$. For arbitrary elements $x, y \in M$, let then $u = xyx^p$ and $v = xy$, and consider the expression xyx^p. Since $xyx^p \mathrel{\mathscr{J}} xy$, and $(xyx^p)^p = (xy)^p x^p$, we obtain

$$\begin{aligned} xyx^p = xyx^p(xyx^p)^p &= xyx^p((xyx^p)^p(xy)^p)^p \\ &= xyx^p((xy)^p x^p(xy)^p)^p \\ &= xy((xy)^p(xy)^p)^p \\ &= xy(xy)^p = xy, \end{aligned}$$

hence $M \in \mathbf{GR}_1$. We now claim that $(f^p g^p f^p)^p$ and $(f^p g^p)^p$, together with the identity, generate an idempotent monoid not belonging to $\mathbf{R}_1$. To make notations lighter, let $a = f^p$, $b = g^p$, $u = (f^p g^p f^p)^p$, and $v = (f^p g^p)^p$; all four elements are idempotent. We prove that $uv = v$ and $vu = u$, which leads to $\langle 1, u, v \rangle = \{1, u, v\}$. Indeed,

$$\begin{aligned} vu = (ab)^p(aba)^p &= (ab)^p aba(aba)^{p-1} \\ &= (ab)^{p+1} a(aba)^{p-1} \\ &= (ab)\, a(aba)^{p-1} = (aba)^p = u, \end{aligned}$$

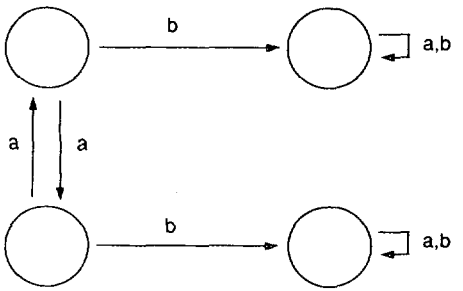

FIG. 1. An automaton with transformation monoid $GR_{1(2)}$.

and

$$uv = (aba)^p(ab)^p = (aba)^{p-1}abaab(ab)^{p-1}$$
$$= (aba)^{p-1}(ab)^{p+1} = \cdots = (ab)^{2p} = (ab)^p = v.$$

And, since $u = uvu \neq uv = v$, we have $\langle 1, u, v\rangle \notin \mathbf{R}_1$. ∎

Further, $\mathbf{GJ}_1 = \mathbf{J}_1 \vee \mathbf{G}$. Indeed, defining identity $gf^p = f^p g$ can be used to show that $f^p g^p fg = f^p fg^p g = fg = ff^p gg^p = fgf^p g^p$, which is

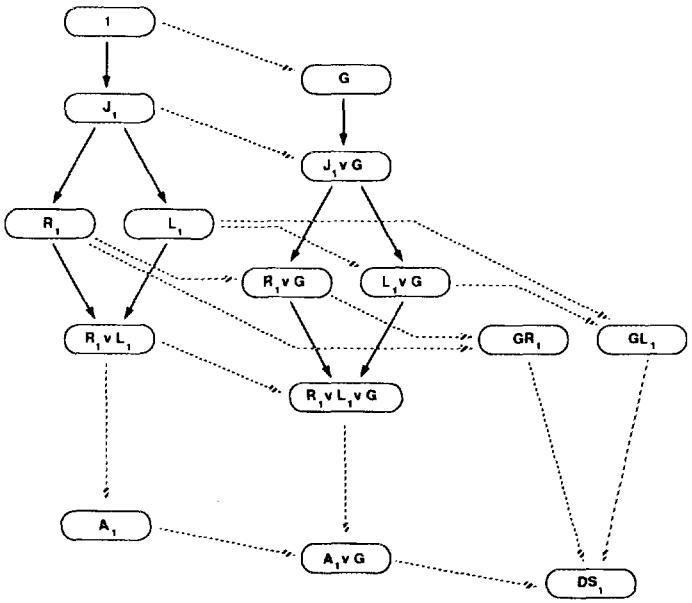

FIG. 2. Varieties of threshold one monoids. A solid line joining two varieties indicates the absence of intermediate varieties.

condition (2) of Proposition 3.1. The minimal and maximal extensions of $\mathbf{R}_1$, however, do not coincide.

PROPOSITION 3.3. $\mathbf{R}_1 \vee \mathbf{G} \subset \mathbf{GR}_1$.

Proof. Consider the transformation monoid $\langle a, b \rangle$ of the automaton depicted in Fig. 1. Denoted $GR_{1(2)}$, this is a threshold one monoid of period 2, such that $ab \neq a^2b^2ab = bab = b$. Using Propositions 5.1 or 5.2, it can be verified that this monoid belongs to $\mathbf{GR}_1$. ∎

A dual statement holds for variety $\mathbf{GL}_1$. The lattice of the varieties of threshold one monoids is sketched on Fig. 2.

4. MEMBERSHIP TESTING

We now study the computational complexity of the membership problem in the varieties of threshold one monoids defined in the previous section. We prove the main theorem, obtaining our statement on the variety $\mathbf{A}_1 \vee \mathbf{G}$ as a collateral result (Theorem 4.7). We complete the section with an investigation of the varieties $\mathbf{GR}_1$ and $\mathbf{GL}_1$ (Theorem 4.10). Our proofs build on established knowledge on the membership problem in permutation groups and in aperiodic transformation monoids. For the convenience of the reader, we state those results by Babai *et al.* (1987) (statement 1) and by Beaudry *et al.* (1989) (statements 2 to 5), as follows.

PROPOSITION 4.1. *Let* $\mathbf{V}$ *be a variety of monoids.*

(1) *If* $\mathbf{V} \subseteq \mathbf{G}$, *then* MEMB($\mathbf{V}$) *is feasible in NC*;

(2) MEMB($\mathbf{J}_1$) *is feasible in* AC^0;

(3) *if* $\mathbf{J}_1 \subset \mathbf{V} \subseteq \mathbf{R}_1 \vee \mathbf{L}_1$, *then* MEMB($\mathbf{V}$) *is P-complete*;

(4) *if* $\mathbf{R}_1 \vee \mathbf{L}_1 \subset \mathbf{V} \subseteq \mathbf{A}_1$, *then* MEMB($\mathbf{V}$) *is NP-complete*;

(5) *if* $\mathbf{V}$ *contains a monoid of threshold two or more, then* MEMB($\mathbf{V}$) *is NP-hard.*

We proceed with the main theorem, which we state anew, as a set of six assertions.

THEOREM 4.2. *Let* MEMB($\mathbf{V}$) *denote the restriction of the membership problem to transformation monoids belonging to the variety* $\mathbf{V}$.

(i) MEMB($\mathbf{J}_1$) *is feasible in* AC^0;

(ii) MEMB($\mathbf{V}$) *lies outside of* AC^0 *for every variety* $\mathbf{V} \not\subseteq \mathbf{J}_1$;

(iii) MEMB($\mathbf{J}_1 \vee \mathbf{G}$) *is feasible in NC*;

(iv) MEMB($\mathbf{V}$) *is P-hard for every variety* $\mathbf{V} \not\subseteq \mathbf{J}_1 \vee \mathbf{G}$;

(v) MEMB($\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$) *is feasible in P*;

(vi) MEMB($\mathbf{V}$) *is NP-hard for every variety* $\mathbf{V} \not\subseteq \mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$.

Proof. Assertion (i) repeats statement (2) of Proposition 4.1. Assertion (iv) is proved by observing that every monoid outside of variety $\mathbf{J}_1 \vee \mathbf{G}$ is either of threshold 2 or more, and then 4.1(5) applies, or it belongs to a variety of threshold one monoids which strictly contains $\mathbf{J}_1 \vee \mathbf{G}$; by Proposition 3.2, this variety contains at least one of $\mathbf{R}_1$ and $\mathbf{L}_1$, where membership testing is *P*-hard (statement (3) of Proposition 4.1). To show assertion (ii), we adapt this argument to $\mathbf{J}_1$: a monoid outside of $\mathbf{J}_1$ either falls into one of the above cases, or it contains a nontrivial group, in which case membership testing is shown not to be feasible in AC^0 (this is Proposition 4.3). An analogous study of cases is used to demonstrate assertion (vi): if a variety of monoids is not included in $\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$, then we distinguish between three cases, depending on whether it is not a variety of threshold one monoids, or it is included in $\mathbf{DS}_1$ but not in $\mathbf{A}_1 \vee \mathbf{G}$, or it is included in $\mathbf{A}_1 \vee \mathbf{G}$ but not in $\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$. The first and third cases mean *NP*-hardness by statement (5) of Proposition 4.1 and by Theorem 4.7, respectively. To deal with the second case, we show that from every threshold one monoid M outside of $\mathbf{A}_1 \vee \mathbf{G}$ we can obtain a simpler monoid (Lemma 4.8) which generates a variety where membership testing is *NP*-hard (Lemma 4.9). This implies that MEMB($\langle M \rangle$) is itself *NP*-hard, a result which extends to all threshold one varieties not included in $\mathbf{A}_1 \vee \mathbf{G}$. Finally, assertions (iii) and (v) are proved by presenting algorithms which fall into the appropriate complexity classes (Lemmas 4.4 and 4.6). ∎

PROPOSITION 4.3. *If* $\mathbf{V} \subseteq \mathbf{G}$ *is a non-trivial variety of groups, then* MEMB($\mathbf{V}$) *is not feasible in* AC^0.

Proof. This statement is obtained by a reduction from problem MOD_p, which consists in deciding whether an input of n bits adds up to a multiple of p, $p \geqslant 2$; this has been shown not to be feasible in AC^0 (Ajtai, 1983; Furst *et al.*, 1984; Smolensky, 1987). Let $b_1, ..., b_n$ be the input bits. We build an automaton (X, A), where $A = \{a_1, ..., a_n\}$, and where X is a set of $p(n+1)$ states, partitioned into $n+1$ connected components C_j, $0 \leqslant j \leqslant n$, with p states each, denoted x_{jk}, $0 \leqslant k \leqslant p-1$. Whenever $j \geqslant 1$ and $j \neq i$, generator a_i acts on component C_j as the identity. In component C_i, we have $x_{ik}a_i = x_{i(k+1)}$ for each $0 \leqslant k < p$; the sum is taken modulo p. In component C_0, generator a_i acts as the identity if $b_i = 0$, otherwise it maps state x_{0k} to $x_{0(k+1)}$, $0 \leqslant k < p$. The test-transformation acts as the identity on component C_0 and maps x_{jk} to $x_{j(k+1)}$, for all $1 \leqslant j \leqslant n$ and $0 \leqslant k < p$. Each component C_j, $j \geqslant 1$, is used to ensure that the corresponding input bit is

read once. The actual count modulo p takes place in component C_0. With an appropriate encoding for the instance of group membership, the reduction can be made *DLOGTIME* uniform. For example, if the encoding is a sequence of tuples (i, j, k, l, m), specifying that generator a_i maps x_{jk} to x_{lm}, a log-time deterministic Turing machine first tests whether $j = l$. If this holds, then it tests whether $j = 0$; if so, it then reads the i th input bit, and, depending on its value, verifies whether $m = k$, if $b_i = 0$, or $m = k + 1 \pmod p$, if $b_i = 1$. Similar tests are done when $j \neq 0$; they do not involve any access to the inputs. ▮

LEMMA 4.4. *Membership testing in* $\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$ *can be done in polynomial time.*

Proof. From an instance of MEMB($\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$), we build an instance of MEMB($\mathbf{R}_1 \vee \mathbf{L}_1$) and an instance of MEMB($\mathbf{G}$). The former involves automaton (X, A^p), where by Proposition 3.1, $\langle A^p \rangle = \{f^p : f \in \langle A \rangle\}$ is an idempotent monoid generated by $A^p = \{a^p : a \in A\}$, and $f \in \langle A \rangle \Rightarrow f^p \in \langle A^p \rangle$. The membership test in (X, A^p) begins with the computation of the set

$$\mathscr{A}(f^p) = \{a^p \in A^p : f^p = ua^p v \text{ for some } u, v \in \langle A^p \rangle\},$$

from which we define $\mathscr{B}(f) = \{a \in A : a^p \in \mathscr{A}(f^p)\}$. We compute instead $\mathscr{A}(f)$, using for this the equivalence $a \in \mathscr{A}(f) \Leftrightarrow Xaf = Xf$. Proved for the idempotent monoids in Beaudry *et al.* (1989), this fact is demonstrated in the non-aperiodic case as follows. From Pin (1984, Chap. 3), we use the equivalence $Xuv = Xv \Leftrightarrow uv \mathscr{L} v$ to deduce that

$$Xaf = Xf \Rightarrow af \mathscr{J} f \Rightarrow \mathscr{A}(af) = \mathscr{A}(f) \Rightarrow a \in \mathscr{A}(f).$$

Conversely, $Xaf \subseteq Xf$ is obvious, and

$$a \in \mathscr{A}(f) \Rightarrow faf \mathscr{H} f \Rightarrow Xfaf = Xf \Rightarrow Xaf \supseteq Xf.$$

Therefore,

$$a \in \mathscr{B}(f) \Leftrightarrow a^p \in \mathscr{A}(f^p) \Leftrightarrow Xa^p f^p = Xf^p \Leftrightarrow Xaf = Xf \Leftrightarrow a \in \mathscr{A}(f).$$

The test in $\langle A^p \rangle$ verifies whether the action of f on X is compatible with membership of f in one of the H-classes of $\langle A \rangle$. We must complete this with a second test, aimed at deciding whether f coincides with an element of this H-class, which is a group; this amounts therefore to solving an instance of MEMB($\mathbf{G}$). However, we must first compute generators for the group of the H-class of f. The following property of $\mathbf{A}_1 \vee \mathbf{G}$ gives us an efficient method to do so.

PROPOSITION 4.5. *Let transformation f belong to $\langle A\rangle \in \mathbf{A}_1 \vee \mathbf{G}$, a monoid of period p. The H-class of f is a group generated by the set $\mathscr{C}(f) = \{f^p a f^p : a \in \mathscr{A}(f)\}$.*

Proof. First, $a \in \mathscr{A}(f) \Rightarrow f^p a f^p \mathscr{H} f$, by statement (2) of Proposition 2.1; further, since $u \mathscr{H} f \wedge v \mathscr{H} f \Leftrightarrow u^p = v^p = f^p$, Proposition 3.1 leads to $(uv)^p = u^p v^p = f^p f^p = f^p$, and therefore to $uv \mathscr{H} f$. This means that $\langle \mathscr{C}(f)\rangle$ is a subset of the H-class of f. Conversely, consider an arbitrary element g of this H-class. We have $\mathscr{A}(f) = \mathscr{A}(g)$ and $g^p = f^p$, by Proposition 2.1(4). We can thus write $g = a_1 \cdots a_r$, where $a_i \in \mathscr{A}(f)$, $1 \leqslant i \leqslant r$, and

$$g = g^p g g^p = g^p a_1 \cdots a_r g^p = f^p a_1 \cdots a_r f^p.$$

Assume that, in a monoid M of period p belonging to $\mathbf{A}_1 \vee \mathbf{G}$, we have $xyzx = xyx^p zx$, for all $x, y, z \in M$ such that $\mathscr{A}(xy) = \mathscr{A}(zx)$. Setting $xy = f^p a_1 \cdots a_i$ and $zx = a_{i+1} \cdots a_r f^p$, and observing that

$$f = f^{2p+1} = f^p a_1 \cdots a_i \cdot a_{i+1} \cdots a_r f^p$$

$$\Rightarrow \mathscr{A}(f) = \mathscr{A}(f^p a_1 \cdots a_i) = \mathscr{A}(a_{i+1} \cdots a_r f^p),$$

we can use the assumption to insert in the expression of g a factor $f^p f^p$ between a_i and a_{i+1}, for every $1 \leqslant i < r$, in order to obtain $g = f^p a_1 f^p \cdots f^p a_r f^p$, and therefore $g \in \langle \mathscr{C}(f)\rangle$. We now proceed with the proof of the assumption.

Having $M \in \mathbf{A}_1 \vee \mathbf{G}$ implies $M \subseteq \phi(S \times T)$, with $S \in \mathbf{A}_1$ and $T \in \mathbf{G}$, a group such that $u^p = 1$, $\forall u \in T$, and ϕ a monoid homomorphism. Then

$$xyzx = \phi(r, u)\,\phi(s, v)\,\phi(t, w)\,\phi(r, u) = \phi(rstr, uvwu) = \phi(rsrtr, uvwu),$$

where the last step uses a property of the idempotent monoids, namely that $\mathscr{A}(c) \subseteq \mathscr{A}(d) = \mathscr{A}(e) \Rightarrow dce = de$ (Green and Rees, 1952). Next,

$$\begin{aligned}\phi(rsrtr, uvwu) &= \phi(rsr^p tu, uvu^p wu)\\ &= \phi(r, u)\,\phi(s, v)(\phi(r, u))^p \phi(t, w)\,\phi(r, u) = xyx^p zx,\end{aligned}$$

where we use idempotency of r and the fact that $u^p = 1$. ∎

Proof of Lemma 4.4 (Continued). From the original instance (X, A, f), we built a test for f^p in the transformation monoid of (X, A^p) and a test for f in the permutation group of the automaton $(Xf, \mathscr{C}(f))$. A positive answer to both tests is necessary in order to have $f \in \langle A\rangle$. This also suffices: consider $g^p h g^p$, where $g^p \in \langle A^p\rangle$ is such that $\forall x \in X$, $xg^p = xf^p$, and where $h \in \langle \mathscr{C}(f)\rangle$ satisfies $\forall x \in Xf$, $xh = xf$. For every state $x \in Xf$, we

have $xg^p = xf^p = x \Rightarrow xg^phg^p = xh = xf$. Meanwhile, $(g^phg^p)^p = g^ph^pg^p = f^ph^pf^p = f^p$ implies that for every $x \notin Xf$,

$$xg^phg^p = x(g^phg^p)^pg^phg^p(g^phg^p)^p = xf^phf^p = xf^ph = xf.$$

This proves the correctness of the following algorithm.

input: automaton (X, A), test-transformation f; with $|X| = m$, let $p = m!$
step 1: Verify that $Xf^2 = Xf$;
compute the set $\mathscr{A}(f) = \{a \in A : Xaf = Xf\}$;
step 2: build the automaton (X, A^p) and test for membership of f^p in $\langle A^p \rangle$;
step 3: build the automaton $(Xf, \mathscr{G}(f))$;
test for membership of f (restricted to Xf) in its permutation group;
step 4: $f \in \langle A \rangle$ iff steps 2 and 3 are both successful.

Note that parameter p need not be computed explicitly, as we shall see below; further, the period of the monoid can always be taken as $m!$. We proceed with the analysis of the algorithm. Steps 1 and 4 are feasible in AC^0. Step 2 contains a membership test in a monoid of $\mathbf{R}_1 \vee \mathbf{L}_1$, and before this the construction of f^p and of the a^p, $a \in A$. The construction can be done in AC^0, as follows. For each $x \in X$, verify first whether it belongs to Xf; if so, then $xf^p = x$. Else, since $xf^{p+1} = xf$, the image of x by f^p is the unique state $y \in Xf$ such that $yf = xf$. Notice that in the case of f, this method is valid only if we know in advance that f is a transformation of threshold one, hence the test at the beginning of step 1. Step 3 consists in first computing $\mathscr{G}(f)$ in AC^0, then performing a membership test in the permutation group $\langle \mathscr{G}(f) \rangle$. Observe that, from the complexity viewpoint, everything in this algorithm is doable in AC^0, except the two membership tests. In variety $\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$, both tests are feasible in polynomial time, by statements (1) and (3) of Proposition 4.1. ▮

The above proof of correctness works for every subvariety of $\mathbf{A}_1 \vee \mathbf{G}$. The algorithm can therefore be adapted to other minimal extensions. For instance, if we substitute in step 2 an algorithm which solves MEMB($\mathbf{J}_1$) in AC^0 (see statement (2) of Proposition 4.1), we obtain a test for membership in $\mathbf{GJ}_1 = \mathbf{J}_1 \vee \mathbf{G}$, whose complexity is dominated by the instance of group membership, at step 3.

LEMMA 4.6. *Membership testing in* $\mathbf{GJ}_1$ *can be done in NC.*

For the case of arbitrary monoids belonging to variety $\mathbf{A}_1 \vee \mathbf{G}$, it suffices to substitute in step 2 an algorithm which solves MEMB($\mathbf{A}_1$) in nondeterministic polynomial time.

THEOREM 4.7. *If* $\mathbf{V}$ *is a variety of threshold one monoids such that* $\mathbf{V} \not\subseteq \mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$ *and* $\mathbf{V} \subseteq \mathbf{A}_1 \vee \mathbf{G}$, *then* MEMB($\mathbf{V}$) *is NP-complete.*

Proof. The argument for *NP*-easiness is given above. *NP*-hardness is a consequence of the structure of the lattice of subvarieties of $\mathbf{A}_1 \vee \mathbf{G}$: any $\mathbf{V}$ such that $\mathbf{V} \not\subseteq \mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$ and $\mathbf{V} \subseteq \mathbf{A}_1 \vee \mathbf{G}$ must contain a variety of idempotent monoids to which Proposition 4.1(4) applies. ∎

Also, the algorithm can be applied to monoids belonging to variety $\mathbf{J}_1 \vee \mathbf{H}$, where $\mathbf{H} \subseteq \mathbf{G}$ is a variety of groups. In this case, step 2 in the algorithm can now be done in AC^0, while step 3 cannot (see Proposition 4.3). An analysis of the computational complexity of MEMB($\mathbf{H}$) is then necessary in order to determine how the complexity of steps 2 and 3 combine to determine the overall complexity of MEMB($\mathbf{J}_1 \vee \mathbf{H}$).

We now prove the two lemmas used to demonstrate assertion (vi). We show that from every threshold one monoid M outside of $\mathbf{A}_1 \vee \mathbf{G}$, we can obtain a simpler monoid, which generates a variety where membership testing is *NP*-hard. This implies that MEMB($\langle M \rangle$) is itself *NP*-hard, and so is MEMB($\mathbf{V}$) for any variety of threshold one monoids containing such an M, i.e., any subvariety of $\mathbf{DS}_1$ not included in $\mathbf{A}_1 \vee \mathbf{G}$.

For every $p \geqslant 2$, define a monoid $GR_{1(p)} = \{a^i : 0 \leqslant i < p\} \cup \{a^i b : 0 \leqslant i < p\}$ with $2p$ elements, such that $a^i \neq a^{i-1}$, $a^i b \neq a^{i-1} b$ $\forall i$, $a^p = 1$, $b^2 = ba = b$, and $ab \neq ba$. This monoid lies in $\mathbf{GR}_1$, outside of $\mathbf{A}_1 \vee \mathbf{G}$, while its dual $GL_{1(p)}$ belongs to $\mathbf{GL}_1 - (\mathbf{A}_1 \vee \mathbf{G})$. An automaton with transformation monoid $GR_{1(2)}$ is shown in Fig. 1.

LEMMA 4.8. *Let* M *be a threshold one monoid of period* p. *If* $M \notin \mathbf{A}_1 \vee \mathbf{G}$, *then there exist a monoid* N *in variety* $\langle GR_{1(q)} \rangle$ *and a monoid* P *in* $\langle GL_{1(r)} \rangle$, *with* $q, r \geqslant 1$ *integers dividing* p, *such that* $N \prec M$ *and* $P \prec M$, *and at least one of* N *and* P *lies outside of* $\mathbf{A}_1 \vee \mathbf{G}$.

Proof. By Proposition 3.1, a monoid M not in $\mathbf{A}_1 \vee \mathbf{G}$ contains two elements c and d such that $cd \neq cdc^p d^p$ or $cd \neq c^p d^p cd$. Assume that the second inequality holds; the other case can be treated dually. It can be verified that the hypothesis is equivalent to having $cd^p \neq c^p d^p cd^p$, so that from now on we assume that d is idempotent.

We build a monoid N, isomorphic to $GR_{1(q)}$ for an integer $q \geqslant 2$, in two steps. For the first step, let $W = \{cx : x \in \langle 1, c, d \rangle\}$, and define operation $*$ as follows: $cx * cy = cxy$. With this operation, W is a monoid such that $W \prec M$. Furthermore, with notations $a = cc$ and $b = cd$, observe that b is idempotent under $*$, that the pth power of a acts as the identity c, and that a and b together generate the monoid. The hypothesis $cd \neq c^p dcd$ translates in W into $b \neq a^{p-1} * b * a * b$, which implies that $a * b \neq b * a * b$ (here, a^{p-1} denotes the $(p-1)$th power of a, taken relative to the operation $*$).

Using Proposition 2.1(5), we partition this monoid in two J-classes: one consists of the powers of a, the other gathers the rest of W. The latter class is divided into R-classes; each can be described as a subset of the form $\{a^i * b * x : x \in W\}$, $0 \leqslant i < p$. We claim that some of these R-classes are distinct. Otherwise, we would have $(a * b)\,\mathscr{R}\,(b * a * b)$. Since $(a * b)^{p+1} = a * b$ implies $(a * b)\,\mathscr{L}\,(b * a * b)$, we obtain $(a * b)^p = (b * a * b)^p$, by statement (4) of Proposition 2.1. Composing both sides to the right with $b * a * b$ then leads to $a * b = b * a * b$; this contradicts the hypothesis, so that the claim is proved. There are therefore $q \geqslant 2$ distinct R-classes. Note that q is a divisor of p; otherwise $b\,\mathscr{R}\,(a^i * b)$ for an i not dividing p. Using then the fact that $u\,\mathscr{R}\,wu \Rightarrow u\,\mathscr{R}\,wwu$, deduced from the definition of relation $\mathscr{R}$, we obtain $b\,\mathscr{R}\,(a^{ki} * b)$ for all k, in particular those for which $ki \equiv 1 \pmod{p}$, and this leads to $(a * b)\,\mathscr{R}\,(b * a * b)$.

We now map W onto the set $N = \{f^i : 0 \leqslant i < q\} \cup \{f^i \circ g : 0 \leqslant i < q\}$, as follows. For each $i < q$, the image of a^{i+jq}, $j \geqslant 0$, is f^i, while the whole R-class of element $a^i * b$ is mapped onto $f^i \circ g$. In this set, define operation $\circ$ such that $f \circ (f^i \circ g) = f^{i+1} \circ g$, where $i+1$ is taken modulo q, and $(f^i \circ g) \circ x = f^i \circ g$ for all $x \in N$. Every f^i is the i th power of f, taken relative to $\circ$. The set N with operation $\circ$ is a monoid; it is a homomorphic image of W, and is isomorphic to $GR_{1(q)}$. ∎

LEMMA 4.9. *Problems* MEMB($\langle GR_{1(p)} \rangle$) *and* MEMB($\langle GL_{1(p)} \rangle$) *are NP-hard for all* $p \geqslant 2$.

Proof. We first prove *NP*-hardness for MEMB($\langle GR_{1(2)} \rangle$), by reduction from the following variant of problem 3SAT (Garey and Johnson, 1979).

Given a set of Boolean variables $U = \{u_1, ..., u_n\}$ and a set of clauses $K = \{c_1, ..., c_m\}$, each of the form $c_j = (u_{j1}, u_{j2}, u_{j3})$, where none of the variables is negated, decide whether there exists an assignment of truth values to the variables such that, for each clause c_j, exactly one of u_{j1}, u_{j2}, and u_{j3} has value *true*.

From an instance (U, C) of 3SAT, we build an instance (X, A, f) of MEMB($\langle GR_{1(2)} \rangle$), as follows. We define $A = \{a_1, ..., a_n\} \cup \{b, d, 1\}$, where each generator a_i is associated to variable u_i. The set X is partitioned into connected components C_j, $1 \leqslant j \leqslant m$, each consisting of a strongly connected component K_j with eight states labelled $(FFF)_j$ to $(TTT)_j$, of a second SCC K_j' with eight states labelled $(000)_j$ to $(111)_j$, and of states x_j and y_j. The generators act on connected component C_j as follows.

(1) Every a_i such that $u_i \notin \{u_{j1}, u_{j2}, u_{j3}\}$ acts on C_j as the identity.

(2) Generator a_{j1} permutes state $(FPQ)_j$ with $(TPQ)_j$, and $(0\alpha\beta)_j$ with $(1\alpha\beta)_j$, for every combination of $P, Q \in \{F, T\}$ and $\alpha, \beta \in \{0, 1\}$.

It maps each of states x_j and y_j to itself. The action of generators a_{j2} and a_{j3} is defined similarly.

(3) Generator b maps $(TFF)_j$ to $(100)_j$, $(FTF)_j$ to $(010)_j$ and $(FFT)_j$ to $(001)_j$, and every other state of K_j to x_j. Meanwhile, it acts as the identity on the states of K_j', on x_j, and on y_j.

(4) Generator d maps all the states of C_j onto x_j, with the exception of $(000)_j$ and y_j, which are mapped to y_j.

Connected component C_j is represented in Fig. 3, where the index j, arrows to x_j, and self-loops have been omitted in order to improve legibility. In C_j, test-transformation f maps the three states y_j, $(FFF)_j$, and $(000)_j$, onto y_j, and the other 15 states onto x_j. It is straightforward to verify that the instance (X, A, f) can be built from (U, C) in logarithmic space.

We claim that f encodes a solution to 3SAT if it can be written as $f = vbw$, where v is an expression containing neither b nor d, where w contains at least one d, and where the occurrences of a_i in v are counted in order to provide the truth value assigned to variable u_i, with an odd number of a_i meaning $u_i := true$, and an even number $u_i := false$.

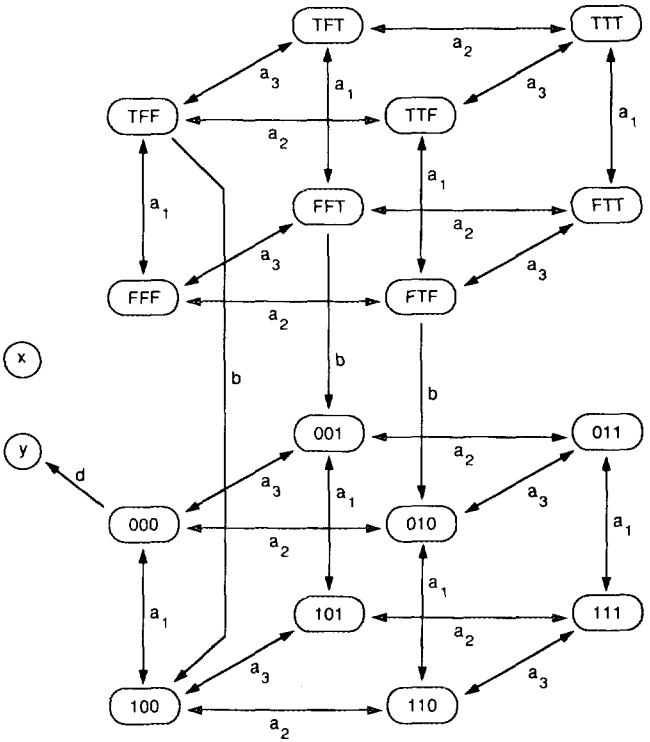

FIG. 3. Connected component of (X, A) reducing 3SAT to MEMB($\mathbf{GR}_1$).

Indeed, let a solution to an instance of 3SAT assign the value true to variables $u_1, ..., u_k$. Consider the transformation $g = a_1 \cdots a_k b a_1 \cdots a_k d$. For every clause c_j, exactly one of a_{j1}, a_{j2}, and a_{j3} appears in g, so that g acts on component C_j the same way as f does; therefore, $f \in \langle A \rangle$. Conversely, if $f \in \langle A \rangle$, then it can be expressed as $f = gbhdk$, with $g \in \langle a_1, ..., a_n \rangle$ and $h \in \langle a_1, ..., a_n, b \rangle$. To see this, observe that the presence of at least one d in f, and of at least one b to the left of the d, are necessary in order to have $(FFF)_j f = y_j$. Furthermore, in order to bring $(FFF)_j$ to y_j, we must first have $(FFF)_j gb \in K'_j$, which imposes $(FFF)_j g \in \{(TFF)_j, (FTF)_j, (FFT)_j\}$; this implies that exactly one of a_{j1}, a_{j2}, or a_{j3} occurs in g an odd number of times. In our interpretation, this means that clause c_j is satisfied. (The presence of SCC K'_j is necessary in order to uniquely define the image by f of every state of K_j, something which we could not obtain with a smaller construction.)

We also have to show that this actually is an instance of MEMB($\langle GR_{1(2)} \rangle$), by proving that the monoid we work on belongs indeed to the variety generated by $GR_{1(2)}$. Since this is a technical exercise on a very specific monoid, we defer it to the Appendix.

For $p \geqslant 3$, we adapt this reduction to the variety $\langle GR_{1(p)} \rangle$ as follows. In each connected component C_j, we expand SCCs K_j and K'_j from 8 up to p^3 states, and we redefine the generators in such a way that a solution to 3SAT is encoded as $f = vbw$ as before, where the number of occurrences in v of generator a_i is either congruent to 1 modulo p, if $u_i := true$, or to 0, if $u_i := false$.

The automaton built for this reduction has connected components of constant size. Thanks to this, membership testing in this automaton can be reduced to a polynomial-size instance of MEMB($\langle GL_{1(p)} \rangle$), using a method described in Beaudry *et al.* (1989). ▮

To conclude this section, we show that MEMB($\mathbf{GR}_1$) and MEMB($\mathbf{GL}_1$) are *NP*-complete. Since by Proposition 3.2, these varieties are the maximal extensions of $\mathbf{R}_1$ and $\mathbf{L}_1$, respectively, this means that "combining" groups with monoids from either $\mathbf{R}_1$ or $\mathbf{L}_1$, no matter how intricately, does not take the computational complexity of the membership problem outside of *NP*.

THEOREM 4.10. *Problems* MEMB($\mathbf{GR}_1$) *and* MEMB($\mathbf{GL}_1$) *are NP-complete.*

Since *NP*-hardness was proved above, we only have to exhibit for each variety an algorithm which tests membership in nondeterministic polynomial time.

LEMMA 4.11. *Membership testing in* $\mathbf{GR}_1$ *can be done in NP.*

Proof. We build an algorithm for membership testing, which works in four steps. It is based on Proposition 5.1, which shows that the set of those transformations of $\langle A \rangle$ which permute Xf is generated by a subset of A (that is, its restriction to Xf). The first step consists in computing $\mathscr{A}(f)$. Steps 2 and 3 use a decomposition of f as $f = b_1 h_1 b_2 h_2 \cdots b_k h_k$, with $b_i \in \mathscr{A}(f)$, $1 \leqslant i \leqslant k$, and where each h_i belongs to $\langle b_1, ..., b_i \rangle$. Since the action of h_i reduces to permuting the states of $Xb_1 h_1 \cdots b_{i-1} h_{i-1} b_i = Xb_1 \cdots b_i$, we can guess this action, and then use a test for membership in the permutation group of automaton $(Xb_1 \cdots b_i, \{b_1, ..., b_i\})$. The algorithm thus reads as follows.

input: automaton (X, A), test-transformation f;
step 1: compute the set $\mathscr{A}(f) = \{a \in A : Xaf = Xf\}$;
step 2: guess an ordering $b_1, ..., b_k$ for the elements of $\mathscr{A}(f)$;
step 3: for $i := 1$ to k do
guess a permutation h_i of the set $Xb_1 \cdots b_i$;
test whether h_i belongs to the permutation group of $(Xb_1 \cdots b_i, \{b_1, ..., b_i\})$; if not, halt;
step 4: if $f = b_1 h_1 \cdots b_k h_k$, then $f \in \langle A \rangle$. ∎

LEMMA 4.12. *Membership testing in* $\mathbf{GL}_1$ *can be done in NP.*

Proof. Proposition 5.1, on which the above algorithm is based, does not have an equivalent in $\mathbf{GL}_1$. Therefore, instead of testing for membership of f in (X, A), we work in the reverse automaton $(2^X, A^{-1})$, where $\langle A^{-1} \rangle \in \mathbf{GR}_1$, and we decide whether there exists a transformation $g^{-1} \in \langle A^{-1} \rangle$ such that $\{y\} g^{-1} = \{y\} f^{-1}$ for every state $y \in Xf$. We guess a decomposition of g into $g = h_k b_k \cdots h_1 b_1$, that is, actually $g^{-1} = b_1^{-1} h_1^{-1} \cdots b_k^{-1} h_k^{-1}$, and we apply on g^{-1} a sequence of tests similar to those done on an instance of MEMB($\mathbf{GR}_1$). In order to test membership is nondeterministic polynomial time, we restrict the size of the automaton we work on: we show that each h_i^{-1} needs to be defined only on a polynomial-sized subset of 2^X.

Let $g_i = b_i h_{i-1} b_{i-1} \cdots h_1 b_1$ be a transformaion of (X, A). From Pin (1984, Chap. 3) and Proposition 2.1(5), defining identity $h_i g_i = g_i^p h_i g_i$ together with $\mathscr{A}(g_i) = \mathscr{A}(h_i g_i)$ implies that $h_i g_i \mathscr{R} g_i$, which in turn implies that $xg_i = yg_i \Leftrightarrow xh_i g_i = yh_i g_i$, for all $x, y \in X$. Therefore, for any $z \in Xg_i$, there exists a state $y \in Xg_i$, such that

$$\{z\} g_i^{-1} h_i^{-1} = \{x \in X : xh_i g_i = z\} = \{y\} g_i^{-1} h_i^{-1};$$

in other words, h_i^{-1} permutes the $\{x\} g_i^{-1}$, $x \in Xg_i$, between themselves.

Starting with $Y_0 = \{\{y\} : y \in Xf\}$, we can iteratively define each set $Y_i \subseteq 2^X$, $1 \leqslant i \leqslant k$, as being $Y_i = Y_0 g_i^{-1}$, or equivalently $Y_i = Y_{i-1} b_i^{-1}$, with the properties that $Y_i h_i^{-1} = Y_i$, *and* that $|Y_i| \leqslant |Y_0| \leqslant |X|$. The algorithm reads therefore as follows.

input: automaton (X, A), test-transformation f;
step 1: compute the set $\mathscr{A}(f) = \{a \in A : Xaf = Xf\}$;
step 2: guess an ordering $b_1, ..., b_k$ for the elements of $\mathscr{A}(f)$;
step 3: let $Y_0 = \{\{y\} : y \in Xf\}$;
step 4: for $i := 1$ to k do
compute the set $Y_i = \{Eb_i^{-1} : E \in Y_{i-1}\}$;
guess a permutation h_i^{-1} of Y_i;
test whether h_i^{-1} belongs to the permutation group of $(Y_i, \{b_1^{-1}, ..., b_i^{-1}\})$;
if not, halt;
step 5: for each state $y \in Xf$, test whether $\{y\} b_1^{-1} h_1^{-1} \cdots b_k^{-1} h_k^{-1} = \{y\} f^{-1}$;
if this is so, then $f \in \langle A \rangle$. ∎

5. Characterization of Automata

We now solve the characterization problem in some varieties of threshold one monoids which were relevant to our study of the membership problem. Knowledge provided by this work is central to our proof of Lemma 4.11. Also, addressing this problem goes along with the intuition that it would make little sense to consider an instance of MEMB(**V**) for some variety **V** and declare it easy to solve, if it were hard to test whether this actually is an instance of MEMB(**V**). We show that transformation monoids in $\mathbf{GJ}_1$, $\mathbf{GR}_1$, and $\mathbf{GL}_1$ can be characterized in AC^0. Meanwhile, efficient characterizations for varieties $\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$, for $\mathbf{A}_1 \vee \mathbf{G}$, and for $\mathbf{DS}_1$, that is, algorithms which avoid testing exhaustively the defining identities on all monoid elements, still remain to be found.

The first result concerns variety of $\mathbf{GR}_1$. It shows that automata (X, A) for which $\langle A \rangle \in \mathbf{GR}_1$ are subject to restrictions which strongly influence their behaviour (condition 3 in the proposition). The same result is stated in another form (condition 2), which highlights those properties peculiar to $\mathbf{GR}_1$. This statement uses the notion of the alphabet of a strongly connected component $K \subseteq X$:

$$\mathscr{A}(K) = \{a \in A : K \cap Xa \neq \varnothing\}.$$

As mentioned previously, this proposition implies that, for any $g \in \langle A \rangle$, the group of those elements of $\langle A \rangle \in \mathbf{GR}_1$ which permute Xg is generated by a subset of A.

PROPOSITION 5.1. *The following statements on an automaton* (X, A) *are equivalent*:

(1) *the transformation monoid* $\langle A \rangle$ *of* (X, A) *belongs to* $\mathbf{GR}_1$;

(2) $\langle A \rangle \in \mathbf{DS}_1$ *and, for every SCC* K *and* $a \in A$, *either* $Ka \cap K = \varnothing$ *or* $Ka = K$;

(3) *for every* $a \in A$ *and SCC* K, *either* $Ka = K$ *or* $Ka \cap K = \varnothing$; *in the latter case, for every state* $x \in K$, xa *belongs to an SCC* K' *such that* $\mathscr{A}(K) \subset \mathscr{A}(K')$.

Proof. $(1 \Rightarrow 3)$ Let $\langle A \rangle \in \mathbf{GR}_1$ be a monoid of period p. Let $a \in A$ and SCC K be such that $Xa \cap K \neq \varnothing$, so that there are states $x \in X$ and $y \in K$ such that $xa = y$. Then, $a^{p+1} = a \Rightarrow ya \in K$. For every other state $z \in K$, there exists a transformation $f \in \langle A \rangle$ such that $yaf = z$. From this, we obtain

$$(af)^{p+1} = af \Rightarrow y(af)^{p+1} = yaf = z \Rightarrow za \in K,$$

and therefore $Ka \subseteq K$. In order to show that $Ka = K$, assume that there exist $x \in K$ and $h \in \langle A \rangle$ such that $xah \in K - Ka$. Then $aha^p = ah \Rightarrow xah \in Ka$, a contradiction. In the case where $K \cap Xa = \varnothing$, consider a state $x \in K$ and a generator $b \in \mathscr{A}(K)$; as shown above, b^p acts as the identity on K. Denoting by K' the SCC of xa, we have $xa = xb^p a = xb^p ab^p$, so that $K' \cap Xb \neq \varnothing$, and therefore $b \in \mathscr{A}(K')$.

$(3 \Rightarrow 2)$ Consider a state x and a transformation $g = a_1 \cdots a_r$, and denote by K the SCC of x. An induction on r shows that the image xg of x belongs to an SCC K' such that $\mathscr{A}(K) \cup \{a_1, ..., a_r\} \subseteq \mathscr{A}(K')$. Therefore, g permutes the states of K', and $xg^{p+1} = xg$ for some $p \geqslant 1$.

$(2 \Rightarrow 1)$ Let $\langle A \rangle$ be a threshold one monoid of period p. For any state x and transformations f and g of an automaton (X, A) satisfying (2), having $x(fg)^{p+1} = xfg$ implies $Ka \cap K \neq \varnothing$ for every generator $a \in \mathscr{A}(fg)$, where K denotes the SCC of xfg. Hence f and g act as permutations on K, and therefore $(xfg)f^p = xfg$. ∎

This result suggests an algorithm which decides whether the transformation monoid of an automaton belongs to $\mathbf{GR}_1$; computation of the SCCs is done in nondeterministic log-space, and condition (3) is verified on each of them in AC^0.

We now develop an alternate method to characterize a transformation monoid in this variety: we show that it suffices to test whether the generators satisfy the defining identities. This method has the advantage of being applicable to the varieties $\mathbf{GL}_1$ and $\mathbf{GJ}_1$.

PROPOSITION 5.2. *The transformation monoid of* (X, A) *belongs to* $\mathbf{GR}_1$ *if, and only if,* $\exists p > 0$: $\forall a, b \in A$, $a^{p+1} = a$ *and* $aba^p = ab$.

Proof. It suffices to prove the (*if*) direction; this is done in three steps. We first show that $aha^p = ah$ for every $a \in A$ and $h \in \langle A \rangle$, by induction on the length of an expression for h. Indeed, if $h = gb$, where $b \in A$ and $aga^p = ag$, then

$$agba^p = aga^pba^p = aga^{p-1}aba^p = aga^pb = agb.$$

Next, we show $\langle A \rangle \in \mathbf{DS}_1$, which is equivalent to proving that $Xh^2 = Xh$ for every $h \in \langle A \rangle$. With $h = ab$, where $a, b \in A$, assume that $Xabab \subset Xab$. This implies that $|Xabab| < |Xab|$, which means that

$$|Xaba| < |Xab| \vee |Xabab| < |Xaba|,$$

and this leads to a contradiction. Indeed, in the first case, we have

$$|Xab| = |Xaba^p| = |Xabaa^{p-1}| \leqslant |Xaba| < |Xab|;$$

in the second case,

$$|Xaba| = |Xabab^p| = |Xababb^{p-1}| \leqslant |Xabab| < |Xaba|.$$

The argument can be extended to longer expressions. Finally, we show that $ghg^p = gh$ for all $g, h \in \langle A \rangle$, by induction on the length of an expression for g. As an induction hypothesis, assume that $g = kb$, with $b \in A$, that $khk^p = kh$, and that $kbhk^p = kbh$. Then

$$gh = kbh = kbhk^p = kbhkk^{p-1} = kbhkbb^{p-1}k^{p-1}.$$

We then use the fact that $(kb)^{p+1} = kb$ to obtain

$$\begin{aligned} gh &= kbh(kb)\, b^{p-1}k^{p-1} = kbh(kb)^pkbb^{p-1}k^{p-1} \\ &= kbh(kb)^pkk^{p-1} = kbh(kb)^p = ghg^p. \quad \blacksquare \end{aligned}$$

COROLLARY 5.3. *The transformation monoid of* (X, A) *belongs to* $\mathbf{GL}_1$ *if, and only if,* $\exists p > 0$: $\forall a, b \in A$, $a^{p+1} = a$ *and* $a^pba = ba$.

COROLLARY 5.4. *The transformation monoid of* (X, A) *belongs to* $\mathbf{GJ}_1$ *if, and only if,* $\exists p > 0$: $\forall a, b \in A$, $a^{p+1} = a$ *and* $a^pb = ba^p$.

Whether the transformation monoid of (X, A) belongs to $\mathbf{GR}_1$, to $\mathbf{GL}_1$, or to $\mathbf{GJ}_1$, can therefore be decided in AC^0 with the following algorithm, which we write in terms of $\mathbf{GR}_1$. The first step consists in verifying whether each generator a is of threshold one. If this is so, then a^p can be computed in AC^0 with the method described in the proof of Lemma 4.4. Adaptation of the algorithm to varieties $\mathbf{GJ}_1$ or $\mathbf{GL}_1$ consists merely in modifying the test in step 2.

input: automaton (X, A); with $|X| = m$, let $p = m!$;
step 1: for every $a \in A$, test whether $Xa^2 = Xa$;
step 2: for every $a, b \in A$, test whether $aba^p = ab$.

6. Comments

Within the conjecture $NC \neq P \neq NP$, we have established in the main theorem a one-to-one correspondence between monoid varieties $\mathbf{J}_1$, $\mathbf{J}_1 \vee \mathbf{G}$, and $\mathbf{R}_1 \vee \mathbf{L}_1 \vee \mathbf{G}$ and complexity classes AC^0, NC, and P, respectively. This suggests that every class of computational complexity involved in the study of the membership problem is associated with a unique, largest variety of monoids. Therefore, a natural extension to our work would be to look for a largest variety in which the membership problem belongs to a complexity class such as NP. Given the results obtained on the aperiodic monoids, this would be an extension of the aperiodic variety **DA**, or of one of its subvarieties, maybe in the sense of our "maximal extensions." At least, Theorems 4.7 and 4.10 suggest that NP-completeness extends beyond $\mathbf{GR}_1$, $\mathbf{GL}_1$, and $\mathbf{A}_1 \vee \mathbf{G}$, quite probably to the "maximal extension" of $\mathbf{A}_1$, i.e., the whole of $\mathbf{DS}_1$. The significance of this correspondence between varieties of monoids and complexity classes remains to be determined. For instance, charting the whole lattice of this varieties of monoids from the viewpoint of the membership problem could prove true a property of the form "if **V** and **W** are two varieties such that MEMB(**V**) and MEMB(**W**) belong to complexity class X, then so does MEMB(**V** $\vee$ **W**)," whose meaning might extend beyond its immediate application to the study of the membership problem, and provide a powerful insight in the analysis of other problems in related areas.

Appendix

We show that the transformation monoid $\langle A \rangle$ of the automaton described in the proof of Lemma 4.9 belongs to the variety generated by $GR_{1(2)}$.

Denoting by N_j the transformation monoid of the automaton (C_j, A) formed by connected component C_j, $1 \leqslant j \leqslant m$, we observe that $\langle A \rangle \prec N_1 \times \cdots \times N_m$, so that it suffices to prove that each N_j belongs to $\langle GR_{1(2)} \rangle$. For $1 \leqslant i \leqslant 3$, define monoids $U_i = \{1, \alpha_i, \beta, \alpha_i\beta\}$ and $V_i = \{1, \alpha_i, \delta, \alpha_i\delta\}$; each is isomorphic to $GR_{1(2)}$. Define also $W = \{1, \beta, \delta\}$, such that $\beta\delta = \beta$ and $\delta\beta = \delta$. Further, let each α_i act as the identity in W, in U_k, and in V_k, for every $k \neq i$, while β (resp. δ) acts as 1 in the monoids V_k (resp. U_k),

$1 \leqslant k \leqslant 3$. Consider next the monoid M generated by $\{(c, c, c, c, c, c, c) : c \in \{\alpha_1, \alpha_2, \alpha_3, \beta, \delta\}\}$, a submonoid of the direct product of the seven monoids defined above, and therefore an element of the variety $\langle GR_{1(2)} \rangle$. We claim that N_j is a homomorphic image of M. To convince the reader of our point, we work on a simplified version of the problem, involving only monoids U_1, V_1, and W, and where all the features of the interaction between generators β and δ, and the α_i's, are retained; extending our argument to the actual monoid N_j is straightforward.

Consider the monoid M generated by $\{(c, c, c) : c \in \{\alpha_1, \beta, \delta\}\}$; it can be seen to be isomorphic to the transformation monoid of the set $\{1, 2, 3, 4, 5, 6, 7\}$, generated by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 4 & 6 & 6 & 7 \end{pmatrix}$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 6 & 7 & 7 & 6 & 7 \end{pmatrix}$$

This monoid has eighteen elements:

$$M' = \{1, \alpha, \beta, \delta, \alpha\beta, \alpha\delta, \beta\alpha, \beta\delta, \delta\alpha, \delta\beta, \alpha\beta\alpha, \alpha\beta\delta, \alpha\delta\alpha,$$
$$\alpha\delta\beta, \beta\alpha\delta, \delta\alpha\beta, \alpha\beta\alpha\delta, \alpha\delta\alpha\beta\}.$$

Its operation has the following properties:

$$\alpha^2 = 1 \qquad \beta^2 = \beta \qquad \delta^2 = \delta$$

$$\beta\alpha\beta = \beta\alpha \qquad \delta\alpha\delta = \delta\alpha \qquad \beta\delta\beta = \beta\delta \qquad \delta\beta\alpha = \delta\beta\delta = \delta\beta$$

$$\beta\alpha\delta\alpha = \beta\alpha\delta\beta = \beta\alpha\delta \qquad \delta\alpha\beta\alpha = \delta\alpha\beta\delta = \delta\alpha\beta$$

Meanwhile, our simplified version of N_j is the transformation monoid of the automaton $(\{T, F, 0, 1, x, y\}, \{a, b, d\})$, where the generators act as follows:

$$a = \begin{pmatrix} T & F & 0 & 1 & x & y \\ F & T & 1 & 0 & x & y \end{pmatrix} \qquad b = \begin{pmatrix} T & F & 0 & 1 & x & y \\ x & 0 & 0 & 1 & x & y \end{pmatrix}$$

$$d = \begin{pmatrix} T & F & 0 & 1 & x & y \\ x & x & y & x & x & y \end{pmatrix}$$

The ten elements of this monoid constitute the set

$$N = \{1, a, b, d, ab, ad, ba, aba, bad, abad\}$$

and satisfy the following properties:

$$a^2 = 1 \qquad b^2 = b \qquad d^2 = d$$
$$bab = ba \qquad da = db = d \qquad bd = d$$

The argument consists in verifying exhaustively on the two sets M and N that a function $\phi : M \to N$, such that $\phi(\alpha) = a$, $\phi(\beta) = b$, and $\phi(\delta) = d$, where we use $\phi(c)$ as a shorthand for $\phi((c, c, c))$, can be defined to have the properties that ϕ is a monoid homomorphism, that $\phi(\beta\delta) = d$, and that $\forall x \in M$, $\phi(\delta x) = d$.

ACKNOWLEDGMENTS

The author thanks Bernard Courteau and Pierre McKenzie for the helpful discussions he had with them on this article. Several improvements and corrections were also contributed by the referees.

RECEIVED November 5, 1990; FINAL MANUSCRIPT RECEIVED December 30, 1991

REFERENCES

AJTAI, M. (1983), Σ_1^1 formulae on finite structures, *Ann. Pure Appl. Logic* **24**, 1–48.

BABAI, L., LUKS, E. M., AND SERESS, A. (1987), Permutation groups in NC, *in* "Proceedings, 19th ACM Symposium on Theory of Computing," pp. 409–420.

BEAUDRY, M. (1988), Membership testing in commutative transformation semigroups, *Inform. and Comput.* **79**, 84–93.

BEAUDRY, M., MCKENZIE, P., AND THÉRIEN, D. (1989), Testing membership: Beyond permutation groups, *in* "Proceedings, 6th Symposium on Theoretical Aspects of Computer Science," pp. 388–399, Lecture Notes in Computer Science, Vol. 349, Springer-Verlag, New York/Berlin. [Journal version has appeared as The membership problem in aperiodic transformation monoids, *J. Assoc. Comput. Mach.* **39** (1992), 599–616.

BUSS, S. (1987), The formula value problem is in *ALOGTIME*, *in* "Proceedings, 19th ACM Symposium on Theory of Computing," pp. 123–131.

COOK, S. A. (1985), A taxonomy of problems with fast parallel solutions, *Inform. and Comput.* **64**, 2–22.

FENNEMORE, C. (1971), All varieties of bands I, II, *Math. Nachr.* **48**, 237–252 and 253–262.

FURST, M., HOPCROFT, J. E., AND LUKS, E. M. (1980), Polynomial time algorithms for permutation groups, *in* "Proceedings, 21st IEEE Symposium on Foundations of Computer Science," pp. 36–41.

FURST, M., SAXE, J. B., AND SIPSER, M. (1984), Parity, circuits, and the polynomial-time hierarchy, *Math. Systems Theory* **17**, 13–27.

GAREY, M., AND JOHNSON, D. (1979), "Computers and Intractability: A Guide to the Theory of NP-Completeness," Freeman, San Francisco.

GERHARD, J. A. (1970), The lattice of equational classes of idempotent semigroups, *J. Algebra* **15**, 195–224.

GREEN, J. A., AND REES, G. (1952), Semigroups such that $x^r = x$, *Proc. Cambridge Philos. Soc.* **48**, 35–40.

HOPCROFT, J. E., AND ULLMAN, J. D. (1979), "Introduction to Automata Theory, Languages, and Computation," Addison–Wesley, Reading, MA.

KOZEN, D. (1977), Lower bounds for natural proof systems, *in* "Proceedings, 18th IEEE Symposium on Foundations of Computer Science," pp. 254–266.

LALLEMENT, G. (1979), "Semigroups and Combinatorial Applications," Addison–Wesley, Reading, MA.

LUKS, E. M., (1986), Parallel algorithms for permutation groups and graph isomorphism, *in* "Proceedings, 27th IEEE Symposium on Foundations of Computer Science," pp. 292–302.

LUKS, E. M., AND MCKENZIE, P. (1988), Parallel algorithms for solvable permutation groups, *J. Comput. System Sci.* **37**, 39–62.

MCKENZIE, P., AND COOK, S. A. (1987), The parallel complexity of Abelian permutation groups problems, *SIAM J. Comput.* **16**, 880–909.

PETRICH, M. (1975), Varieties of orthodox bands of groups, *Pacific J. Math.* **58**, 209–217.

PIN, J.-É. (1984), "Variétés de langages formals," Masson, Paris; translated as "Varieties of Formal Languages," Plenum, New York.

SIMS, C. C. (1970), Computational methods in the study of permutation groups, *in* "Computational Problems in Abstract Algebra" (J. Leech, Ed.), pp. 169–183, Pergamon, Oxford.

SMOLENSKY, R., (1987), Algebraic methods in the theory of lower bounds for Boolean circuit complexity, *in* "Proceedings 19th ACM Symposium on Theory of Computing," pp. 77–82.

STERN, J. (1985), Complexity of some problems from the theory of automata, *Inform. and Comput.* **66**, 163–176.

WISMATH, S. L. (1986), The lattice of varieties and pseudovarieties of band monoids, *Semigroup Forum* **33**, 187–198.