Semigroup Forum Vol. 29 (1984) 99-108

RESEARCH ARTICLE

POWER MONOIDS AND FINITE $\mathcal{J}$-TRIVIAL MONOIDS

Stuart W. MARGOLIS and Jean-Eric PIN (*)

1. INTRODUCTION

Throughout this paper, except for free semigroups, all semigroups considered will be finite. Let M be a monoid. Then P(M), the power set of M forms a monoid under the usual multiplication of subsets. Power monoids have been studied in various contexts, either for their own interest ([7], [8]) or in connection with language theory ([3], [5], [6], [9], [11]). In this paper we investigate the properties of a submonoid of P(M), denoted by $P_1(M)$, which consists of all subsets of M containing the identity of M. Although the difference between P(M) and $P_1(M)$ may appear insignificant, there is a rather big gap between the two monoids. For example $P_1(M)$ is $\mathcal{J}$-trivial for *all* monoids M. The operation $M \to P_1(M)$ can be extended to varieties as follows. Let $\underline{V}$ be a variety of finite semigroups or monoids (i.e. a class of finite semigroups, or monoids, closed under division and finite direct products) and let $\underline{P_1V}$ be the variety of *monoids* generated by $\{P_1(S^1) \mid S \in \underline{V}\}$.

Our first result shows that the operation $\underline{V} \to \underline{P_1V}$ on varieties is equivalent to a simple operation on the corresponding varieties of languages (theorem 2.1). We also give a classification of the varieties $\underline{P_1V}$ when $\underline{V}$ is a variety of monoids (theorems 3.2, 3.4, 3.9). As a corollary, we deduce a new characterization of $\mathcal{J}$-trivial monoids (Corollary 3.8).

It is no longer a surprise to see that arguments of language theory are necessary to prove some statements of pure semigroup theory. In particular, just as in [4] [5] or [12], Simon's theorem [10] on piecewise testable languages is used as an important tool.

(*) Communicated by G. Lallement

NOTATIONS :

We refer the reader to the books by Eilenberg [1] or Lallement [2] for undefined terms in this paper and in particular for the definitions of a variety of monoids, semigroups or languages.

Eilenberg's variety theorem establishes a one-to-one correspondence between varieties of monoids (or semigroups) and $*$-varieties (+varieties) of languages. In the sequel, the term "corresponding variety" always refers to this correspondence. An example is provided by the theorem of Simon (see [1], [2] or [10]). Recall that a language over A is piecewise testable if it is in the boolean algebra generated by the languages of the form $A^*a_1A^*a_2\dots a_nA^*$, $n > 0$, $a_1,\dots,a_n \in A$. A monoid is $\mathcal{J}$-trivial if for all $a,b \in M$, $a \mathcal{J} b$ implies $a = b$. Then we have

THEOREM 1.1 [10] A language is piecewise testable iff its syntactic monoid is $\mathcal{J}$-trivial and finite.

Let us denote by $\underline{J}$ the variety of all finite $\mathcal{J}$-trivial monoids. Then the corresponding $*$variety $\mathcal{J}$ assigns to each alphabet A, the set $A^*\mathcal{J}$ of piecewise testable languages over A. We denote by $\underline{Com}$ the variety of all commutative monoids and by $\underline{A}$ the variety of aperiodic monoids. Note that $\underline{A} \cap \underline{Com} = \underline{J} \cap \underline{Com}$. A *non-commutative variety* is a variety that is not contained in $\underline{Com}$ that is, contains at least one non-commutative monoid. If S is semigroup, S^1 denotes the monoid equal to S if S is a monoid and to $S \cup \{1\}$ if S is not a monoid. $S^{(n)}$ denotes the direct product of n copies of S. The cyclic monoid $\{1,x,x^2,\dots,x^r = x^{r+1}\}$ is denoted by $Z_{1,r}$. Let M be a monoid. Then

$P_1(M) = \{A \mid A \subseteq M \text{ and } 1 \in A\}$ is a monoid under the multiplication

of subsets. Although M is always a submonoid of $P(M)$, M is not generally embedded in $P_1(M)$. Finally, if $\underline{V}$ is a variety of semigroups or monoids, $\underline{P_1V}$ is the variety of monoids generated by $\{P_1(S^1) \mid S \in \underline{V}\}$.

Let $L \subset A^*$ be a language. A monoid M recognizes L if there exist a morphism $\eta : A^* \to M$ and a subset P of M such that $L = P\eta^{-1}$

2. INVERSE 1-SUBSTITUTION

In this section, we show that the operation $\underline{V} \to \underline{P_1V}$ on varieties is equivalent to a simple operation on the corresponding families of recognizable sets. Recall that a *substitution* σ from A^* to B^* is a monoid morphism $\sigma : A^* \to P(B^*)$. One extends σ to a mapping from $P(A^*)$ by setting $L\sigma = \bigcup_{u \in L} u\sigma$. The *inverse substitution* σ^{-1} is the mapping from $P(B^*)$ to $P(A^*)$ defined by

$$K\sigma^{-1} = \{u \in A^* \mid u\sigma \cap K \neq \emptyset\}.$$

Thus, the term "inverse" is taken in the sense of relations since a substitution from A^* to B^* can also be viewed as a relation from A^* to B^*([5, p35] for more details). The connection between the operation $\underline{V} \to \underline{PV}$ on varieties and inverse substitution has been established in [5] (see also [9]). Thus it is not surprising to find the same connection between the more restricted operation $\underline{V} \to \underline{P_1V}$ and inverses of a restricted class of substitutions, called *1-substitutions*. Formally a 1-substitution σ from A^* to B^* is a substitution such that for all $a \in A$, $1 \in a\sigma$.
Given a +-variety (or *-variety) $\mathcal{V}$, define for any alphabet A, the class $A^*\bar{\mathcal{V}}$ as follows : $A^*\bar{\mathcal{V}}$ is the boolean algebra generated by languages of the form $L\sigma^{-1}$ for some 1-substitution $\sigma : A^* \to B^*$ and some language $L \in B^+\mathcal{V}$ $(B^*\mathcal{V})$.
Then we can state :

THEOREM 2.1 <u>Let $\underline{V}$ be a variety of semigroups (monoids) and let $\mathcal{V}$ be the corresponding +-variety (*-variety) of languages. Then the *-variety of languages corresponding to $\underline{P_1V}$ is precisely $\bar{\mathcal{V}}$, the variety obtained from $\mathcal{V}$ by boolean closure of inverses of languages under 1-substitutions</u>.

<u>Proof</u> :
Let $\mathcal{V}'$ be the $*$-variety corresponding to $\underline{P_1V}$. We have to prove $\mathcal{V}' = \bar{\mathcal{V}}$. We just discuss the case where $\underline{V}$ is a variety of semigroup, the monoid case being similar.
(a) $\bar{\mathcal{V}} \subseteq \mathcal{V}'$
Let $\sigma : A^* \to B^*$ be a 1-substitution and let $L \in B^+\mathcal{V}$. Then there exists a semigroup S in $\underline{V}$, a morphism $\eta : B^+ \to S$ and a subset P of S

such that $L = P\eta^{-1}$. By setting $1\eta = 1$, one extends η to a monoid morphism $\eta : B^* \to S^1$. Define a morphism $\varphi : A^* \to P_1(S^1)$ by setting, for all $a \in A$, $a\varphi = a\sigma\eta$, and let R be the subset of $P_1(S^1)$ defined by $R = \{Q \in P_1(S^1) \mid Q \cap P \neq \emptyset\}$. Then we have

$$\begin{aligned} R\varphi^{-1} &= \{u \in A^* \mid u\sigma\eta \cap P \neq \emptyset\} \\ &= \{u \in A^* \mid u\sigma \cap P\eta^{-1} \neq \emptyset\} \\ &= \{u \in A^* \mid u\sigma \cap L \neq \emptyset\} = L\sigma^{-1} \end{aligned}$$

Therefore, $L\sigma^{-1}$ is recognized by a monoid of $\underline{P_1V}$ and thus $L\sigma^{-1} \in A^*V'$ as required.

(b) $V' \subseteq \bar{V}$

Let A be an alphabet. Since $\underline{P_1V}$ is generated by the monoids $P_1(S^1)$ with $S \in \underline{V}$, A^*V' is equal to the Boolean algebra generated by languages of the form $R\eta^{-1}$ where $R \subseteq P_1(S^1)$ with $S \in \underline{V}$ and where $\eta : A^* \longrightarrow P_1(S^1)$ is a monoid morphism. Therefore it is sufficient to prove that $R\eta^{-1} \in A^*\bar{V}$. Since $R = \bigcup_{Q \in R}\{Q\}$ one has only to show that $\{Q\}\eta^{-1} \in A^*\bar{V}$ for all $Q \in P_1(S^1)$. Set, for $P \subseteq S \cup \{1\}$,

$R_P = \{R \in P_1(S^1) \mid R \cap P \neq \emptyset\}$.

Then an elementary computation shows that $\{Q\} = \left(\bigcap_{q \in Q \setminus \{1\}} R_{\{q\}}\right) \setminus R_{S \setminus Q}$. (1)

Therefore, since η^{-1} commutes with Boolean operations, we just have to show -according to (1)- that $R_P\eta^{-1} \in A^*\bar{V}$ for all $P \subset S \setminus \{1\}$. Let $\alpha : B \to S$ be a bijection. Extend α to a semigroup morphism $\alpha : B^+ \to S$ and to a monoid morphism $\bar{\alpha} : B^* \to S^1$. Next define a 1-substitution $\sigma : A^* \to B^*$ by setting $a\sigma = (a\eta)\bar{\alpha}^{-1}$ for all $a \in A$.

We claim that

$$R_P\eta^{-1} = P\alpha^{-1}\sigma^{-1} \tag{2}$$

Taking (2) for granted, we can easily prove the theorem. Indeed, since $S \in \underline{V}$, we have $P\alpha^{-1} \in B^+V$ and thus $P\alpha^{-1}\sigma^{-1} \in A^*\bar{V}$ by the definition of $\bar{V}$. Thus by (2), $R_P\eta^{-1} \in A^*\bar{V}$ as required.

We now prove (2). First, since $1\sigma = \{1\}$, we have $1\sigma \cap P\alpha^{-1} = \emptyset$,

and since $1 \notin P$, $P\alpha^{-1} = P\bar{\alpha}^{-1}$. Therefore $P\alpha^{-1}\sigma^{-1} = \{u \in A^+ \mid u\sigma \cap P\bar{\alpha}^{-1} \neq \emptyset\}$
Similarly, since $1\eta = \{1\}$, we have $1\eta \cap P = \emptyset$ and thus

$$R_P\,\eta^{-1} = \{u \in A^+ \mid u\eta \cap P \neq \emptyset\}.$$

Consequently it is sufficient to show that for all $u \in A^+$ the condition (i) $u\sigma \cap P\bar{\alpha}^{-1} \neq \emptyset$ and (ii) $u\eta \cap P \neq \emptyset$ are equivalent. The fact that (i) implies (ii) follows from the following sequences of inclusions :

$$(u\sigma \cap P\bar{\alpha}^{-1})\bar{\alpha} \subset ((u\eta)\bar{\alpha}^{-1} \cap P\bar{\alpha}^{-1})\bar{\alpha} \subset (u\eta)\bar{\alpha}^{-1}\bar{\alpha} \cap P\bar{\alpha}^{-1}\bar{\alpha} = u\eta \cap P$$

Conversely, assume $u\eta \cap P \neq \emptyset$. If $u = a_1 \ldots a_n$ with $a_1, \ldots, a_n \in A$, there exist $p_1 \in a_1\eta, \ldots, p_n \in a_n\eta$: such that $p_1 \ldots p_n = p \in P$. Let $v_1 \in p_1\alpha^{-1}, \ldots, v_n \in p_n\alpha^{-1}$ and $v = v_1 \ldots v_n$. Then $v\alpha \in P$ and thus $v \in u\sigma \cap P\alpha^{-1} = u\sigma \cap P\bar{\alpha}^{-1}$. Therefore $u\sigma \cap P\bar{\alpha}^{-1} \neq \emptyset$ and (ii) implies (i) as required. This concludes the proof of the theorem.

3. MAIN RESULTS.

The aim of this section is to describe varieties of the form $\underline{P}_1\underline{V}$ where $\underline{V}$ is a variety of monoids. We start with a useful observation.

PROPOSITION 3.1 *If $\underline{V}$ is a variety of monoids then $\underline{P}_1\underline{V}$ is contained in $\underline{J}$, the variety of all $\mathcal{J}$-trivial monoids.*

Proof Let M be a monoid and let A and B be two $\mathcal{J}$-related elements in $P_1(M)$. Then $CAC' = B$, $DBD' = A$ for some $C, C', D, D' \in P_1(M)$ and therefore $A = 1.A.1 \subseteq B$ and $1.B.1 \subseteq A$. Thus $A = B$ and $P_1(M)$ is $\mathcal{J}$-trivial.

The next theorem provides a complete description of $\underline{P}_1\underline{V}$ when $\underline{V}$ is a variety of commutative monoids.

THEOREM 3.2 *Let $\underline{V}$ be a variety of commutative monoids*

(1) *If $\underline{V}$ is the trivial variety, so is $\underline{P}_1\underline{V}$.*

(2) *If $\underline{V}$ is a commutative non trivial variety, then $\underline{P}_1\underline{V} = \underline{J} \cap \underline{Com}$, the variety of all commutative $\mathcal{J}$-trivial monoids.*

Proof (1) is clear

(2) If M is a commutative monoid, so is $P_1(M)$. Thus the inclusion $\underline{P_1V} \subset \underline{J} \cap \underline{Com}$ follows at once from proposition 3.1. We now prove the opposite inclusion. Let $M \neq 1$ be a monoid in $\underline{V}$ and let n be a positive integer.

Define $a \in P_1(M^{(n)})$ to be the subset of $M^{(n)}$ consisting of all n-tuples $(m_1, \ldots, m_n)$ having at least $(n-1)$ components equal to 1. Then, for $1 < r < n$, a^r is the set of all n-tuples having at least $(n-r)$ components equal to 1. It follows that the submonoid of $P_1(M^{(n)})$ generated by a is isomorphic with the cyclic monoid $Z_{1,n}$, and thus $Z_{1,n} \in \underline{P_1V}$. Since $\underline{J} \cap \underline{Com}$ is generated by the monoids $Z_{1,n}$ $(n > 0)$ - see [1] - we have $\underline{J} \cap \underline{Com} \subset \underline{P_1V}$ and this completes the proof of (2).

We turn now to non-commutative varieties of monoids. As shown in [4] one can distinguish two main families of such varieties.

PROPOSITION 3.3 *Let $\underline{V}$ be a non commutative variety of monoids. Then $\underline{V}$ contains either a non-commutative aperiodic monoid or a non-commutative group.*

We first consider the case where $\underline{V}$ contains a non-commutative aperiodic monoid.

THEOREM 3.4 *If $\underline{V}$ is a variety containing a non-commutative aperiodic monoid, then $\underline{P_1V} = \underline{J}$.*

Proof : The inclusion $\underline{P_1V} \subseteq \underline{J}$ follows from proposition 3.1. The opposite inclusion requires a sequence of lemmata the first two of which were proved in [4].

LEMMA 3.5 *If $\underline{V}$ is a variety containing a non-commutative aperiodic monoid then one of the following conditions holds :*

(1) $\underline{V}$ contains the variety $\underline{R}_1$ of all R-trivial and idempotent monoids,

(2) $\underline{V}$ contains the variety $\underline{R}_1^r$ of all L-trivial and idempotent monoids,

(3) $\underline{V}$ contains the syntactic monoid M_6 of $\{ab\}$ over the alphabet $\{a,b\}$

LEMMA 3.6

If n is a positive integer, let us set $A_n = \{a_1,\dots,a_n,\bar{a}_1\dots,\bar{a}_n\}$.

(1) If $\underline{V}$ contains $\underline{R}_1$, then for all $n > 0$, A_n^*V, contains the language

$$K_n = \{\bar{a}_1,\dots,\bar{a}_n\}^* a_1 \{\bar{a}_1,\dots,\bar{a}_n,a_1\}^* a_2 \dots a_n \{\bar{a}_1,\dots,\bar{a}_n,a_1,\dots,a_n\}^*.$$

(2) If $\underline{V}$ contains $\underline{R}_1^r$, then for all $n > 0$, A_n^*V contains the language

$$K_n' = \{\bar{a}_1,\dots,\bar{a}_n,a_1,\dots,a_n\}^* a_1 \dots a_n \{\bar{a}_1,\dots,\bar{a}_n\}^*.$$

(3) If $\underline{V}$ contains M_6, then for all $n > 0$, A_n^*V contains the language $L_n = \{a_1\dots a_n\}$.

The next lemma is an immediate consequence of lemmata 3.5 and 3.6.

LEMMA 3.7

Set, for $n > 0, A_n = \{a_1,\dots,a_n, \bar{a}_1,\dots,\bar{a}_n\}$. If $\underline{V}$ contains a non commutative aperiodic monoid then for all $n > 0$, A_n^*V contains a language L_n such that $\{a_1\dots a_n\} \subseteq L_n \subseteq A_n^* a_1 A_n^* \dots a_n A_n^*$.

We now conclude the proof of theorem 3.4 :

Let B be an alphabet and let $b_1,\dots,b_n$ be a sequence of n (not necessarily distinct) letters of B. Define a 1-substitution $\sigma : B^* \to A_n^*$ by setting, for all $b \in B$, $b\sigma = \{1\} \cup \{a_k \mid b_k = b\}$.

By Lemma 3.7, there exists a language L such that

$$\{a_1\dots a_n\} \subseteq L \subseteq A_n^* a_1 A_n^* \dots a_n A_n^*$$

Therefore we have

$$(a_1 \dots a_n)\sigma^{-1} \subseteq L\sigma^{-1} \subseteq (A_n^* a_1 A_n^* \dots a_n A_n^*)\sigma^{-1} \quad \text{i.e.}$$

$B^* b_1 B^* \dots b_n B^* \subseteq L\sigma^{-1} \subseteq B^* b_1 B^* \dots b_n B^*$.

It follows that $L\sigma^{-1} = B^* b_1 B^* \dots b_n B^*$. Thus, with the notations of theorem 2.1, we have $L\sigma^{-1} \in B^*V$ and thus B^*V contains all piecewise testable languages. By Simon's theorem 1.1 and theorem 2.1 we deduce that $\underline{J}$ is contained in $\underline{P}_1\underline{V}$.

COROLLARY 3.8

For any non commutative aperiodic monoid M *and for any* $\mathcal{J}$*-trivial monoid* N, *there exists an integer* $n > 0$ *such that* N *divides* $P_1(M^{(n)})$.

PROOF : let M and M' be two monoids. It is easy to see that if M is a submonoid (quotient) of M', then $P_1(M)$ is a submonoid (quotient) of $P_1(M')$. Moreover $P_1(M) \times P_1(M')$ is a submonoid of $P_1(M \times M')$. Therefore if $\underline{V}$ is the variety generated by M, then every element of $\underline{P}_1\underline{V}$ divides $P_1(M^{(n)})$ for some $n > 0$. Now theorem 3.4 shows that if M is a noncommutative aperiodic monoid then $\underline{P}_1\underline{V} = \underline{J}$. Thus every $\mathcal{J}$-trivial monoid N divides $P_1(M^{(n)})$ for some $n > 0$.

THEOREM 3.9 (1) *If* $\underline{V}$ *is a variety of monoids containing a non-commutative group, then* $\underline{P}_1\underline{P}_1\underline{V} = \underline{J}$.

(2) *If* $\underline{V}$ *contains all p-groups for some prime* p, *then* $\underline{P}_1\underline{V} = \underline{J}$.

PROOF : (1) By theorem 3.4 it is sufficient to show that $\underline{P}_1\underline{V}$ contains a noncommutative aperiodic monoid. Let G be a non-commutative group of $\underline{V}$ and let $a,b \in G$ such that $ab \neq ba$. Assume that $\{1,a\}\{1,b\} = \{1,b\}\{1,a\}$ holds in $P_1(G)$, that is

$\{1,a,b,ab\} = \{1,a,b,ba\}$. Then $ab = 1,b$ or a and thus $a=b$, $a=1$ or $b=1$. In any case $ab = ba$, a contradiction. Thus $P_1(G)$ is a non-commutative monoid and by proposition 3.1 this monoid is $\mathcal{J}$-trivial, hence aperiodic.

(2) Let $\underline{V}$ be a variety containing all p-groups for some prime p. Let A_n be as in Lemma 3.7. It follows from theorem 10.1 of [1] that

$L_n = \{w \in A_n^* \mid \binom{w}{a_1 \ldots a_n} \equiv 1 (\mathrm{mod}\, p)\} \in A_n^* \mathcal{V}$. Here $\binom{w}{a_1 \ldots a_n}$ denotes the number of factorizations of w of the form $w = u_1 a_1 u_2 a_2 \ldots u_n a_n u_{n+1}$ where $a_i \in A$ $u_i \in A_n^*$, $1 < i < n+1$. Clearly $\{a_1 \ldots a_n\} \subseteq L_n \subseteq A_n^* a_1 A_n^* a_2 \ldots a_n A_n^*$. The rest of the proof is as in Lemma 3.7.

We do not know if theorem 3.9 is in its best form as stated. More precisely it might happen that $\underline{P}_1\underline{V} = \underline{J}$ holds for all non commutative varieties of monoids $\underline{V}$.

REFERENCES

(1) Eilenberg, S., Automata, Languages and Machines, Academic Press, New-York, 1974(Vol. A) and 1976(Vol. B).

(2) Lallement, G., Semigroups and Combinatorial Applications, Wiley, New-York, 1979.

(3) Margolis, S.W., On M- Varieties Generated by Power Monoids. Semigroup Forum, 22, (1981) 339-354.

(4) Margolis, S.W. and Pin, J.E., Minimal Noncommutative Varieties of Finite Monoids. To appear in Pacific Journal of Mathematics.

(5) Pin, J.E., Variétés de Langages et Monoïde des Parties. Semigroup Forum Vol. 20 (1980) 11-47.

(6) Pin, J.E., Varietés de Langages et Variétés de Semigroupes. Thèse Paris (1981).

(7) Putcha, M., On the Maximal Semilattice Decomposition of the Power Semigroup of a Semigroup. Semigroup Forum Vol. 15(1978) 263-267.

(8) Putcha, M., Subgroups of the Power Semigroup of a Finite Semigroup. Can. J. Math. Vol XXXI, N° 5, 1979, 1077-1083.

(9) Reutenauer, Ch., Sur les Variétés de Langages et de Monoides. 4th GI Conférence, Lecture Notes in Computer Science 67, Springer, (1979), 260-265.

(10) Simon I., Piecewise Testable Events in Automata Theory and Formal Languages, 2nd GI Conference, Lecture Notes in Computer Science 33, Springer (1975) 214-222.

(11) Straubing, H., Recognizable Sets and Power Sets of Finite Semigroups. Semigroup Forum., Vol 18 (1979) 331-340.

(12) Straubing, H., On Finite $\mathcal{J}$-trivial Monoids. Semigroup Forum 19, (1980) 107-110.

STUART W. MARGOLIS
Department of Computer Science and Electrical Engineering
The University of Vermont
Burlington, VT 05405
U.S.A.

JEAN ERIC PIN
Laboratoire d'Informatique Théorique et de Programmation
Université Paris VI et CNRS
Tour 55-65, 4 place Jussieu
75230 Paris Cedex 05 FRANCE

Received May 2, 1983 and July 15, 1983 in revised and final form.