# Power Semigroups and Polynomial Closure

Stuart W. Margolis
Department of Computer Science
Bar Ilan University
52900 Ramat Gan, Israel

Benjamin Steinberg
Faculdade de Ciências
da Universidade do Porto
4099-002 Porto, Portugal*

April 17, 2000

**Abstract**

We show that the pseudovariety of semigroups which are locally block groups is precisely that generated by power semigroups of semigroups which are locally groups; that is $\mathbf{P}(\mathbf{LG}) = \mathbf{L}(\mathbf{PG})$ (using that $\mathbf{PG} = \mathbf{BG}$). We also will show that this pseudvariety corresponds to the Boolean polynomial closure of the $\mathbf{LG}$-languages which is hence polynomial time decidable.

More generally, it is shown that if $\mathbf{H}$ is a pseudovariety of groups closed under semidirect product with the pseudovariety of $p$-groups for some prime $p$, then the pseudovariety of semigroups associated to the Boolean polynomial closure of the $\mathbf{LH}$-languages is $\mathbf{P}(\mathbf{LH})$. The polynomial closure of the $\mathbf{LH}$-languages is similarly characterized.

## 1 Introduction

A common approach to studying rational languages is to attempt to decompose them into simpler parts. Concatenation hierarchies allow this to be done in a natural way which, in addition, has applications to logic and circuit theory [8]. A concatenation hierarchy is built up from a base variety of languages $\mathbf{V}$ by taking, alternately, the polynomial closure and the boolean polynomial closure of the previous half level of the hierarchy. The most famous example in the literature of such a hierarchy is the dot-depth hierarchy, introduced by Brzozowski [2], which starts of with the trivial +-variety, and whose union is the +-variety of star-free (aperiodic) languages.

*The second author was supported in part by NSF-NATO postdoctoral fellowship DGE-9972697, and by FCT through *Centro d e Matemática da Universidade do Porto.*

Pin and Margolis [6] also studied the group hierarchy which takes as its base the $*$-variety of all group languages.

In [13, 14], the author studied the levels one-half and one of the concatenation hierarchy associated to a pseudovariety of groups $\mathbf{H}$. In particular, it was shown that if $\mathbf{H}$ is a pseudovariety of groups closed under semidirect product with the pseudovariety $\mathbf{G}_p$ of $p$-groups for some prime $p$, then

$$\mathbf{PH} = BPol(\mathbf{H})$$

where $BPol(\mathbf{H})$ is the pseudovariety corresponding to the Boolean polynomial closure of the $\mathbf{H}$-languages [8]. A similar equality was shown to hold between the pseudovariety corresponding to the polynomial closure of the $\mathbf{H}$-languages and an ordered analog of $\mathbf{PH}$. All the aforementioned pseudovarieties were considered as pseudovarieties of monoids.

In this paper, we prove a semigroup analog of these results; here $\mathbf{H}$ is replaced by $\mathbf{LH}$, the pseudovariety of semigroups whose submonoids are in $\mathbf{H}$; we are then able to show that $BPol(\mathbf{LH}) = \mathbf{P}(\mathbf{LH})$ and its ordered analog (provided, of course, $\mathbf{H} = \mathbf{G}_p * \mathbf{H}$ for some prime $p$). Special cases include: $\mathbf{G}$, the pseudovariety of finite groups; $\mathbf{G}_p$; $\mathbf{G}_{sol}$, the pseudovariety of finite solvable groups. For the case of $\mathbf{G}$, we can characterize $\mathbf{P}(\mathbf{LG})$ as $\mathbf{L}(\mathbf{PG})$, semigroups which are locally block groups; hence $BPol(\mathbf{LG})$ has a polynomial time membership algorithm.

## 2 Preliminaries

As this paper extends the results of [14] to the semigroup context, it seems best to refer the reader there for basic notation and definitions, only monoids will be replaced throughout by semigroups; the reader is also referred to the general references [1, 3, 7, 8].

A *semigroup* $S$ is a set with an associative multiplication. An *ordered semigroup* $(S, \leq)$ is a semigroup $S$ with a partial order $\leq$, *compatible* with the multiplication; that is to say, $m \leq n$ implies $rm \leq rn$ and $mr \leq nr$. Any semigroup $S$ can be viewed as an ordered semigroup with the equality relation as the ordering, and free semigroups will always be regarded this way.

An *order ideal* of an ordered semigroup $(S, \leq)$ is a subset $I$ such that $y \in I$ and $x \leq y$ implies $x \in I$. We note that the collection of order ideals is closed under union and intersection. If $X \subseteq S$ and $s \in S$, then $s^{-1}X$ and $Xs^{-1}$ will denote, as usual, the, respectively, *left* and *right quotients* of $X$ by $s$. If $I$ is an order ideal, then so is any of its left or right quotients.

Morphisms of ordered semigroups are defined in the natural way. One can also define recognizability of a subset of an ordered semigroup; the only difference is that all subsets in the usual definition are now required to be order ideals.

A *pseudovariety* of (ordered) semigroups is a class of finite (ordered) semigroups closed under finite products (with the product order), submonoids (with the induced order), and images under (order-preserving) morphisms. Pseudovarieties of (ordered) monoids are defined similarly. An important example of such is $\mathbf{J}^+ = [\![x \leq 1]\!]$ (finite ordered monoids with 1 as the greatest element). We use $\mathbf{N}$ for the pseudovariety of nilpotent semigroups (finite semigroups $S$ such that $S^n = 0$ for some $n > 0$). We often identify a pseudovariety of semigroups with the pseudovariety of ordered semigroups which it generates.

If $S$ is a semigroup, the power set $\mathcal{P}(S)$ is a semigroup under setwise multiplication. We use $\mathcal{P}'(S)$ for the subsemigroup consisting of the nonempty subsets of $S$. We note that the order $\supseteq$ on $\mathcal{P}(S)$ is compatible with the multiplication. If $U_1 = \{0, 1\}$ under multiplication, one can show that $\mathcal{P}(S)$ is a quotient of a subsemigroup of $U_1 \times \mathcal{P}'(S)$.

If $\mathbf{V}$ is a pseudovariety of semigroups, we use $\mathbf{PV}$ to denote the pseudovariety generated by semigroups of the form $\mathcal{P}(S)$ with $S \in \mathbf{V}$, and $\mathbf{P'V}^+$ to denote the pseudovarieties generated by ordered semigroups of the form $(\mathcal{P}'(S), \supseteq)$ with $S \in \mathbf{V}$. Suppose that $\mathbf{V}$ contains a non-trivial monoid $M$; then $\{\{1\}, M\} \subseteq \mathcal{P}'(M)$ is isomorphic to $U_1$. It now follows from the previous paragraph that if $\mathbf{V}$ contains a non-trivial monoid, then $\mathbf{PV}$ is generated, as a pseudovariety of semigroups, by $\mathbf{P'V}^+$.

If $\mathbf{V}$ is a pseudovariety of (ordered) monoids, $\mathbf{LV}$ denotes the pseudovariety of (ordered) semigroups, all of whose submonoids are in $\mathbf{V}$. For instance, $\mathbf{LJ}^+ = [\![x^\omega y x^\omega \leq x^\omega]\!]$ where $x^\omega$ is interpreted as the idempotent power of $x$.

If $\mathbf{V}$ is a pseudovariety of (ordered) semigroups, then $\mathbf{EV}$ is the pseudovariety of (ordered) semigroups whose idempotents generate a subsemigroup in $\mathbf{V}$.

A *relational morphism* of (ordered) semigroups $\mu : S \rightarrow\!\!\!\!\!\!\circ\,\,\, T$ is a function $\mu : S \rightarrow \mathcal{P}'(T)$ such that $s_1\mu s_2\mu \subseteq (s_1 s_2)\mu$ for all $s_1, s_2 \in S$. Note that if $S$ is an (ordered) semigroup and $e \in T$ is an idempotent, then $e\mu^{-1}$ is a subsemigroup of $S$ (where $e\varphi^{-1}$ is the inverse relation). If $\mathbf{V}$, $\mathbf{W}$ are pseudovarieties of (ordered) semigroups, then the Mal'cev product $\mathbf{V} \textcircled{m} \mathbf{W}$ consists of all (ordered) semigroups $S$ with a relational morphism $\varphi : S \rightarrow\!\!\!\!\!\!\circ\,\,\, W \in \mathbf{W}$ such that $e\varphi^{-1} \in \mathbf{V}$ for each idempotent $e$ of $W$. One can show that $\mathbf{V} \textcircled{m} \mathbf{W}$ is generated by (ordered) semigroups $S$ with a homomorphism $\varphi : S \rightarrow W \in \mathbf{W}$ such that $e\varphi^{-1} \in \mathbf{V}$ for each idempotent $e$

of $W$.

If $\mathbf{V}_1$ and $\mathbf{V}_2$ are pseudovarieties of (ordered) semigroups, then $\mathbf{V}_1 * \mathbf{V}_2$ denotes the pseudovariety generated by semidirect products of (ordered) semigroups in $\mathbf{V}_1$ with those in $\mathbf{V}_2$. The semidirect product is an associative operations on pseudovarieties; see [1, 3, 14, 11] for more details. If $\mathbf{V}_1$ and $\mathbf{V}_2$ are pseudovarieties of groups, $\mathbf{V}_1 * \mathbf{V}_2$ can be shown to consist of all groups which are an extension of a group in $\mathbf{V}_1$ by a group in $\mathbf{V}_2$.

If $A$ is an alphabet, we let $Rec(A^+)$ denote the recognizable subsets of $A^+$. A *class of recognizable languages* is a correspondence $\mathbf{C}$ which associates to each alphabet $A$, a set $\mathbf{C}(A^+) \subseteq Rec(A^+)$. If $\mathbf{V}$ is a pseudovariety of ordered semigroups, then one can define a class of recognizable languages, which we also denote by $\mathbf{V}$, by letting $\mathbf{V}(A^+)$ be the set of all languages of $A^+$ recognized by a member of $\mathbf{V}$. Then the following result, proved by Eilenberg [3] for semigroups and by Pin [7] in the version below, holds.

**Proposition 2.1.** *Let* $\mathbf{V}$ *and* $\mathbf{W}$ *be pseudovarieties of ordered semigroups. Then* $\mathbf{V} \subseteq \mathbf{W}$ *if and only if, for each finite alphabet* $A$, $\mathbf{V}(A^+) \subseteq \mathbf{W}(A^+)$.

This, of course, leaves the question as to which classes arise in this fashion. The answer is again due to Eilenberg [3] for semigroups and Pin [7] for ordered semigroups. A *positive variety* of languages is a class of recognizable languages $\mathbf{V}$ such that:

1. For every alphabet $A$, $\mathbf{V}(A^+)$ is closed under finite unions and intersections;
2. If $\varphi : A^+ \to B^+$ is a morphism, then $L \in \mathbf{V}(B^+)$ implies $L\varphi^{-1} \in \mathbf{V}(A^+)$;
3. If $L \in \mathbf{V}(A^+)$ and $a \in A$, then $a^{-1}L, La^{-1} \in \mathbf{V}(A^+)$.

A *variety of languages* is a positive variety closed under complementation.

**Proposition 2.2.** *If* $\mathbf{V}$ *is a pseudovariety of (ordered) semigroups, the class* $\mathbf{V}$ *is a (positive) variety.*

If $\mathbf{V}$ is a (positive) variety of languages, then we associate to it the pseudovariety, also denoted by $\mathbf{V}$, generated by syntactic (ordered) semigroups [7, 8, 14] of languages $L \in \mathbf{V}(A^+)$ for some finite alphabet $A$. The reason for this abuse of notation is that the class of rational languages associated to the pseudovariety $\mathbf{V}$ obtained in this manner is the original (positive) variety.

## 3 Polynomials

If $\mathbf{V}$ is a pseudovariety of semigroups and $A$ an alphabet, then a *monomial* over $\mathbf{V}$ in variables $A$ is an expression

$$u_0 L_1 u_1 \cdots u_{n-1} L_n u_n$$

with the $u_i \in A^*$, $L_i \in \mathbf{V}(A^+)$, and $u_0$ non-empty if $n = 0$. A *polynomial* over $\mathbf{V}$ in variables $A$ is a finite union of monomials (over $\mathbf{V}$ in variables $A$).

The class

$$Pol(\mathbf{V})(A^+) = \{\text{polynomials over } \mathbf{V} \text{ in variables } A\}$$

is then a positive variety of languages [10]. We let $BPol(\mathbf{V})(A^+)$ be the closure of $Pol(\mathbf{V})(A^+)$ under finite boolean operations. Then one can verify that $BPol(\mathbf{V})$ is a variety of languages. One defines a hierarchy of (positive) varieties of languages as follows:

- $\mathbf{V}_0 = \mathbf{V}$;
- $\mathbf{V}_{n+\frac{1}{2}} = Pol(\mathbf{V}_n)$;
- $\mathbf{V}_{n+1} = BPol(\mathbf{V}_n)$.

The dot depth hierarchy [2] comes from letting $\mathbf{V}_0$ be the trivial pseudovariety.

We recall the following important theorem of Pin and Weil [10].

**Theorem 3.1.** *Let $\mathbf{V}$ be a pseudovariety of ordered semigroups. Then $Pol(\mathbf{V}) = \mathbf{LJ}^+ ⓜ \mathbf{V}$.*

We end this section with a technical lemma.

**Lemma 3.2.** *Let $\mathbf{V}$ be a pseudovariety of semigroups containing $\mathbf{N}$. Then every polynomial in $\mathbf{V}$ over $A$ can be written as a finite union of monomials of the form $L_0 a_1 \cdots a_n L_n$ with the $a_i \in A$ and the $L_i \in \mathbf{V}(A^+)$.*

*Proof.* The hypotheses are equivalent to assuming $\mathbf{V}$ contains all finite languages. It suffices to show that any monomial $M = u_0 K_1 u_1 \cdots u_{n-1} K_n u_n$ with the $u_i \in A^*$ and $K_i \in \mathbf{V}(A^+)$ can be so expressed. We induct on $n$ which we refer to as the *degree* of $M$. If $n = 0$, then by taking $L_0 = \{u_0\}$ we are done; now assume $n > 0$. Observe that if $w \in K_1$, then

$$M = (u_0 w u_1) K_2 \cdots u_{n-1} K_n u_n \cup u_0 (K_1 \setminus \{w\}) u_1 K_2 \cdots u_{n-1} K_n u_n. \quad (1)$$

Since $\mathbf{V}(A^+)$ contains all finite languages, it follows that $K_1 \setminus \{w\} \in \mathbf{V}(A^+)$. Since the first term in (1) has smaller degree, the above argument shows that we can remove a finite number of words from $K_1$. In particular, we may assume that every word in $K_1$ has length at least 5. Note that $(u^{-1}K_1v^{-1}) \in \mathbf{V}(A^+)$ for all $u, v \in A^+$. Since every word in $K_1$ is assumed to have length at least 5, it follows that

$$K_1 = \bigcup_{u,v\in A^2} u(u^{-1}K_1v^{-1})v$$

and so

$$M = \bigcup_{u,v\in A^2} (u_0u)(u^{-1}K_1v^{-1})(vu_1)\cdots u_{n-1}K_nu_n.$$

Thus we may assume that $u_0$ and $u_1$ have length at least 2. Suppose $u_0 = wa$ and $u_1 = a'w'$ with $a, a' \in A$, $w, w' \in A^+$. Then let $L_0 = \{w\}$, $a_1 = a$, $L_1 = K_1$, $a_2 = a'$. Now $M' = w'K_2u_2\cdots u_{n-1}K_nu_n$ has smaller degree and hence can be expressed as a finite union of monomials of the desired form. But then $M = L_0a_1L_1a_2M'$ can be written as a finite union of the monomials of the desired form. $\square$

## 4 Counters

Suppose that we have $a_1, \ldots, a_n \in A$, and $L_0, \ldots, L_n \subseteq A^+$. Then, for $0 \le r < m$, we define

$$(L_0a_1\cdots a_nL_n)_{r,m}$$

to consist of those words $w \in A^+$ with exactly $r$ factorizations of the form $w_0a_1\cdots a_nw_n$, with $w_i \in L_i$ all $i$, modulo $m$. Such a language is called a *product with $m$-counter*. A variety of languages is said to be *closed under products with $m$-counter* if $L_0, \ldots, L_n \in \mathbf{V}(A^+)$ implies that $(L_0a_1\cdots a_nL_n)_{r,m} \in \mathbf{V}(A^+)$. The following result is due to Weil [17].

**Theorem 4.1.** *Let $\mathbf{V}$ be a pseudovariety of semigroups. Then $\mathbf{V}$ is closed under products with $p$-counters, $p$ a prime, if and only if $\mathbf{V} = \mathbf{LG}_p \textcircled{m} \mathbf{V}$.*

## 5 The Power Operator and Polynomial Closure

We will need the following version [14, Proposition 5.1] of a well-known proposition (see, for instance, [8] which also references the original sources); the proof is included for completeness. If $B$ and $A$ are alphabets, a homomorphism $\varphi : B^+ \to A^+$ is called a *literal morphism* if $B\varphi \subseteq A$.

**Proposition 5.1.** *Let $L \in Rec(B^+)$ be recognized by a semigroup $S$, with $L = P\psi^{-1}$, and $\varphi : B^+ \to A^+$ be literal morphism. Then $(\mathcal{P}(S), \supseteq)$ recognizes $L\varphi$. If, in addition, $B\varphi = A$, then $(\mathcal{P}'(S), \supseteq)$ recognizes $L\varphi$.*

*Proof.* Let $\psi : B^+ \to S$ be a morphism and $P \subseteq S$ with $L = P\psi^{-1}$. We define a morphism $\tau : A^+ \to (\mathcal{P}(S), \supseteq)$ by $a\tau = \{b\psi | b \in B, b\varphi = a\}$ for $a \in A$, and we let

$$Q = \{X \in \mathcal{P}(S) | X \cap P \neq \emptyset\}.$$

Note that if $B\varphi = A$, then $a\tau \neq \emptyset$ for all $a \in A$, whence $A^+\tau \subseteq \mathcal{P}'(S)$. Also $\emptyset \notin Q$. Observe that $Q$ is an order ideal since if $Y \supseteq X$ and $X \cap P \neq \emptyset$, then $Y \cap P \neq \emptyset$. Suppose $w\tau \in Q$ and $w = a_0 \cdots a_n$ with $a_0, \ldots, a_n \in A$. Then, by definition of $\tau$ and $Q$, there exist $b_0, \ldots, b_n \in B$ such that $b_j\varphi = a_j$ for all $j$ and $b_0\psi \cdots b_n\psi \in P$. But then $b_0 \cdots b_n \in L$ and $(b_0 \cdots b_n)\varphi = a_0 \cdots a_n$, so $w \in L\varphi$.

Conversely, suppose $w \in L\varphi$. Let $w = v\varphi$ with $v \in L$. By definition of $\tau$, $v\psi \in w\tau$. But $v\psi \in P$, so $w\tau \in Q$ whence $w \in Q\tau^{-1}$. □

The proof idea for the next theorem is borrowed from [5].

**Theorem 5.2.** *Let $\mathbf{V}$ be a pseudovariety of semigroups such that, for some prime $p$, $\mathbf{LG}_p \textcircled{m} \mathbf{V} = \mathbf{V}$. Then*

$$\mathbf{LJ}^+ \textcircled{m} \mathbf{V} \subseteq \mathbf{P}'\mathbf{V}^+ \text{ whence}$$
$$BPol(\mathbf{V}) \subseteq \mathbf{PV}.$$

*Proof.* The second inequality follows immediately from the first. To prove the first, since

$$\mathbf{N} \subseteq \mathbf{LG}_p \subseteq \mathbf{V},$$

it suffices, by Lemma 3.2, to consider a monomial over $\mathbf{V}$ in variables $A$ of the form

$$L = L_0 a_1 \cdots a_n L_n$$

with $L_0, \ldots, L_n \in \mathbf{V}(A^+)$, $a_1, \ldots, a_n \in A$. Let $B = A \cup \overline{A}$ with $\overline{A}$ a disjoint copy of $A$. We define a literal morphism $\varphi : B^+ \to A^+$ such that $B\varphi = A$ by $a\varphi = a$ and $\overline{a}\varphi = a$, and show that $L$ is the image of an element of $\mathbf{V}(B^+)$. For each $j$, let $K_j = L_j\varphi^{-1}$. Then $K_j \in \mathbf{V}(B^+)$ for each $j$. Let

$$K = (K_0\overline{a_1} \cdots \overline{a_n}K_n)_{1,p}.$$

By Theorem 4.1, $K \in \mathbf{V}(B^+)$. We show $K\varphi = L$. Clearly $K\varphi \subseteq L$. For the converse, suppose $u \in L$. Then $u = w_0 a_1 \cdots a_n w_n$ with each $w_j \in L_j$. Consider $v = w_0\overline{a_1} \cdots w_{n-1}\overline{a_n}w_n$. Then, since the $w_j$ are in $A^+$, $v$ has exactly one factorization in $K_0\overline{a_1} \cdots \overline{a_n}K_n$, namely the one above; hence $v \in K$. But $v\varphi = u$, so $K\varphi = L$. Thus, by the above proposition, $L \in \mathbf{P}'\mathbf{V}^+(A^+)$. □

# 6 Semigroups which are Locally Groups

In this section, we characterize the operations we have been considering for pseudovarieties of semigroups which are locally groups.

**Proposition 6.1.** *Let* $\mathbf{V}_1, \mathbf{V}_2$ *be pseudovarieties of (ordered) semigroups. Then* $\mathbf{LV}_1 \circledcirc \mathbf{LV}_2 \subseteq \mathbf{L}(\mathbf{LV}_1 \circledcirc \mathbf{V}_2)$. *In particular, if* $\mathbf{V}_1$ *and* $\mathbf{V}_2$ *are pseudovarieties of groups,* $\mathbf{LV}_1 \circledcirc \mathbf{LV}_2 \subseteq \mathbf{L}(\mathbf{V}_1 * \mathbf{V}_2)$.

*Proof.* It suffices to show that given a semigroup homomorphism $\varphi : S \to T$ such that $T \in \mathbf{LV}_2$ and, for all idempotents $e \in T$, $e\varphi^{-1} \in \mathbf{LV}_1$, one has that $S \in \mathbf{L}(\mathbf{LV}_1 \circledcirc \mathbf{V}_2)$. Let $M \subseteq S$ be a submonoid; then $M\varphi \in \mathbf{V}_2$, being a monoid. If $f \in M\varphi$ is an idempotent, then $f\varphi^{-1} \in \mathbf{LV}_1$ whence $f\varphi^{-1} \cap M \in \mathbf{LV}_1$. Thus $M \in \mathbf{L}(\mathbf{LV}_1 \circledcirc \mathbf{V}_2)$.

Suppose now that $\mathbf{V}_1, \mathbf{V}_2$ are pseudovarieties of groups. Then if $M \subseteq S$ is a monoid with identity $e$, we see that $e\varphi\varphi^{-1} \in \mathbf{LV}_1$. Since $e\varphi\varphi^{-1}$ contains all the idempotents of $M$ ($M\varphi$ being a group), it follows that $M$ is a group which is an extension of a group in $\mathbf{V}_1$ by a group in $\mathbf{V}_2$ whence $M \in \mathbf{V}_1 * \mathbf{V}_2$ as desired. □

We then obtain from Theorem 5.2:

**Corollary 6.2.** *Let* $\mathbf{H}$ *be a pseudovariety of groups such that* $\mathbf{G}_p * \mathbf{H} = \mathbf{H}$ *for some prime* $p$. *Then*

$$\mathbf{LJ}^+ \circledcirc \mathbf{LH} \subseteq \mathbf{P}'(\mathbf{LH})^+ \text{ and}$$
$$BPol(\mathbf{LH}) \subseteq \mathbf{P}(\mathbf{LH}).$$

*Proof.* Proposition 6.1 shows that $\mathbf{LG}_p \circledcirc \mathbf{LH} = \mathbf{LH}$ whence Theorem 5.2 applies to prove the result. □

To prove the converse, we need the following characterization of finite completely simple semigroups.

**Lemma 6.3.** *A finite semigroup* $S$ *is completely simple if and only if* $S \in \mathbf{LG}$ *and* $S^2 = S$.

*Proof.* If $S$ is completely simple, then clearly $S^2 = S$; also it is well-known that any subsemigroup of a finite completely simple semigroup is completely simple, and that a completely simple monoid is a group.

The converse follows immediately from the Delay Theorem [15, 16], but we give an elementary proof here. Suppose that $S \in \mathbf{LG}$ and $S^2 = S$. We begin by showing that $S$ is completely regular. Consider the natural map

$\varphi : S^+ \to S$ which evaluates each letter as itself; let, for $s \in S$, $L_s = \{w \in S^+ | w\varphi = s\}$; $L_s$ is rational, being recognized by $S$. Observe that $S^2 = S$ implies $S^n = S$ for all $n > 0$ whence we can conclude that $L_s$ is infinite. The Pumping Lemma then applies to show that there exist $s_1, s_2, s_3 \in S$ such that $s = s_1 s_2^n s_3$ for all $n > 0$. Thus, by choosing $n$ carefully, we see that $s = s_1 e s_3$ with $e$ an idempotent. Then $s^{k+1} = s_1(es_3s_1e)^k s_3$ for $k > 0$. Since $S \in \mathbf{LG}$, it follows that for some $m > 0$, $(es_3s_1e)^m = e$ whence

$$s^{m+1} = s_1(es_3s_1e)^m s_3 = s_1 e s_3 = s.$$

Thus $S$ is completely regular (and so every element is $\mathcal{H}$-equivalent to an idempotent).

Thus, to finish our proof, it suffices to show that all idempotents of $S$ are $\mathcal{J}$-equivalent. Let $e, f \in S$ be idempotents. Then $(efe)^n = e$ for some $n > 0$ (since $s \in \mathbf{LG}$) so $e \in SfS$. Dually, $f \in SeS$ so $e \; \mathcal{J} \; f$. The result follows. $\square$

We now prove a theorem which implies the converse of Corollary 6.2.

**Theorem 6.4.** *Let* $\mathbf{V} \subseteq \mathbf{LG}$. *Then* $\mathbf{P'V}^+ \subseteq \mathbf{LJ}^+ ⓜ \mathbf{V}$. *Furthermore, if* $\mathbf{V}$ *contains a non-trivial monoid, then* $\mathbf{PV} \subseteq BPol(\mathbf{V})$.

*Proof.* The second statement follows from the first. It suffices to show that if $S \in \mathbf{V}$, then $(\mathcal{P}'(S), \supseteq) \in \mathbf{LJ}^+ ⓜ \mathbf{V}$. The identity map $\psi : \mathcal{P}'(S) \to \mathcal{P}'(S)$ gives rise to a relational morphism $\psi : \mathcal{P}'(S) \multimap S$; in fact, $X\psi Y\psi = XY = (XY)\psi$. Let $e \in S$ be an idempotent. Then

$$e\psi^{-1} = \{X \in \mathcal{P}'(S) | e \in X\}.$$

An idempotent of $e\psi^{-1}$ is then a subsemigroup $E \subseteq S$ with $e \in E$ and $E^2 = E$. Lemma 6.3 shows that $E$ is completely simple, so $EeE = E$. It follows that if $Y \in e\psi^{-1}$, then $EYE \supseteq EeE = E$ whence the local monoid with identity $E$ has $E$ as its greatest element; we conclude that $e\psi^{-1} \in \mathbf{LJ}^+$. $\square$

Since $\mathbf{LH}$ contains a non-trivial monoid, we immediately obtain the following theorem which is one of our main results.

**Theorem 6.5.** *Let* $\mathbf{H}$ *be a pseudovariety of groups such that* $\mathbf{G}_p * \mathbf{H} = \mathbf{H}$ *for some prime* $p$. *Then* $Pol(\mathbf{H}) = \mathbf{P'}(\mathbf{LH})^+$ *and* $BPol(\mathbf{LH}) = \mathbf{P}(\mathbf{LH})$. *In particular, these results hold for* $\mathbf{H}$ *any of* $\mathbf{G}$, $\mathbf{G}_p$ *(p prime), or* $\mathbf{G}_{sol}$.

## 7 Locally Block Groups

A *block group* is a semigroup whose regular elements have unique inverses (or, equivalently, semigroups which do not have a right or left zero subsemigroup). The pseudovariety of such is denote $\mathbf{BG}$. We use $\mathbf{D}$ for the pseudovariety of semigroups whose idempotents are right zeros.

We now recall some important facts whose consequences we shall use without comment:

1. $\mathbf{PG} = \mathbf{J} * \mathbf{G} = \mathbf{BG} = \mathbf{EJ}$ [4];
2. $\mathbf{L}(\mathbf{EJ}) = \mathbf{EJ} * \mathbf{D}$ [12, Proposition 10.2], [16, The Delay Theorem];
3. $\mathbf{LG} = \mathbf{G} * \mathbf{D}$ [15, 16];
4. If $\mathbf{H}$ is a pseudovariety of groups, then $BPol(\mathbf{H}) = \mathbf{J} * \mathbf{H}$ [9, 14];
5. For any pseudovariety of semigroups $\mathbf{V}$, $\mathbf{J} * \mathbf{V}$ is generated by semidirect products $M * N$ with $M \in \mathbf{J}^+$ and $N \in \mathbf{V}$ [14];
6. If $M$ is a monoid in $\mathbf{J}^+$, then $M \in \mathbf{LJ}^+$.

**Proposition 7.1.** *Let* $\mathbf{H}$ *be a pseudovariety of groups. Then*

$$\mathbf{P}'(\mathbf{LH})^+ \subseteq Pol(\mathbf{LH}) \subseteq \mathbf{L}(Pol(\mathbf{H}));$$
$$\mathbf{P}(\mathbf{LH}) \subseteq BPol(\mathbf{LH}) \subseteq \mathbf{L}(BPol(\mathbf{H})).$$

*Proof.* The first containment of the first statement follows from Theorem 6.4. The second containment follows from Proposition 6.1 which shows that

$$Pol(\mathbf{LH}) = \mathbf{LJ}^+ \circledm \mathbf{LH} \subseteq \mathbf{L}(\mathbf{LJ}^+ \circledm \mathbf{H}) = \mathbf{L}(Pol(\mathbf{H})).$$

The second statement follows from the first. $\square$

The following lemma will be of use.

**Lemma 7.2.** *Let* $\varphi : S * T \to T$ *be a semidirect product projection from a semidirect product of (ordered) semigroups, and let* $e \in T$ *be an idempotent. Then any submonoid of* $e\varphi^{-1}$ *(order) embeds in* $S$.

*Proof.* We shall use additive notation for the binary operation in $S$ though we do not assume commutativity. Define a map $\psi : e\varphi^{-1} \to S$ by $(s, e) \mapsto es$. Then

$$((s_1, e)(s_2, e))\psi = (s_1 + es_2, e)\psi = es_1 + es_2 = (s_1, e)\psi + (s_2, e)\psi$$

so $\psi$ is a homomorphism. By the definition of an action [11], $\psi$ preserves order. We show that $\psi$ is an (order) embedding when restricted to submonoids of $e\varphi^{-1}$. Let $M \subseteq e\varphi^{-1}$ be a submonoid with identity $(f, e)$. Then, for $(s, e) \in M$,

$$(s, e) = (f, e)(s, e) = (f + es, e) = (f + (s, e)\psi, e)$$

whence $\psi$ is an (order) embedding. $\square$

Using our collection of facts and the above lemma, one deduces immediately

**Corollary 7.3.** *Let* $\mathbf{V}$ *be a pseudovariety of semigroups. Then*

$$\mathbf{J}^+ * \mathbf{V} \subseteq \mathbf{LJ}^+ \textcircled{m}\, \mathbf{V} = Pol(\mathbf{V});$$
$$\mathbf{J} * \mathbf{V} \subseteq BPol(\mathbf{V}).$$

We now show that for the case of $\mathbf{G}$, all the pseudovarieties in question are the same.

**Theorem 7.4.** $\mathbf{P}(\mathbf{LG}) = \mathbf{L}(\mathbf{PG}) = \mathbf{L}(\mathbf{BG})$

*Proof.* Proposition 7.1 shows that $\mathbf{P}(\mathbf{LG}) \subseteq \mathbf{L}(\mathbf{PG})$ (here we are using that $\mathbf{PG} = \mathbf{J} * \mathbf{G} = BPol(\mathbf{G})$). For the other direction, using that $\mathbf{PG} = \mathbf{EJ}$, we see that

$$\mathbf{L}(\mathbf{PG}) = \mathbf{EJ} * \mathbf{D} = \mathbf{J} * \mathbf{G} * \mathbf{D} = \mathbf{J} * \mathbf{LG}.$$

But, by Corollary 7.3,

$$\mathbf{J} * \mathbf{LG} \subseteq BPol(\mathbf{LG}).$$

However, by Theorem 6.5, the righthand side is none other than $\mathbf{P}(\mathbf{LG})$. The result follows. $\square$

It is clear that one can verify if a semigroup is locally a block group in polynomial time whence $\mathbf{P}(\mathbf{LG}) = BPol(\mathbf{LG})$ has polynomial time membership problem. Observe that we have also shown that $\mathbf{L}(\mathbf{BG}) = \mathbf{J} * \mathbf{LG}$. We note that an entirely similar argument would show that $\mathbf{P}'(\mathbf{LG})^+ = Pol(\mathbf{LG}) = \mathbf{L}(\mathbf{P}'\mathbf{G}^+)$ if one could show that $\mathbf{EJ}^+$ is local (the argument of [12, Proposition 10.2] fails because $(B_2^1)^+ \notin \mathbf{EJ}^+$).

# References


[1] J. Almeida, Finite Semigroups and Universal Algebra, World Scientific, 1994.

[2] J. A. Brzozowski, *Hierarchies of aperiodic languages*, RAIRO Inform. Théor. **10** (1976), 33-49.

[3] S. Eilenberg, Automata, Languages and Machines, Academic Press, New York, Vol A, 1974: Vol B, 1976.

[4] K. Henckell, S. Margolis, J. -E. Pin, and J. Rhodes, *Ash's type II theorem, profinite topology and Malcev products. Part I*, Int. J. Algebra and Computation **1** (1991), 411-436.

[5] S. W. Margolis and J.-E. Pin, *Varieties of finite monoids and topology for the free monoid*, in "Proceedings of the 1984 Marquette Conference on Semigroups" (K. Byleen, P. Jones and F. Pastijn eds.), Marquette University (1984), 113-130.

[6] S. W. Margolis and J.-E. Pin, *Product of group languages*, *Proc. FCT Conf.*, Lecture Notes in Computer Science, Vol 199 (Springer, Berlin, 1985), 285-299.

[7] J.-E. Pin, *Eilenberg's theorem for positive varieties of languages*, Russian Maths. (Iz. VUZ) **39** (1995), 74-83.

[8] J.-E. Pin, *Syntactic semigroups*, Chap. 10 in Handbook of language theory, Vol. I, G. Rozenberg and A. Salomaa (ed.), Springer Verlag, 1997, 679–746.

[9] J.-E. Pin, *Bridges for concatenation hierarchies*, in 25th ICALP, Berlin, 1998, pp. 431–442, Lecture Notes in Computer Science 1443, Springer Verlag.

[10] J.-E. Pin and P. Weil, *Polynomial closure and unambiguous product*, Theory Comput. Systems **30** (1997), 1-39.

[11] J.-E. Pin and P. Weil, *Semidirect product of ordered semigroups*, preprint 2000.

[12] B. Steinberg, *Semidirect products of categories and applications*, J. Pure Appl. Algebra **142** (1999), 153-182.

[13] B. Steinberg, *A note on the equation* $\mathbf{PH} = \mathbf{J} * \mathbf{H}$, Semigroup Forum, to appear.

[14] B. Steinberg, *Polynomial closure and topology*, Internat. J. Algebra and Computation, to appear.

[15] H. Straubing, *Finite semigroup varieties of the form* $\mathbf{V} * \mathbf{D}$, J. Pure Appl. Algebra **36** (1985), 53-94.

[16] B. Tilson, *Categories as algebra*, J. Pure and Applied Algebra **48** (1987) 83-198.

[17] P. Weil, *Closure of varieties of languages under products with counter*, J. Comput. System Sci. **45** (1992), 316-339.