Power Semigroups and Polynomial Closure

Stuart W. Margolis  Benjamin Steinberg
Department of Computer Science  Faculdade de Ciências
Bar Ilan University  da Universidade do Porto
52900 Ramat Gan, Israel  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 $\mathbf{P} \langle \mathbf{LG} \rangle = \mathbf{L} \langle \mathbf{PG} \rangle$ (using that $\mathbf{PG} = \mathbf{BG}$). We also will show that this pseudovariety 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 $\mathbf{P} \langle \mathbf{LH} \rangle$. 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 de Matemática da Universidade do Porto.
Pin and Margolis [6] also studied the group hierarchy which takes as its base
the \( s \)-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 poly-
nomial 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 pseudo-
varieties 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 \( BPol(\mathbf{LH}) = P(\mathbf{LH}) \) and its ordered
analog (provided, of course, \( \mathbf{H} = \mathbf{G}_p \ast \mathbf{H} \) 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 \( P(\mathbf{LG}) \) as
\( L(\mathbf{PG}) \), 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 $J^+ = [x \leq 1]$ (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 non-empty 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 $V$ is a pseudovariety of semigroups, we use $PV$ to denote the pseudovariety generated by semigroups of the form $\mathcal{P}(S)$ with $S \in V$, and $P^V$ to denote the pseudovarieties generated by ordered semigroups of the form $(\mathcal{P}'(S), \supseteq)$ with $S \in V$. Suppose that $V$ contains a non-trivial monoid $M$; then $\{1\} \subseteq \mathcal{P}'(M)$ is isomorphic to $U_1$. It now follows from the previous paragraph that if $V$ contains a non-trivial monoid, then $PV$ is generated, as a pseudovariety of semigroups, by $P^V$.

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

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

A relational morphism of (ordered) semigroups $\mu : S \rightarrow T$ is a function $\mu : S \rightarrow \mathcal{P}'(T)$ such that $s_1 \mu s_2 \mu \subseteq \mu^s_1 \mu s_2$ 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 $V$, $W$ are pseudovarieties of (ordered) semigroups, then the Mal’cev product $V \otimes W$ consists of all (ordered) semigroups $S$ with a relational morphism $\varphi : S \rightarrow W \in W$ such that $e \varphi^{-1} \in V$ for each idempotent $e$ of $W$. One can show that $V \otimes W$ is generated by (ordered) semigroups $S$ with a homomorphism $\varphi : S \rightarrow W \in W$ such that $e \varphi^{-1} \in V$ for each idempotent $e$.
of $W$.

If $V_1$ and $V_2$ are pseudovarieties of (ordered) semigroups, then $V_1 * V_2$ denotes the pseudovariety generated by semidirect products of (ordered) semigroups in $V_1$ with those in $V_2$. The semidirect product is an associative operations on pseudovarieties; see [1, 3, 14, 11] for more details. If $V_1$ and $V_2$ are pseudovarieties of groups, $V_1 * V_2$ can be shown to consist of all groups which are an extension of a group in $V_1$ by a group in $V_2$.

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

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

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 $V$ such that:

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

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

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

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

If $V$ is a pseudovariety of semigroups and $A$ an alphabet, then a monomial over $V$ in variables $A$ is an expression

$$u_0L_1u_1 \cdots u_{n-1}L_nu_n$$

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

The class

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

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

- $V_0 = V$
- $V_{n+\frac{1}{2}} = Pol(V_n)$
- $V_{n+1} = BPol(V_n)$.

The dot depth hierarchy [2] comes from letting $V_0$ be the trivial pseudovariety.

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

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

We end this section with a technical lemma.

**Lemma 3.2.** Let $V$ be a pseudovariety of semigroups containing $N$. Then every polynomial in $V$ over $A$ can be written as a finite union of monomials of the form $L_0a_1 \cdots a_nL_n$ with the $a_i \in A$ and the $L_i \in V(A^*)$.

**Proof.** The hypotheses are equivalent to assuming $V$ contains all finite languages. It suffices to show that any monomial $M = u_0K_1u_1 \cdots u_{n-1}K_nu_n$ with the $u_i \in A^*$ and $K_i \in V(A^*)$ 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

$$M = (u_0uw_1)K_2 \cdots u_{n-1}K_nu_n \cup u_0(K_1 \setminus \{ w \})u_1K_2 \cdots u_{n-1}K_nu_n. \quad (1)$$
Since $V(A^+)$ contains all finite languages, it follows that $K_1 \setminus \{w\} \in V(A^+)$. 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 $(u^{-1}K_1v^{-1}) \subseteq V(A^+)$ 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

$$M = \bigcup_{u,v \in A^2} (u_0u)(u_0^{-1}K_1v^{-1})(vu_1)\cdots u_{n-1}K_nu_n.$$ 

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 $M' = wK_2u_2\cdots u_{n-1}K_nu_n$ 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. \qed

4 Counters

Suppose that we have $a_1, \ldots, a_n \in A$, and $L_0, \ldots, L_n \subseteq A^+$. Then, for $0 \leq r < m$, 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 $L_0, \ldots, L_n \in V(A^+)$ implies that $(L_0a_1 \cdots a_nL_n)_{r,m} \in V(A^+)$. The following result is due to Weil [17].

**Theorem 4.1.** Let $V$ be a pseudovariety of semigroups. Then $V$ is closed under products with $p$-counters, $p$ a prime, if and only if $V = LG_p \otimes V$.

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 $L \in \operatorname{Rec}(B^+)$ be recognized by a semigroup $S$, with $L = P\psi^{-1}$, and \( \varphi : B^+ \rightarrow A^+ \) 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 $\psi : B^+ \rightarrow S$ be a morphism and $P \subseteq S$ with $L = P\psi^{-1}$. We define a morphism $\tau : A^+ \rightarrow (\mathcal{P}(S), \supseteq)$ by $a\tau = \{ b\varphi | b \in B, b\varphi = a \}$ 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 $V$ be a pseudovariety of semigroups such that, for some prime $p$, $LG_p \bar{\otimes} V = V$. Then

$$LJ^+ \bar{\otimes} V \subseteq \mathcal{P}V^+$$

whence

$$BPol(V) \subseteq PV.$$

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

$$N \subseteq LG_p \subseteq V,$$

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

$L = L_0a_1 \cdots a_nL_n$

with $L_0, \ldots, L_n \in V(A^+)$, $a_1, \ldots, a_n \in A$. Let $B = A \cup \overline{A}$ with $\overline{A}$ a disjoint copy of $A$. We define a literal morphism $\varphi : B^+ \rightarrow A^+$ 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 $V(B^+)$. For each $j$, let $K_j = L_j\varphi^{-1}$. Then $K_j \in V(B^+)$ for each $j$. Let

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

By Theorem 4.1, $K \in V(B^+)$. We show $K\varphi = L$. Clearly $K\varphi \subseteq L$. For the converse, suppose $u \in L$. Then $u = w_0a_1 \cdots a_nw_n$ 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, $L \in \mathcal{P}V^+(A^+)$.  

7
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 $V_1, V_2$ be pseudovarieties of (ordered) semigroups. Then $LV_1 \ominus LV_2 \subseteq L(LV_1 \ominus V_2)$. In particular, if $V_1$ and $V_2$ are pseudovarieties of groups, $LV_1 \ominus LV_2 \subseteq L(V_1 * V_2)$.

*Proof.* It suffices to show that given a semigroup homomorphism $\varphi : S \to T$ such that $T \in LV_2$ and, for all idempotents $e \in T$, $e\varphi^{-1} \in LV_1$, one has that $S \in L(LV_1 \ominus V_2)$. Let $M \subseteq S$ be a submonoid; then $M\varphi \in V_2$, being a monoid. If $f \in M\varphi$ is an idempotent, then $f\varphi^{-1} \in LV_1$ whence $f\varphi^{-1} \cap M \in LV_1$. Thus $M \in L(LV_1 \ominus V_2)$.

Suppose now that $V_1, V_2$ are pseudovarieties of groups. Then if $M \subseteq S$ is a monoid with identity $e$, we see that $e\varphi\varphi^{-1} \in LV_1$. 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 $V_1$ by a group in $V_2$ whence $M \in V_1*V_2$ as desired. \qed

We then obtain from Theorem 5.2:

**Corollary 6.2.** Let $H$ be a pseudovariety of groups such that $G_p * H = H$ for some prime $p$. Then

$$LJ^+ \ominus LH \subseteq P'(LH)^+ \text{ and }$$

$$BPoL(LH) \subseteq P(LH).$$

*Proof.* Proposition 6.1 shows that $LG_p \ominus LH = LH$ whence Theorem 5.2 applies to prove the result. \qed

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 $S \in LG$ 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 $S \in LG$ 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 \( s = s_1s_2s_3 \) for all \( n > 0 \). Thus, by choosing \( n \) carefully, we see that \( s = s_1e_3 \) with \( e \) an idempotent. Then \( s^{k+1} = s_1(s_3s_1e)^k s_3 \) for \( k > 0 \).

Since \( S \in \mathbf{LG} \), it follows that for some \( m > 0 \), \( (s_3s_1e)^m = e \) whence

\[
s^{m+1} = s_1(s_3s_1e)^m s_3 = s_1es_3 = s.
\]

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 \( (ef)^n = e \) for some \( n > 0 \) (since \( s \in \mathbf{LG} \)) so \( e \in SfS \). Dually, \( f \in SeS \) so \( e \in \mathcal{J}f \). The result follows.

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

**Theorem 6.4.** Let \( V \subseteq \mathbf{LG} \). Then \( P^+V^+ \subseteq LJ^+ \otimes V \). Furthermore, if \( V \) contains a non-trivial monoid, then \( PV \subseteq BPo1(V) \).

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

\[
ev^{-1} = \{ X \in \mathcal{P}'(S) | e \in X \}.
\]

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 \( e\psi^{-1} \in \mathbf{LJ}^+ \).

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 \( H \) be a pseudovariety of groups such that \( G_p \ast H = H \) for some prime \( p \). Then \( Po1(H) = \mathcal{P}'(\mathbf{LH})^+ \) and \( BPo1(\mathbf{LH}) = \mathcal{P}(\mathbf{LH}) \). In particular, these results hold for \( H \) any of \( G \), \( G_p \) (\( p \) prime), or \( G_{sol} \).
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 sub-semigroup). The pseudovariety of such is denote $BG$. We use $D$ for the pseudovariety of semigroups whose idempotents are right zeros.

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

1. $PG = J * G = BG = EJ$ [4];

2. $L(EJ) = EJ * D$ [12, Proposition 10.2], [16, The Delay Theorem];

3. $LG = G * D$ [15, 16];

4. If $H$ is a pseudovariety of groups, then $BPol(H) = J * H$ [9, 14];

5. For any pseudovariety of semigroups $V$, $J * V$ is generated by semidirect products $M * N$ with $M \in J^+$ and $N \in V$ [14];

6. If $M$ is a monoid in $J^+$, then $M \in LJ^+$.

**Proposition 7.1.** Let $H$ be a pseudovariety of groups. Then

$$P'(LH)^+ \subseteq Pol(LH) \subseteq L(Pol(H));$$

$$P(LH) \subseteq BPol(LH) \subseteq L(BPol(H)).$$

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

$$Pol(LH) = LJ^+ \oplus LH \subseteq L(LJ^+ \oplus H) = L(Pd(H)).$$

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 sub-
monoids 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 imme-
diately

**Corollary 7.3.** Let $V$ be a pseudovariety of semigroups. Then
\[
J^+ * V \subseteq LJ^+ \circ \circ V = Pd(V);
\]
\[
J * V \subseteq BPd(V).
\]

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

**Theorem 7.4.** $P(LG) = L(PG) = L(BG)$

*Proof.* Proposition 7.1 shows that $P(LG) \subseteq L(PG)$ (here we are using that
$PG = J * G = BPol(G)$). For the other direction, using that $PG = EJ$,
we see that
\[
L(PG) = EJ * D = J * G * D = J * LG.
\]
But, by Corollary 7.3,
\[
J * LG \subseteq BPd(LG).
\]
However, by Theorem 6.5, the righthand side is none other than $P(LG)$.
The result follows. \(\square\)

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