$BG = PG$: A SUCCESS STORY

Jean-Eric Pin*

August 14, 2004

1 Introduction

All semigroups and monoids except free monoids and free groups are assumed finite in this paper. A monoid M *divides* a monoid N if M is a quotient of a submonoid of N. The set of idempotents of a monoid M is denoted $E(M)$. The word "variety" will be used for pseudo-variety — that is, a collection of finite monoids closed under division and finite direct product.

A block group is a monoid such that every $\mathcal{R}$-class (resp. $\mathcal{L}$-class) contains at most one idempotent. Block groups form a variety of monoids, denoted $\mathbf{BG}$, which is the topic of this paper. More precisely, we want to make some comments on the following cryptic line, which states that six apparently distinct varieties of monoids are in fact all equal:

$$\Diamond\mathbf{G} = \mathbf{PG} = \mathbf{J} * \mathbf{G} = \mathbf{J} ⓜ \mathbf{G} = \mathbf{BG} = \mathbf{EJ}$$

As $\mathbf{BG}$ was already introduced, let us now briefly present the other five actors. More detailed definitions will be given in the forthcoming sections. The variety $\Diamond\mathbf{G}$ is the variety generated by Schützenberger products of groups, $\mathbf{PG}$ is the variety generated by power groups, $\mathbf{J} * \mathbf{G}$ is the variety generated by semidirect products of a $\mathcal{J}$-trivial monoid by a group, $\mathbf{J} ⓜ \mathbf{G}$ is the variety generated by Malcev products of a $\mathcal{J}$-trivial monoid by a group and finally $\mathbf{EJ}$ is the variety of monoids M such that $E(M)$ generates a $\mathcal{J}$-trivial monoid.

All but one of these equalities were obtained by Margolis and the author around 1984 [16, 17], but the last missing inclusion $\mathbf{J} ⓜ \mathbf{G} \subset \mathbf{J} * \mathbf{G}$ resisted for seven years. During these seven years, several fundamental results were obtained on the Malcev product and the semidirect product and in particular on the varieties of the form $\mathbf{V} * \mathbf{G}$ or $\mathbf{V} ⓜ \mathbf{G}$. On the positive side, it was shown that the equality $\mathbf{V} * \mathbf{G} = \mathbf{V} ⓜ \mathbf{G}$ holds when the variety $\mathbf{V}$ is *local* in the sense of categories [39, 15]. On the negative side, it was observed that in general, $\mathbf{V} * \mathbf{G}$ is a proper subvariety of $\mathbf{V} ⓜ \mathbf{G}$. The case of the variety $\mathbf{V} = \mathbf{J}$ seemed to be a real difficult problem. On the one hand, a deep result of Knast [13] showed that the variety $\mathbf{J}$ was not local and this led Margolis and the author to believe that the inclusion $\mathbf{J} ⓜ \mathbf{G} \subset \mathbf{J} * \mathbf{G}$ might be proper. On the other hand, if the inclusion had been proper, power groups would have satisfied other (pseudo)identities than the ones of $\mathbf{BG}$.

As it happens often with difficult problems, the solution came from a more general result, namely Ash's proof of Rhodes "cover conjecture" [3, 4]. An account of the discovery and the consequences of this result is given in [11]. The final solution

*From 1st Sept 1993, LITP, Université Paris VI, Tour 55-65, 4 Place Jussieu, 75252 Paris Cedex 05, FRANCE. **E-mail:** pin@liafa.jussieu.fr

given by Henckell and Rhodes [10, 11] combines Ash's theorem, derived categories and Knast's result with a subtle computation on weak inverses.

The article is organized as follows. After a very short section of general definitions, block groups are defined in Section 3 and power groups in Section 4. The Schützenberger product is introduced in Section 5 and the part of the proof that makes use of language theory is presented in Section 6. Section 7 is devoted to Malcev products and contains a short outline of the proof of Henckell and Rhodes. A consequence of the equality $\mathbf{BG} = \mathbf{PG}$ on ordered monoids is discussed in Section 8 and connections with topology are briefly mentioned in Section 9.

2 General definitions

We refer the reader to [5, 6, 12, 14, 22] for additional background material. Given a subset P of a monoid M, $\langle P \rangle$ denotes the submonoid of M generated by P. The exponent of a semigroup S, that is, the smallest integer n such that s^n is idempotent for all $s \in S$, is usually denoted ω. The wreath product of two monoids M and N is denoted $M \circ N$. Finally, $|X|$ denotes the number of elements of a finite set X.

3 Block groups

The term "block" refers to a little known result of R. L. Graham [7] on 0-simple semigroups.

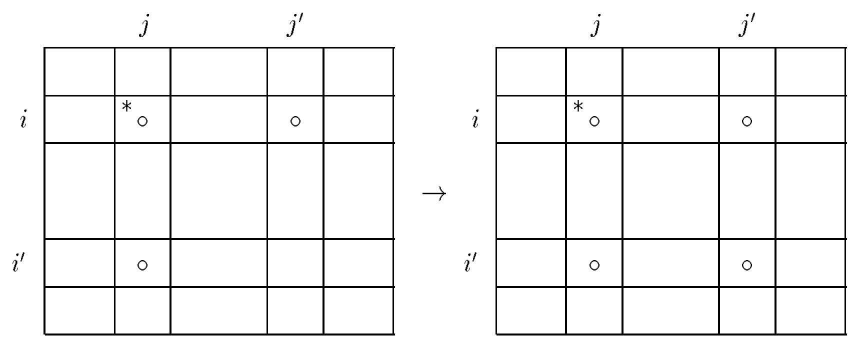
Theorem 3.1 *Let S^0 be a 0-simple semigroup and let T be the subsemigroup of S^0 generated by the union of all maximal groups of S. Then the regular $\mathcal{D}$-classes B_1, ..., B_n of T have the following properties:*

(1) *each B_i is generated by the union of its maximal subgroups,*

(2) *for all $i \neq j$, $B_i B_j = B_j B_i = 0$,*

(3) *for all $s \in S \setminus \bigcup_{1 \leq i \leq n} B_i$, $s^2 = 0$.*

The B_i's are called the *blocks* of S^0. It is easy to compute the blocks given the egg-box picture of S. You are given two different kind of tokens, stars and circles. First put a star and a circle in each $\mathcal{H}$-class which is a group (that is, containing an idempotent). Next, play the following game, as long as you can: each time there is a star in $H_{i,j}$ and circles in $H_{i,j'}$ and $H_{i',j}$, add a circle in $H_{i',j'}$.



When the game is over, one gets the block structure of S.

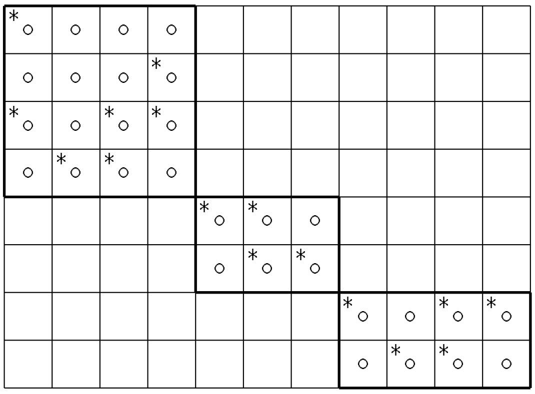


Figure 3.1: The block structure of a 0-simple semigroup.

Let D be a regular $\mathcal{D}$-class of a semigroup S. Then it is well-known that $D^0 = D \cup \{0\}$ is a 0-simple semigroup. Thus, one may define the *blocks of the $\mathcal{D}$-class D* as the blocks of D^0. A *block group* is a monoid in which the blocks of every regular $\mathcal{D}$-class are groups. In this case, every element has at most one semigroup inverse and every regular $\mathcal{D}$-class can be represented as follows.

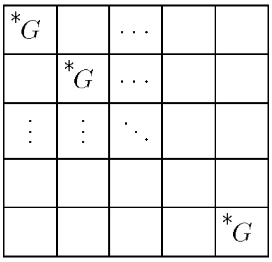


Figure 3.2: A regular $\mathcal{D}$-class of a block group.

Note that a regular monoid is a block group if and only if it is inverse. It follows that M is a block-group if and only if every $\mathcal{R}$-class and every $\mathcal{L}$-class has at most one idempotent. The following theorem of [16] summarizes some equivalent formulations.

Theorem 3.2 *Let M be a monoid. The following conditions are equivalent*

(1) *M is a block group,*

(2) *For every regular $\mathcal{D}$-class D of M, D^0 is a Brandt semigroup,*

(3) *For all $e, f \in E(M)$, $e \mathrel{\mathcal{R}} f$ implies $e = f$ and $e \mathrel{\mathcal{L}} f$ implies $e = f$,*

(4) *For all $e, f \in E(M)$, $efe = e$ implies $ef = e = fe$.*

One can also convert these conditions into equations as follows [16]. Recall that x^ω can be interpreted as the unique idempotent of the subsemigroup of M generated by x.

Theorem 3.3 *Let M be a monoid. The following conditions are equivalent*

(1) *M is a block group,*

(2) *For all $x, y \in M$, $(x^\omega y)^\omega = (yx^\omega)^\omega$,*

(3) *For all $x, y \in M$, $(x^\omega y^\omega)^\omega = (y^\omega x^\omega)^\omega$,*

(4) *For all $x, y \in M$, $(x^\omega y^\omega)^\omega x^\omega = (x^\omega y^\omega)^\omega = y^\omega (y^\omega x^\omega)^\omega$,*

(5) *The submonoid $\langle E(M)\rangle$ is $\mathcal{J}$-trivial.*

The most difficult part of this theorem is (1) implies (5). One first shows by induction on n that if M is a block group and $e_1, \dots, e_n$ are idempotents of M, then, for $0 \le i \le n$, $(e_1 \cdots e_n)^\omega = (e_1 \cdots e_n)^\omega e_1 \cdots e_i$. This shows that $\langle E(M)\rangle$ is $\mathcal{R}$-trivial and a symmetrical proof shows that $\langle E(M)\rangle$ is $\mathcal{L}$-trivial.

It is easy to see that the collection **BG** of all block groups is a variety. If one denotes by **EJ** the variety of monoids M such that $E(M)$ generates a $\mathcal{J}$-trivial monoid, we obtain our first equality:

Proposition 3.4 $\mathbf{BG} = \mathbf{EJ}$.

4 Power groups

Given a monoid M, denote by $\mathcal{P}(M)$ (resp. $\mathcal{P}'(M)$) the monoid of subsets (resp. non empty subsets) of M under the multiplication of subsets, defined, for all $X, Y \subset M$ by $XY = \{xy \mid x \in X \text{ and } y \in Y\}$. For instance, if G is the trivial monoid, then $\mathcal{P}(M)$ is equal to the monoid $U_1 = \{1, 0\}$ with multiplication given by the rules $1.1 = 1$ and $1.0 = 0.1 = 0$. If M is the cyclic group of order 3, $\mathbb{Z}/3\mathbb{Z} = \{0, 1, -1\}$, then $\mathcal{P}'(M)$ has the following structure:

$$\boxed{{}^*\{1\}, \{0\}, \{-1\}}$$

$$\boxed{{}^*\{1,0\}, \{0,-1\}, \{1,-1\}}$$

$$\boxed{{}^*\{1,0,-1\}}$$

Figure 4.1: The $\mathcal{D}$-classes of $\mathcal{P}'(\mathbb{Z}/3\mathbb{Z})$.

The monoids $\mathcal{P}(M)$ and $\mathcal{P}'(M)$ are related as follows

Proposition 4.1 *For every monoid M, $\mathcal{P}'(M)$ is a submonoid of $\mathcal{P}(M)$ and $\mathcal{P}(M)$ divides $\mathcal{P}'(M) \times U_1$.*

The following results summarize the local structure of $\mathcal{P}'(M)$ when M is a group [20, 16].

Proposition 4.2 *Let G be a group and let $X, Y \in \mathcal{P}'(G)$. Then*

(1) *the idempotents of $\mathcal{P}'(G)$ are the subgroups of G,*

(2) *$X \;\mathcal{R}\; Y$ (resp. $X \;\mathcal{L}\; Y$) if and only if there exists $g \in G$ such that $Xg = Y$ (resp. $gX = Y$),*

(3) *$X \;\mathcal{D}\; Y$ if and only if there exist $g_1, g_2 \in G$ such that $g_1 X g_2 = Y$. In particular, if $X \;\mathcal{D}\; Y$, then $|X| = |Y|$.*

Corollary 4.3 *Let G be a group and let H and K be two subgroups of G.*

(1) *H and K are $\mathcal{D}$-equivalent in $\mathcal{P}'(G)$ if and only if they are conjugate,*

(2) *Let D be the $\mathcal{D}$-class of $\mathcal{P}'(G)$ containing H. Then D^0 is a Brandt semigroup of size $|G : N(H)|$ with structure group $N(H)/H$, where $N(H)$ is the normalizer of H.*

This last property shows that $\mathcal{P}'(G)$ is a block group [20].

Corollary 4.4 *If G is a group, then $\mathcal{P}'(G)$ and $\mathcal{P}(G)$ are block groups.*

Given a monoid M, denote by $\mathcal{P}_1(M)$ the submonoid of $\mathcal{P}(M)$ consisting of all subsets of M containing the identity.

Theorem 4.5 *For every monoid M, $\mathcal{P}_1(M)$ is a $\mathcal{J}$-trivial monoid.*

Proof. Let $X, Y \in \mathcal{P}_1(M)$. If $X \mathrel{\mathcal{J}} Y$, then $AXB = Y$ and $CYD = X$ for some $A, B, C, D \in \mathcal{P}_1(M)$. In particular, A, B, C and D contain 1 and thus $X = 1X1 \subset AXB = Y$ and $Y = 1Y1 \subset CYD = X$. Thus $X = Y$. □

For a group G, there is a nice connection between $\mathcal{P}_1(G)$ and $\mathcal{P}'(G)$.

Proposition 4.6 *If G is a group, then $\mathcal{P}'(G)$ is a quotient of a semidirect product of the form $\mathcal{P}_1(G) * G$.*

Proof. Let G act on the left on $\mathcal{P}_1(G)$ by conjugacy. That is, set $g \cdot X = gXg^{-1}$ for all $g \in G$ and $X \in \mathcal{P}_1(G)$. This defines a semidirect product of $\mathcal{P}_1(G)$ by G. Now, one verifies that the map $\pi : \mathcal{P}_1(G) * G \to \mathcal{P}'(G)$ defined by $\pi(X, g) = Xg$ is a surjective morphism. □

Given a variety of monoids $\mathbf{V}$ denote by $\mathbf{PV}$ the variety generated by all monoids of the form $\mathcal{P}(M)$, where $M \in \mathbf{V}$. Thus in particular $\mathbf{PG}$ is the variety generated by all power monoids of groups. By Corollary 4.4, this variety is contained in $\mathbf{BG}$. Denote by $\mathbf{J} * \mathbf{G}$ the variety generated by all semidirect products of a $\mathcal{J}$-trivial monoid by a group. Then $\mathbf{J} * \mathbf{G}$ contains U_1, since U_1 is $\mathcal{J}$-trivial, and by Theorem 4.5 and Proposition 4.6, it contains the monoids of the form $\mathcal{P}'(G)$, where G is a group. These results can be summarized as follows.

Proposition 4.7 *The following inclusions hold:* $\mathbf{PG} \subset \mathbf{J} * \mathbf{G}$ *and* $\mathbf{PG} \subset \mathbf{BG}$.

The author is not aware of any direct proof of the opposite inclusions. The inclusion $\mathbf{J} * \mathbf{G} \subset \mathbf{PG}$ is proved in Section 6 by arguments of language theory and a purely semigroup theoretic proof is still wanted.

5 Schützenberger product

We introduce in this section the variety $\Diamond\mathbf{G}$. Given a monoid M, $\mathcal{P}(M)$ is not only a monoid but also a semiring under union as addition and the product of subsets as multiplication.

Let $M_1, \ldots, M_n$ be monoids. Denote by M the product monoid $M_1 \times \cdots \times M_n$, k the semiring $\mathcal{P}(M)$ and by $M_n(k)$ the semiring of square matrices of size n with entries in k. The Schützenberger product of $M_1, \ldots, M_n$, denoted $\Diamond_n(M_1, \ldots, M_n)$ is the submonoid of the multiplicative monoid $M_n(k)$ composed of all the matrices P satisfying the three following conditions:

(1) If $i > j$, $P_{i,j} = 0$

(2) If $1 \leq i \leq n$, $P_{i,i} = \{(1, \ldots, 1, s_i, 1, \ldots, 1)\}$ for some $s_i \in S_i$

(3) If $1 \leq i \leq j \leq n$, $P_{i,j} \subset 1 \times \cdots \times 1 \times M_i \times \cdots \times M_j \times 1 \cdots \times 1$.

Condition (1) shows that the matrices of the Schützenberger product are upper triangular, condition (2) enables us to identify the diagonal coefficient $P_{i,i}$ with an element s_i of M_i and condition (3) shows that if $i < j$, $P_{i,j}$ can be identified with a subset of $M_i \times \cdots \times M_j$. With this convention, a matrix of $\Diamond_3(M_1, M_2, M_3)$ will have the form

$$\begin{pmatrix} s_1 & P_{1,2} & P_{1,3} \\ 0 & s_2 & P_{2,3} \\ 0 & 0 & s_3 \end{pmatrix}$$

with $s_i \in M_i$, $P_{1,2} \subset M_1 \times M_2$, $P_{1,3} \subset M_1 \times M_2 \times M_3$ and $P_{2,3} \subset M_2 \times M_3$.

Given a variety of monoids $\mathbf{V}$, $\diamondsuit\mathbf{V}$ denotes the variety of monoids generated by all Schützenberger products of the form $\diamondsuit_n(M_1, \ldots, M_n)$ with $n > 0$ and $M_1, \ldots, M_n \in \mathbf{V}$.

6 A tour of language theory

We present in this section a complete proof of the inclusions $\mathbf{J} * \mathbf{G} \subset \diamondsuit\mathbf{G}$ and $\diamondsuit\mathbf{G} \subset \mathbf{PG}$, first given in [16, 17]. The reader is referred to our article [28] in this volume for an introduction to language theory. The idea is the following: by Eilenberg's theorem, varieties of monoids are in one-to-one correspondence with varieties of languages, and thus it suffices to establish the inclusions $\mathcal{V}_1 \subset \mathcal{V}_2 \subset \mathcal{V}_3$, where $\mathcal{V}_1$, $\mathcal{V}_2$ and $\mathcal{V}_3$ denote respectively the varieties of languages corresponding to $\mathbf{J} * \mathbf{G}$, $\diamondsuit\mathbf{G}$ and $\mathbf{PG}$. We first describe the three varieties of languages $\mathcal{V}_1$, $\mathcal{V}_2$ and $\mathcal{V}_3$. Recall that a *group language* is a language recognized by a group.

Let us start with the variety $\mathcal{V}_2$. Given languages $L_0, L_1, \ldots, L_n$ of A^* and letters $a_1, a_2, \ldots, a_n$, the product of $L_0, \ldots L_n$ marked by $a_1, \ldots, a_n$ is the language $L_0 a_1 L_1 a_2 \cdots a_n L_n$. It is known (see [28], Theorem 12.3) that the Schützenberger product is the algebraic operation on monoids that corresponds to the marked product. The following theorem is a simple application of this general result.

Theorem 6.1 *For all alphabet A, $\mathcal{V}_2(A^*)$ is the boolean algebra generated by all the marked products of the form $L_0 a_1 L_1 \cdots a_n L_n$ where $L_0, \ldots, L_n$ are group languages of A^* and $a_1, \ldots, a_n \in A$.*

Next, there exists a description of the variety of languages corresponding to $\mathbf{PV}$, obtained independently by Reutenauer [32] and Straubing [36]. This result can be applied in particular to the variety $\mathbf{PG}$ as follows. A monoid morphism $\varphi : B^* \to A^*$ is *length preserving* if it maps each letter of B onto a letter of A.

Theorem 6.2 *The variety $\mathcal{V}_3$ is the smallest variety of languages $\mathcal{V}$ such that, for each alphabet A, $\mathcal{V}(A^*)$ contains the languages of the form $\varphi(L)$ where L is a group language of B^* and $\varphi : B^* \to A^*$ is a length preserving morphism.*

The variety $\mathcal{V}_1$ can be described by Straubing's "wreath product principle", which is a general construction to describe the languages recognized by the wreath product of two finite monoids. Let M be a monoid, G a group and let $\eta : A^* \to M \circ G$ be a monoid morphism. We denote by $\pi : M \circ G \to G$ the monoid morphism defined by $\pi(f, g) = g$ and we put $\varphi = \pi \circ \eta$. Thus φ is a monoid morphism from A^* into G. Let $B = G \times A$ and $\sigma : A^* \to B^*$ be the map (which is not a morphism!) defined by

$$\sigma(a_1 a_2 \cdots a_n) = (1, a_1)(\varphi(a_1), a_2) \cdots (\varphi(a_1 a_2 \cdots a_{n_1}), a_n)$$

Theorem 6.3 *If a language L is recognized by $\eta : A^* \to M \circ G$, then L is a finite boolean combination of languages of the form $X \cap \sigma^{-1}(Y)$, where $Y \subset B^*$ is recognized by M and where $X \subset A^*$ is recognized by G.*

We are now ready to prove the inclusions announced above.

Proposition 6.4 $\mathbf{J} * \mathbf{G}$ *is contained in* $\diamondsuit\mathbf{G}$.

Proof. Let $L \subset A^*$ be a language of $\mathcal{V}_1(A^*)$. Then L is recognized by a wreath product of the form $M \circ G$, where M is $\mathcal{J}$-trivial and G is a group. With the notations of Theorem 6.3, L is a finite boolean combination of languages of the form $X \cap \sigma^{-1}(Y)$, where $Y \subset B^*$ is recognized by M and $X \subset A^*$ is recognized by G. Since X is recognized by a group, $X \in \mathcal{V}_2(A^*)$. Thus it suffices to verify that $\sigma^{-1}(Y) \in \mathcal{V}_2(A^*)$. But since Y is recognized by a $\mathcal{J}$-trivial monoid, Simon's theorem (see [28, Section 7]) implies that Y is a boolean combination of languages of the form $B^*b_1B^*b_2B^* \cdots b_nB^*$, where the b_i's are letters of B. Now since σ^{-1} commutes with boolean operations, it remains to verify that the languages of the form $\sigma^{-1}(B^*b_1B^*b_2B^* \cdots b_nB^*)$ are in $\mathcal{V}_2(A^*)$. Set, for $1 \leq i \leq n$, $b_i = (g_i, a_i)$. Then we have

$$\begin{aligned}\sigma^{-1}(B^*b_1B^*b_2B^* \cdots b_nB^*) &= \{u \in A^* \mid \sigma(u) \in B^*b_1B^*b_2B^* \cdots b_nB^*\} \\ &= \{u_0a_1u_1 \cdots a_nu_n \mid b_1 = (\varphi(u_0), a_1),\ b_2 = (\varphi(u_0a_1u_1), a_2),\ \ldots, \\ &\qquad\qquad b_n = (\varphi(u_0a_1u_1 \cdots a_{n-1}u_{n-1}), a_n)\} \\ &= \{u_0a_1u_1 \cdots a_nu_n \mid \varphi(u_0) = g_1,\ \varphi(u_0a_1u_1) = g_2,\ \ldots, \\ &\qquad\qquad \varphi(u_0a_1u_1 \cdots a_{n-1}u_{n-1}) = g_n\}\end{aligned}$$

Setting $h_0 = g_1$, $h_1 = (g_1\varphi(a_1))^{-1}g_2$, $\ldots$, $h_{n-1} = (g_1\varphi(a_1)g_2 \cdots g_{n-1}\varphi(a_{n-1}))^{-1}g_n$, and $H_i = \varphi^{-1}(h_i)$ for $0 \leq i \leq n$, one gets finally

$$\begin{aligned}&\sigma^{-1}(B^*b_1B^*b_2B^* \cdots b_nB^*) \\ &\quad = \{u_0a_1u_1 \cdots a_nu_n \mid \varphi(u_0) = h_0,\ \varphi(u_1) = h_1,\ \ldots,\ \varphi(u_{n-1}) = h_{n-1}\} \\ &\quad = H_0a_1H_1a_2 \cdots H_{n-1}a_nA^*\end{aligned}$$

Since the H_i and A^* are group languages, it follows that $\sigma^{-1}(B^*b_1B^*b_2B^* \cdots b_nB^*)$ belongs to $\mathcal{V}_2(A^*)$. $\square$

Proposition 6.5 $\Diamond\mathbf{G}$ *is contained in* $\mathbf{PG}$.

Proof. It suffices to prove that every language of the form $L = L_0a_1L_1 \cdots a_nL_n$, where the a_i's are letters and the L_i's are group languages of A^*, can be written as $\varphi(L)$ where L is a group language of B^* and $\varphi : B^* \to A^*$ is a length preserving morphism. Let $\bar{A}$ be a copy of A and let $\varphi : (A \cup \bar{A})^* \to A^*$ be the length preserving morphism defined by $\varphi(a) = \varphi(\bar{a}) = a$ for every $a \in A$. Set, for $1 \leq i \leq n$, $K_i = \varphi^{-1}(L_i)$. Finally, fix a prime number p and let K be the set of all words $u \in (A \cup \bar{A})^*$ whose number of factorizations of the form $u_0\bar{a}_1u_1 \cdots \bar{a}_nu_n$ — where $u_0 \in K_0, \ldots, u_n \in K_n$ — is congruent to 1 modulo p. One can show [26] that K is a group language. We claim that $\varphi(K) = L$. Indeed K is contained in $K_0\bar{a}_1K_1 \cdots \bar{a}_nK_n$ by construction and thus $\varphi(K) \subset \varphi(K_0\bar{a}_1K_1 \cdots \bar{a}_nK_n) \subset L_0a_1L_1 \cdots a_nL_n = L$. Conversely, let $u \in L$. Then u admits a factorization of the form $u = u_0a_1u_1 \cdots a_nu_n$ where $u_0 \in K_0, \ldots, u_n \in K_n$. Let $v = u_0\bar{a}_1u_1 \cdots \bar{a}_nu_n$. Then $v \in K_0\bar{a}_1K_1 \cdots \bar{a}_nK_n$ and $\varphi(v) = u$. Furthermore, $u_0\bar{a}_1u_1 \cdots \bar{a}_nu_n$ is the unique factorization of v in $K_0\bar{a}_1K_1 \cdots \bar{a}_nK_n$ and thus $v \in K$. Therefore $L \subset \varphi(K)$ and thus L is equal to $\varphi(K)$, proving the claim and the theorem. $\square$

Let us summary the results obtained so far

Corollary 6.6 *The following formulæ hold:* $\mathbf{PG} = \mathbf{J} * \mathbf{G} = \Diamond\mathbf{G} \subset \mathbf{BG} = \mathbf{EJ}$.

7 Malcev products

Given a variety of semigroups $\mathbf{V}$, a monoid M is called a $\mathbf{V}$-*extension of a group* G if there exists a surjective morphism $\pi : M \to G$ such that $\pi^{-1}(1) \in \mathbf{V}$. Given a variety of monoids $\mathbf{V}$, the Malcev product $\mathbf{V} \circledM \mathbf{G}$ is the variety of monoids generated by the $\mathbf{V}$-extensions of groups. One can define alternatively the Malcev product by using *relational morphisms*. Recall that a relational morphism between monoids M and N is a function $\tau : M \to \mathcal{P}(N)$ such that:

(1) $\tau(m)\tau(n) \subset \tau(mn)$ for all $m, n \in M$,

(2) $\tau(m)$ is non-empty for all $m \in M$,

(3) $1 \in \tau(1)$

We will be only interested in relational morphisms into groups in this paper. Note that if $\tau : M \to G$ is a relational morphism into a group G, then $\tau^{-1}(1)$ is a submonoid of M. Let $\mathbf{V}$ be a variety. Then a monoid M belongs to the Malcev product $\mathbf{V} \circledM \mathbf{G}$ if and only if there exists a relational morphism τ from M into a group G such that $\tau^{-1}(1) \in \mathbf{V}$.

The Malcev product is usually a more powerful operation than the semidirect product.

Theorem 7.1 *Let* $\mathbf{V}$ *be any variety. Then* $\mathbf{V} * \mathbf{G} \subset \mathbf{V} \circledM \mathbf{G}$.

Proof. Let $M \in \mathbf{V} * \mathbf{G}$. Then M divides a monoid of the form $N * G$ where G is a group and $N \in \mathbf{V}$. Let $\pi : N * G \to G$ be the projection. Then $\pi^{-1}(1)$ is isomorphic to N and thus belongs to $\mathbf{V}$. Therefore $N * G$ is in $\mathbf{V} \circledM \mathbf{G}$ and so is M, since M divides $N * G$. $\square$

Corollary 7.2 $\mathbf{J} * \mathbf{G}$ *is contained in* $\mathbf{J} \circledM \mathbf{G}$.

It is not difficult to see that a $\mathcal{J}$-trivial extension of a group is a block group.

Proposition 7.3 $\mathbf{J} \circledM \mathbf{G}$ *is contained in* $\mathbf{BG}$.

Proof. Let M be a $\mathbf{J}$-extension of a group G and let $\pi : M \to G$ be a surjective morphism such that $\pi^{-1}(1)$ is $\mathcal{J}$ trivial. Now since $\pi(\langle E(M)\rangle) = \langle 1 \rangle = 1$, $\langle E(M)\rangle$ is contained in $\pi^{-1}(1)$ and hence it is $\mathcal{J}$-trivial. Thus, by Theorem 3.3, M is a block group. $\square$

It is slightly more difficult to establish the opposite inclusion.

Proposition 7.4 $\mathbf{BG}$ *is contained in* $\mathbf{J} \circledM \mathbf{G}$.

Proof. Let M be a block group and let $x \in M$. We claim that the partial action of x on M defined by

$$s \cdot x = \begin{cases} sx & \text{if } s \mathrel{\mathcal{R}} sx \\ \text{undefined} & \text{otherwise} \end{cases}$$

is one-to-one. Indeed, suppose that $rx = sx = t$ for some $r, s, t \in M$. Then $r \mathrel{\mathcal{R}} s \mathrel{\mathcal{R}} t$ and there exist $y, z \in M$ such that $ty = r$ and $tz = s$. Let $\mathrm{Stab}(r) = \{u \in M \mid ru = r\}$ be the right stabilizer of r and let G be its minimal ideal. Since $M \in \mathbf{BG}$, $\mathrm{Stab}(r) \in \mathbf{BG}$ and thus G is a group. Let e be the identity of G. Then $re = r$ and hence

(1) $r \cdot xye = t \cdot ye = r \cdot e = r$

(2) $r \cdot ezxye = r \cdot zxye = s \cdot xye = t \cdot ye = r \cdot e = r$

Therefore, xye and $ezxye$ are in G and thus $e \mathrel{\mathcal{R}} ez \mathrel{\mathcal{R}} ezxye$. It follows that the $\mathcal{H}$-class of ez contains an idempotent. But since M is a block group, the unique idempotent in the $\mathcal{R}$-class of ez is e and hence ez is in G. This means that $r \cdot ez = r$, proving the claim, since $r \cdot ez = r \cdot z = s$.

Furthermore, $s \mathrel{\mathcal{R}} sxy$ if and only if $s \mathrel{\mathcal{R}} sx$ and $sx \mathrel{\mathcal{R}} sxy$. Therefore,

$$s \cdot xy = (s \cdot x) \cdot y \quad \text{for all } s, x, y \in M \tag{1}$$

Let now $\mathfrak{S}(M)$ be the symmetric group on M and let $\tau : M \to \mathfrak{S}(M)$ be the relation that associates to any $x \in M$ the set $\tau(x)$ of all permutations on M that extend the partial permutation on M defined by x. Then formula 1 shows that τ is a relational morphism.

It suffices now to verify that $K = \tau^{-1}(1)$ is a $\mathcal{J}$-trivial monoid. By definition, an element of K defines a partial identity on M. Let $x, y \in K$ and let $s = (xy)^\omega$. Then $s \mathcal{R} sx$, and since x defines a partial identity, it follows $sx = s$, that is $(xy)^\omega = (xy)^\omega x$. Thus K is a $\mathcal{R}$-trivial block group, and hence a $\mathcal{J}$-trivial monoid. □

The results presented so far were obtained by Margolis and the author in 1984 [16]. The last remaining inclusion, $\mathbf{J} \circledM \mathbf{G} \subset \mathbf{J} * \mathbf{G}$ was established seven years later by Henckell and Rhodes [10, 9]

Theorem 7.5 $\mathbf{J} \circledM \mathbf{G}$ *is contained in* $\mathbf{J} * \mathbf{G}$.

The proof relies on several deep results of semigroup theory: the theory of derived categories, Knast's result on graphs and Ash's proof of the Rhodes "cover" conjecture. It is detailed in [11] and thus we shall just give an outline.

Let M be a monoid in $\mathbf{J} \circledM \mathbf{G}$. By the results mentioned above, there exists a relational morphism τ from M into a group G such that $\tau^{-1}(1) \in \mathbf{J}$. One would like to keep $\tau^{-1}(1)$ as small as possible. Define the *kernel* $K(M)$ of M to be the intersection of the submonoids $\tau^{-1}(1)$ over all relational morphisms $\tau : M \to G$ into a group. A compactness argument shows the existence of a relational morphism τ from M into a group G such that $\tau^{-1}(1) = K(M)$. Thus, for this relational morphism, $\tau^{-1}(1)$ is clearly minimal. Actually a stronger result holds: one can show the existence of a relational morphism $\tau : M \to G$ such that, for all $g \in G$, $\tau^{-1}(g)$ is in some sense minimal. To make this definition precise, define a subset X of M to be *pointlike for* τ if there is a $g \in G$ such that $X \subset \tau^{-1}(g)$. A subset of M is called simply *pointlike* if it is pointlike for all relational morphisms from M into a group. Finally, call *universal* a relational morphism $\tau : M \to G$ such that

(1) $\tau^{-1}(1) = K(M)$,

(2) any pointlike subset for τ is pointlike.

Again, the existence of universal morphisms for any monoid M is ensured by a compactness argument. Ash's theorems, first conjectured by Rhodes, give some important properties of these universal relational morphisms. The first theorem of Ash [3, 4] gives a precise description of the kernel of M.

An element $\bar{s}$ of a monoid M is a *weak inverse* of s if $\bar{s}s\bar{s} = \bar{s}$. A submonoid K of M is *closed under weak conjugacy* if for every $u \in K$ and every $\bar{s}, s \in M$ such that $\bar{s}$ is a weak inverse of s, $\bar{s}us \in K$ and $su\bar{s} \in K$. Given a monoid M, denote by $D(M)$ the smallest submonoid of M closed under weak conjugacy.

Theorem 7.6 *For every monoid* M, $K(M) = D(M)$.

The second theorem of Ash [3, 4] gives a deep characterization of the pointlike sets. For $m \in M$, set

$$m^{(1)} = \{m\} \quad \text{and} \quad m^{(-1)} = \{\bar{m} \mid \bar{m} \text{ is a weak inverse of } m\}$$

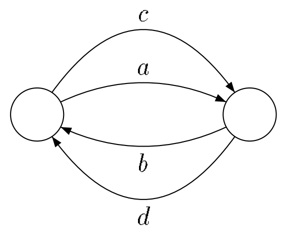
Theorem 7.7 *A subset* X *of a monoid* M *is pointlike if and only if there are elements* $m_1, m_2, \ldots m_n$ *of* M *such that*

$$X \subset D(M)m_1^{(\varepsilon_1)}D(M)m_2^{(\varepsilon_2)}D(M)\cdots D(M)m_n^{(\varepsilon_n)}D(M)$$

where $\varepsilon_i \in \{1, -1\}$ *for* $1 \le i \le n$.

We now recall the definition of a derived category [18, 39]. Let $\tau : M \to G$ be a relational morphism into a group G. The *derived category* of τ is the (small) category $D(\tau)$ whose objects are the elements of G and whose arrows are the triples $(h, (m, g), hg)$ such that $g \in \tau(m)$. The *exponent of a finite category* C is the smallest integer ω such that m^ω is idempotent for every loop $m \in C$. The following result combines two results of Tilson [39] and Knast [13].

Theorem 7.8 *A monoid M belongs to $\mathbf{J} * \mathbf{G}$ if and only if there is a relational morphism $\tau : M \to G$ onto a finite group G whose derived category $D(\tau)$ satisfies the path identity $(ab)^\omega ad(cd)^\omega = (ab)^\omega(cd)^\omega$ for every subcategory of $D(\tau)$ of the form*



We have seen that if $M \in \mathbf{J}\,\textcircled{M}\,\mathbf{G}$, there exists a universal relational morphism $\tau : M \to G$ into a group G such that $\tau^{-1}(1) \in \mathbf{J}$. By Theorem 7.5 it suffices now to show that τ satisfies the path identity $(ab)^\omega ad(cd)^\omega = (ab)^\omega(cd)^\omega$. To verify this identity, consider a subgraph of $D(\tau)$ of the form shown in Figure 7.1

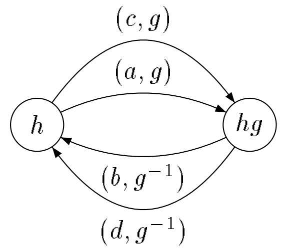


Figure 7.1:

In particular, we have $\{a, c\} \subset g\tau^{-1}$ and since τ is universal for M, $\{a, c\}$ is a pointlike subset of M. By Theorem 7.7, there exist elements $d_0, \ldots, d_k, d'_0, \ldots, d'_k$ of $D(M)$, elements $m_1, \ldots, m_k$ of M and integers $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, 1\}$ such that

$$a \in d_0 m_1^{(\varepsilon_1)} d_1 m_2^{(\varepsilon_2)} \cdots\; d_{k-1} m_k^{(\varepsilon_k)} d_k \tag{2}$$

$$c \in d'_0 m_1^{(\varepsilon_1)} d'_1 m_2^{(\varepsilon_2)} \cdots\; d'_{k-1} m_k^{(\varepsilon_k)} d'_k \tag{3}$$

Thus there is a very loose relation between a and c. The rest of the proof, which is omitted here, amounts to show that this relation suffices to establish the path identity. $\square$

8 Block groups and ordered monoids

A consequence of the equality $\mathbf{BG} = \mathbf{PG}$ related with ordered monoids is presented in this section. Recall that an *ordered monoid* is a monoid equipped with an order relation $\leq$ such that $s \leq t$ implies $sx \leq tx$ and $xs \leq xt$ for all $x, s, t \in M$. An ordered monoid $(M, \leq)$ is called *E-ordered* if, for all $e \in E(M)$, $e \leq 1$. This definition is motivated by the following property of E-ordered monoids.

Proposition 8.1 *Every E-ordered monoid is a block-group.*

Proof. Let $(M, \leq)$ be an E-ordered monoid and let e and f be two $\mathcal{R}$-equivalent idempotents of M. Then $ef = f$ and $fe = e$. Now $e \leq 1$ implies $e = fe \leq f$ and $f \leq 1$ implies $f = ef \leq e$. Thus $e = f$. A dual argument would show that any pair of $\mathcal{L}$-equivalent idempotents are equal. Therefore M is a block group. $\square$

The converse of Proposition 8.1 is false: there exist some block groups that cannot be E-ordered. However, a partial converse holds.

Theorem 8.2 *Every block group is the quotient of some E-ordered monoid.*

Proof. It is easy to verify that the monoids that are quotient of an E-ordered monoid form a variety $\mathbf{V}$. Now if G is a group, then $(\mathcal{P}'(G), \supset)$ is E-ordered. Indeed, by Proposition 4.2 (1), the idempotents of $\mathcal{P}'(G)$ are the subgroups of G, and they contain $\{1\}$, the identity of $\mathcal{P}'(G)$. It follows that $\mathbf{V}$ contains $\mathbf{PG}$ and thus $\mathbf{BG}$, since $\mathbf{PG} = \mathbf{BG}$. $\square$

9 A topological consequence

The progroup topology on A^* is the smallest topology such that every monoid morphism from A^* onto a finite group G is continuous. It is equivalent to say that the group languages form a basis for this topology. The progroup topology was first considered for the free group by M. Hall [8] and by Reutenauer for the free monoid [31, 33]. It is also connected to the study of implicit operations (see the article by J.Almeida and P.Weil elsewhere in this volume).

Some years ago, the author discovered [21, 26, 23] a curious connection between this topology and the Rhodes conjecture $K(M) = D(M)$. The main point was that the Rhodes conjecture reduces to compute the closure of a given recognizable language for this topology. Thus it became a natural and important question to characterize the recognizable closed (resp. open) languages. Several equivalent topological conjectures were presented in [26] and they were later shown to be all equivalent to the Rhodes conjecture [19].

In [29], Reutenauer and the author proposed another conjecture on the progroup topology of the free group and showed that this conjecture also implies the Rhodes conjecture. Again, it was later shown [11] that the Rhodes conjecture and the topological conjecture on the free group were equivalent. The interested reader is referred to the original articles and to the survey [11] for more details.

Finally, when Ash proved the Rhodes conjecture [3, 4], all these topological conjectures became theorems. One year later, a direct proof of the topological conjecture on the free group was obtained by Ribes and Zalesskii [35], giving in turn a new proof of Ash's theorem! The proof of Ribes and Zaleski uses profinite trees acting on groups.

We now come back to the original topological problem: characterize the recognizable closed (resp. open) languages. The author observed that the syntactic monoid of a recognizable closed (resp. open) language is a block group [21, 26]. The characterization of the closed and open recognizable sets is the following. Let L be a subset of A^*, let $\eta : A^* \to M(L)$ be the syntactic morphism of L and let $P = \eta(L)$ be the syntactic image of L. Then

Theorem 9.1

(1) *L is closed if and only if for every $s, t \in M$ and for every $e \in E(M)$, $set \in P$ implies $st \in P$.*

(2) *L is open if and only if for every $s, t \in M$ and for every $e \in E(M)$, $st \in P$ implies $set \in P$.*

The author recently obtained a more combinatorial description of the open sets [27].

Theorem 9.2 *A recognizable language is open if and only if it is a finite union of languages of the form $L_0 a_1 L_1 \cdots a_k L_k$ where the a_i's are letters and the L_i's are group languages.*

10 Conclusion and open problems

The sequence of equalities

$$\Diamond\mathbf{G} = \mathbf{PG} = \mathbf{J} * \mathbf{G} = \mathbf{J} \textcircled{\scriptsize M} \mathbf{G} = \mathbf{BG} = \mathbf{EJ}$$

is reminiscent of another sequence of equalities

$$\Diamond_2\mathbf{G} = \mathbf{Inv} = \mathbf{J_1} * \mathbf{G} = \mathbf{J_1} \textcircled{\scriptsize M} \mathbf{G} = \mathbf{Ecom} = \mathbf{EJ}_1$$

where $\Diamond_2\mathbf{G}$ denotes the variety generated by Schützenberger products of two groups, $\mathbf{J_1}$ the variety of idempotent and commutative monoids (or semilattices), **Ecom** the variety of monoids whose idempotent commute and **Inv** the variety generated by inverse monoids. Not only the second sequence has several similarities with the first one, but its success story is also curiously analogous. Indeed, all but one of these equalities were obtained by Margolis and the author [18] and the last missing inclusion $\mathbf{Ecom} \subset \mathbf{J_1} \textcircled{\scriptsize M} \mathbf{G}$ was obtained by Ash [1, 2].

Let us come back to the equality $\mathbf{BG} = \mathbf{PG}$. It implies in particular that any block group M divides a power group $\mathcal{P}(G)$. It would be interesting to find an upper bound on the size of G as a function of $|M|$. Of course, one could trace the proof of $\mathbf{BG} = \mathbf{PG}$, but with its detours of language theory, and the difficult theorem of Ash, it would give an enormous upper bound.

Another interesting problem is to obtain similar results when the variety $\mathbf{G}$ is replaced by a variety $\mathbf{H}$ of groups. The most interesting cases seem to be the varieties of commutative groups, p-groups (for a given prime p), nilpotent groups and solvable groups. It was for instance proved in [18] that the equalities $\mathbf{J_1} * \mathbf{H} = \Diamond_2\mathbf{H} = \mathbf{J_1} \textcircled{\scriptsize M} \mathbf{H}$ hold for any non trivial variety of groups, but it seems to be a very difficult problem to find an effective characterization of $\mathbf{PG}$ or to find out the varieties of groups for which the equality $\mathbf{J} * \mathbf{H} = \mathbf{J} \textcircled{\scriptsize M} \mathbf{H}$ holds. The topological approach seems to be the more promising way to solve this type of problems.

Acknowledgements

I would like to thank Pascal Weil for his comments on a preliminary version of this article.

References

[1] C.J. Ash, Finite idempotent-commuting semigroups, in S. Goberstein and P. Higgins (eds.) *Semigroups and their applications*, Reidel (Dordrecht, Holland), (1987) 13–23.

[2] C.J. Ash, Finite semigroups with commuting idempotents, *J. Austral. Math. Soc. (Series A)* **43**, (1987) 81–90.

[3] C. J. Ash, Inevitable sequences and a proof of the type II conjecture, in *Proceedings of the Monash Conference on Semigroup Theory*, World Scientific, Singapore, (1991) 31–42.

[4] C. J. Ash, Inevitable Graphs: A proof of the type II conjecture and some related decision procedures, *Int. Jour. Alg. and Comp.* **1** (1991) 127–146.

[5] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, Mathematical Surveys No 7, American Mathematical Society, Providence, RI, Vol. 1, 1961; Vol. 2, 1967.

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

[7] R. L. Graham, On finite 0-simple semigroups and graph theory, *Math. Syst. Theory* **2**, (1968) 325–339.

[8] M. Hall Jr., A topology for free groups and related groups, *Ann. of Maths*, **52**, (1950) 127–139.

[9] K. Henckell, Blockgroups = Power Groups, in *Proceedings of the Monash Conference on Semigroup Theory*, World Scientific, Singapore, (1991) 117–134.

[10] K. Henckell and J. Rhodes, The theorem of Knast, the $PG = BG$ and Type II Conjectures, in J. Rhodes (ed.) *Monoids and Semigroups with Applications*, Word Scientific, (1991) 453–463

[11] K. Henckell, S. W. Margolis, J.-E. Pin and J. Rhodes, Ash's Type II Theorem, Profinite Topology and Malcev Products, *International Journal of Algebra and Computation* **1** (1991) 411–436.

[12] J.M. Howie, *An introduction to Semigroup Theory*, Academic Press, London, 1976.

[13] R. Knast, Some theorems on graph congruences, *RAIRO Inform. Théor.* **17** (1983) 331–342.

[14] G. Lallement, *Semigroups and combinatorial applications*, Wiley, New York, 1979.

[15] S.W. Margolis, Kernels and expansions: an historical and technical perspective, in J. Rhodes (ed.) *Monoids and Semigroups with Applications*, Word Scientific, (1991) 3–30.

[16] 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*, edited by K. Byleen, P. Jones and F. Pastijn (Dept. of Mathematics, Statistics and Computer Science, Marquette University) (1984) 113–130.

[17] S. W. Margolis and J.-E. Pin, Product of group languages, FCT Conference, Lecture Notes in Computer Science **199** (1985) 285–299.

[18] S. W. Margolis and J.-E. Pin, Inverse semigroups and varieties of finite semigroups, *Journal of Algebra* **110** (1987) 306–323.

[19] S. W. Margolis and J.-E. Pin, New results on the conjecture of Rhodes and on the topological conjecture, *J. Pure and Applied Algebra* **80**, (1992) 305–313.

[20] J.-E. Pin, Variétés de langages et monoïde des parties, *Semigroup Forum* **20** (1980) 11–47.

[21] J.-E. Pin, Finite group topology and p-adic topology for free monoids, in *12th ICALP, Lecture Notes in Computer Science* **194**, Springer, Berlin, (1985) 445–455.

[22] J.-E. Pin, *Variétés de langages formels*, 160 p., Masson, Paris (1984). *Varieties of formal languages*, 138 p., North Oxford Academic (London), 1986 and Plenum (New York), 1986.

[23] J.-E. Pin, A topological approach to a conjecture of Rhodes, *Bulletin of the Australian Mathematical Society* **38** (1988) 421–431.

[24] J.-E. Pin, Relational morphisms, transductions and operations on languages, in J.-E. Pin (ed.), *Formal properties of finite automata and applications*, Lect. Notes in Comp. Sci. **386**, Springer, (1989) 120–137.

[25] J.-E. Pin, On a conjecture of Rhodes, *Semigroup Forum* **39** (1989) 1–15.

[26] J.-E. Pin, Topologies for the free monoid, *Journal of Algebra* **137** (1991) 297–337.

[27] J.E. Pin, Polynomial closure of group languages and open sets of the Hall topology, submitted.

[28] J.-E. Pin, Finite semigroups and recognizable languages: an introduction, this volume.

[29] J.-E. Pin and C. Reutenauer, A conjecture on the Hall topology for the free group, *Bull. London Math. Soc.* **23**, (1991) 356–362.

[30] J. Reiterman, The Birkhoff theorem for finite algebras, *Algebra Universalis*, **14** (1982), 1–10.

[31] Ch. Reutenauer, Une topologie du monoïde libre, *Semigroup Forum* **18** (1979) 33–49.

[32] Ch. Reutenauer, Sur les variétés de langages et de monoïdes, *Lecture Notes in Computer Science* **67**, Springer, Berlin, (1979) 260–265.

[33] Ch. Reutenauer, Sur mon article "Une topologie du monoïde libre", *Semigroup Forum* **22** (1981) 93–95.

[34] J. Rhodes, Global structure theorems for arbitrary semigroups, in *Proceedings of the 1984 Marquette Conference on Semigroups, edited by K. Byleen, P. Jones and F. Pastijn (Dept. of Mathematics, Statistics and Computer Science, Marquette University)* (1984) 197–228.

[35] L. Ribes and P.A. Zalesskii, On the profinite topology on a free group, *Bull. London Math. Soc.* **25** (1993) 37–43.

[36] H. Straubing, Recognizable sets and power sets of finite semigroups, *Semigroup Forum*, **18** (1979) 331–340.

[37] B. Tilson, Monoid Kernels, Semidirect Products and their Adjoint Relationship, in J. Rhodes (ed.) *Monoids and Semigroups with Applications*, Word Scientific, (1991) 31–54.

[38] B. Tilson, Type II redux, in Semigroups and Their Applications, edited by S.M. Goberstein and P.M. Higgins, Reidel, Dordrecht, (1987) 201–205.

[39] B. Tilson, Categories as algebras: an essential ingredient in the theory of finite monoids, *J. Pure Applied Algebra* **48** (1987), 83–198.