JOURNAL OF ALGEBRA 110, 306–323 (1987)

Inverse Semigroups and Varieties of Finite Semigroups

S. W. MARGOLIS

Computer Science, Ferguson Building, University of Nebraska, Lincoln, Nebraska 68588-0115

AND

J. E. PIN

LITP, 4 Place Jussieu, Tour 55–65, 75252 Paris Cedex 05, France

Received November 13, 1984

This paper is the third part of a series of three papers devoted to the study of inverse monoids. It is more specifically dedicated to finite inverse monoids and their connections with formal languages. Therefore, except for free monoids, all monoids considered in this paper will be finite.

Throughout the paper we have adopted the point of view of varieties of monoids, which has proved to be an important concept for the study of monoids. Following Eilenberg [2], a variety of monoids is a class of monoids closed under taking submonoids, quotients, and finite direct products. Thus, at first sight, varieties seem to be inadequate for studying inverse monoids since a submonoid of an inverse monoid is not inverse in general. To overcome this difficulty, we consider the variety **Inv** generated by inverse monoids and closed under taking submonoids, quotients, and finite direct products. Now inverse monoids are simply the regular monoids of this variety and we may use the powerful machinery of variety theory to investigate the algebraic structure of these monoids.

Our first result states that **Inv** is the variety generated by one of the following classes of monoids.

(a) Semidirect products of a semilattice by a group.

(b) Extensions of a group by a semilattice.

(c) Schützenberger products of two groups.

(d) Schützenberger products of a group by the trivial monoid 1.

Moreover, equality of the varieties generated by the classes (a), (b), (c),

0021-8693/87 $3.00

and (d) still holds if one replaces "group" by "commutative group," "solvable group," "p-group," or more generally by "group of **H**," where **H** denotes a variety of (finite) groups. A natural guess would be that one obtains in this way all monoids of **Inv** whose groups are in **H**. However, this is not the case and we exhibit an inverse monoid all of whose subgroups are commutative—and even trivial—that is not in the variety generated by extensions of a commutative group by a semilattice.

Now a natural question arises: given a monoid M, is there an algorithm to decide whether or not M belongs to **Inv**? Such decidability problems have proved to be extremely difficult and are related to important problems of language theory. In our case we propose the following conjecture. (See note added in proof.)

Conjecture. A monoid M is in **Inv** iff idempotents of M commute.

It is easy to see that the class of monoids whose idempotents commute is a variety containing **Inv**, but the opposite inclusion probably requires a non-trivial proof. Just to avoid some work for future researchers of this problem, we show how two natural attempts to solve the conjecture fail. First, as we have seen above, it doesn't help much to assume a condition on groups. Second, we prove that it is decidable whether a monoid is (isomorphic to) a submonoid of an inverse monoid. However, we also exhibit a monoid of **Inv** that is not a submonoid of an inverse monoid. Let us conclude our discussion of the conjecture with some more positive results. We show that if the idempotents of a monoid M commute with every element of M, then M belongs to **Inv**. We also show that the conjecture is true iff every monoid whose idempotents commute is quotient of an E-unitary monoid. Therefore our conjecture appears as the finite version of the conjecture discussed in our first paper [8].

It was shown by Eilenberg that varieties of monoids are in one-to-one correspondence with certain classes of recognizable (or regular) languages, called varieties of languages. Although a number of varieties of languages corresponding to classical varieties of monoids have been described (see [2, 5, 13]), no such description was known for **Inv**. In this paper we prove that the variety of languages $\mathscr{I}nv$ corresponding to **Inv** can be described in three different ways. More precisely, for each alphabet A, $A^* \mathscr{I}nv$ is the boolean algebra generated by one of the following classes of languages:

(a) Languages of the form L or LaA^*, where L is a group language and a is a letter of A.

(b) Languages of the form L or A^*aL, where L is a group language and a is a letter of A.

(c) Languages of the form L or KaL, where K and L are group-languages and a is a letter of A.

Our last result makes more precise a result of [3, 6] on the connection between inverse monoids and biprefix codes. It was shown that the variety **Inv** can be described by its finite biprefix codes. Here we use a different construction to take into account the group structure of the monoids. More precisely, we show that if **H** is a variety of groups, then the variety of all monoids of **Inv** whose groups are in **H** can also be described by its finite biprefix codes. As we have observed before, such relativization results are not guaranteed for each property of **Inv**.

Some of these results were announced in [10]. This paper is divided into four main sections. Section 1 contains the preliminaries. The algebraic properties of **Inv** are established in Section 2 and the connection with language theory is presented in Section 3. Finally, our main conjecture is discussed in Section 4.

1. Preliminaries

In this paper all semigroups are *finite*, except in the case of a free semigroup or a free monoid. We assume familiarity with the notations of [8].

A semigroup S *divides* a semigroup T iff S is a quotient of a subsemigroup of T. Notice that division induces a partial order on semigroups.

A *variety of semigroups* is a class of semigroups closed under division and *finite* direct products. Varieties of monoids and varieties of groups are defined similarly. Notice that a variety of groups is a variety of monoids whose elements are groups.

EXAMPLES. **G** denotes the variety of all groups and **Gcom** denotes the variety of all commutative groups.

$\mathbf{J}_1$ denotes the variety of all idempotent and commutative monoids.

$(\mathbf{J}_1)_S$ denotes the variety of all idempotent and commutative semigroups (or semilattices).

A denotes the variety of all aperiodic (or group-free) semigroups.

I denotes the trivial variety of monoids consisting only of the monoid 1.

Given a class $\mathscr{C}$ of semigroups, the *variety of semigroups generated by* $\mathscr{C}$ is the smallest variety containing $\mathscr{C}$. Equivalently, it is the class of all semigroups S such that S divides a direct product $S_1 \times \cdots \times S_n$ of members of $\mathscr{C}$.

In this paper, we are mainly concerned with the variety **Inv** generated by the inverse monoids. Since the class of inverse monoids is closed under direct product, a monoid M belongs to **Inv** iff M divides an inverse monoid.

Let M and N be two monoids. To simplify notation we shall write M

additively, without assuming that M is commutative. The identity of M (resp. N) is denoted by 0 (resp. 1).

A *left action* of N on M is a function $N \times M \to M$,

$$(n, m) \to nm,$$

satisfying for all $m, m_1, m_2 \in M$ and $n, n_1, n_2 \in N$

(1) $n(m_1 + m_2) = nm_1 + nm_2$,

(2) $n_1(n_2 m) = (n_1 n_2) m$,

(3) $1m = m$,

(4) $n0 = 0$.

This action is used to form a monoid $M * N$ on the set $M \times N$ with multiplication $(m, n)(m', n') = (m + nm', nn')$. $M * N$ is called a *semidirect product* of M and N.

To illustrate this notion let us consider the following example. Let Q be a finite set. We denote by $S(Q)$ the symmetric group on Q, that is, the group of all permutations on Q under composition. Similarly $I(Q)$ denotes the monoid of all injective partial functions from Q to Q under composition of partial functions. Finally, 2^Q denotes the idempotent and commutative monoid of subsets of Q under intersection. Define a left action of $S(Q)$ on 2^Q by setting for all $\sigma \in S(Q)$ and $P \subset Q$, $\sigma P = P\sigma^{-1}$. This action defines a semidirect product $2^Q * S(Q)$ and the following result is classical.

PROPOSITION 1.1. *There exists a surjective monoid morphism* $\Theta\colon 2^Q * S(Q) \to I(Q)$ *which is one-to-one the idempotents.*

Proof. For $P \subset Q$ and $\sigma \in S(Q)$, let σ_P be the partial function of Q defined by

$$q\sigma_P = \begin{cases} q\sigma & \text{if } q \in P \\ \varnothing & \text{otherwise.} \end{cases}$$

Then we define a surjective function $\Theta\colon 2^Q * S(Q) \to I(Q)$ by setting $(P, \sigma)\,\Theta = \sigma_P$. Let (P, σ) and (P', σ') be two elements of $2^Q * S(Q)$. Then the domain of $\sigma_P \circ \sigma_{P'}$ is $P \cap P'\sigma^{-1}$ and thus $(P, \sigma)(P', \sigma')\,\Theta = (P, \sigma)\,\Theta(P', \sigma')\,\Theta$. It follows that Θ is a morphism. Finally, (P, σ) is idempotent in $2^Q * S(Q)$ if and only if $\sigma = 1$ and thus Θ is one-to-one on idempotents. ∎

Given two varieties of monoids $\mathbf{V}$ and $\mathbf{W}$, we denote by $\mathbf{V} * \mathbf{W}$ the variety of monoids generated by all semidirect products of the form $M * N$, where $M \in \mathbf{V}$ and $N \in \mathbf{W}$. Similarly we denote by $\mathbf{W} *_{\mathrm{r}} \mathbf{V}$ the variety of monoids generated by all reverse semidirect products of the form $N *_{\mathrm{r}} M$, where $N \in \mathbf{W}$ and $M \in \mathbf{V}$, and by $\Diamond(\mathbf{V}, \mathbf{W})$ the variety of monoids generated by all Schützenberger products of the form $\Diamond(M, N)$, where $M \in \mathbf{V}$ and $N \in \mathbf{W}$.

Let S and T be two semigroups. A *relational morphism* $\tau: S \to T$ is a relation from S to T such that

(1) for all $s \in S$, $s\tau \neq \varnothing$,

(2) for all $s, t \in S$ $(s\tau)(t\tau) \subset (st)\tau$.

Equivalently, τ is a relational morphism if the set $\{(s, t) | t \in s\tau\}$ is a subsemigroup of $S \times T$. Notice that if τ is a function, τ is a morphism in the usual sense. If $\tau: S \to T$ is a relational morphism and if S' is a subsemigroup of S, then $S'\tau$ is a subsemigroup of T. Similarly if T' is a subsemigroup of T, $T'\tau^{-1} = \{s \in S | s\tau \cap T' \neq \varnothing\}$ is a subsemigroup of S.

Let $\mathbf{V}$ be a variety of semigroups. Then a (relational) morphism $\tau: S \to T$ is a (relational) $\mathbf{V}$-morphism if for all subsemigroups T' of T, $T' \in \mathbf{V}$ implies $T'\tau^{-1} \in \mathbf{V}$. A (relational) $\mathbf{A}$-morphism is also called a (relational) *aperiodic morphism.*

If M and N are monoids, a *relational monoid morphism* $\tau: M \to N$ is a relational morphism satisfying the further condition

(3) $1 \in 1\tau$

Relational $\mathbf{V}$-morphisms have proved to be an important tool in the study of varieties of semigroups and languages [2, 13]. In particular, they can be used to define a new operation on varieties. Let $\mathbf{V}$ be a variety of semigroups and let $\mathbf{W}$ be a variety of monoids. Then $\mathbf{V}^{-1}\mathbf{W}$ is the variety of all monoids M such that there exists a relational monoid $\mathbf{V}$-morphism $\tau: M \to N$ with $N \in \mathbf{W}$.

Notice also that the composition of two relational $\mathbf{V}$-morphisms is again a $\mathbf{V}$-morphism.

A relational morphism $\tau: S \to T$ is *injective* if for all $s_1, s_2 \in S$, $s_1\tau \cap s_2\tau \neq \varnothing$ implies $s_1 = s_2$. Let us recall some useful results about injective relational morphisms.

PROPOSITION 1.2. *Let S and T be semigroups. Then S divides T iff there exists an injective relational morphism $\tau: S \to T$.*

PROPOSITION 1.3. *Let $\tau: S \to T$ be an injective relational morphism. Then for any variety of semigroups $\mathbf{V}$, τ is a $\mathbf{V}$-morphism. Moreover $(E(T))\tau^{-1} = E(S)$.*

Proof. We prove the second part of this statement, which is nonstandard. Let $e \in E(S)$. Then $e\tau$ is a non-empty semigroup of T and thus contains an idempotent. It follows that $e \in (E(T))\tau^{-1}$ and hence

$E(S) \subset (E(T))\tau^{-1}$. Conversely let $f \in E(T)$. Then $f\tau^{-1}$ is a subsemigroup of S. If $f\tau^{-1}$ is empty then clearly $f\tau^{-1} \subset E(S)$. Otherwise let e be an idempotent of $f\tau^{-1}$. Then if $s \in f\tau^{-1}$, we have $f \in e\tau \cap s\tau$ and thus $e = s$ since τ is injective. Consequently $f\tau^{-1} = \{e\}$ and $(E(T))\tau^{-1} \subset E(S)$. ∎

Finally, we recall an important theorem of Simon [2]. Let Γ be a graph and let C be the free category over this graph. A *loop* around a vertex u is a morphism from u to u. Thus a loop around u is either the empty path O_u or a path with origin u and end u. Let σ be the function that sends every path $p = e_1 \cdots e_n$ to its set of edges $\{e_1, ..., e_n\}$ and every empty path O_u to $\varnothing$. Then we have:

THEOREM 1.4 [2]. *Let $\sim$ be the smallest congruence on C satisfying $p + p \sim p$ and $p + q \sim q + p$ for any loops p, q around the same vertex. Then for any coterminal paths p, q, we have $p \sim q$ iff $p\sigma = q\sigma$.*

2. THE VARIETY GENERATED BY INVERSE SEMIGROUPS

The aim of this section is to give different characterizations of the variety **Inv**. Our first characterizations simply translate in terms of varieties some well-known facts about inverse semigroups.

THEOREM 2.1. *The equality* $\mathbf{Inv} = \mathbf{J}_1 * \mathbf{G}$ *holds.*

Proof. As is well known [1], any semidirect product of a semilattice by a group is an inverse semigroup. Thus $\mathbf{J}_1 * \mathbf{G} \subset \mathbf{Inv}$. Conversely let $M \in \mathbf{Inv}$. Then by the Preston–Vagner theorem [1], M divides a monoid $I(Q)$ for some finite set Q. Now Proposition 1.1 shows that $I(Q)$ divides $2^Q * S(Q)$. Since $2^Q \in \mathbf{J}_1$ and $S(Q) \in \mathbf{G}$ it follows that $2^Q * S(Q) \in \mathbf{J}_1 * \mathbf{G}$ and hence $M \in \mathbf{J}_1 * \mathbf{G}$. Therefore $\mathbf{Inv} \subset \mathbf{J}_1 * \mathbf{G}$. ∎

Next we have the following connection with the Schützenberger product.

THEOREM 2.2. *For any variety of groups* $\mathbf{H}$, *the following equalities hold*: $\mathbf{J}_1 * \mathbf{H} = \mathbf{H} *_r \mathbf{J}_1 = \diamond(\mathbf{H}, \mathbf{I}) = \diamond(\mathbf{I}, \mathbf{H}) = \diamond(\mathbf{H}, \mathbf{H})$.

Proof. It was shown in [8] that any semidirect product of the form $S * G$, where G is a group, is isomorphic to $G *_r S$. It follows immediately that $\mathbf{J}_1 * \mathbf{H} = \mathbf{H} *_r \mathbf{J}_1$ for any variety of groups $\mathbf{H}$. Next it is shown in [9] that if G, H are groups, then $\diamond(G, H)$ is isomorphic to a semidirect product $S * (G \times H)$, where S is a semilattice. It follows at once that $\diamond(\mathbf{H}, \mathbf{H})$ is contained in $\mathbf{J}_1 * \mathbf{H}$. Since $\diamond(\mathbf{H}, \mathbf{I})$ and $\diamond(\mathbf{I}, \mathbf{H})$ are clearly contained in $\diamond(\mathbf{H}, \mathbf{H})$, it remains to show that $\mathbf{J}_1 * \mathbf{H}$ (resp. $\mathbf{H} *_r \mathbf{J}_1$) is contained in $\diamond(\mathbf{H}, \mathbf{I})$ (resp. $\diamond(\mathbf{I}, \mathbf{H})$). Although a direct (but messy) algebraic proof is possible, we will give a short proof using language theory, which is postponed until the next section (Corollary 3.2). ∎

It is known [8] that an inverse semigroup T is a subsemigroup of a semidirect product $S * G$, where S is a semilattice and G is a group, iff there exists a surjective morphism $\phi: T \to G$ such that $1\phi^{-1} = E(T)$. In fact this result even holds for infinite semigroups. We present here an extension of this theorem to arbitrary finite semigroups.

THEOREM 2.3. *Let T be a semigroup whose idempotents commute and let G be a group. Then the following conditions are equivalent*:

(1) *there is a relational morphism $\tau: T \to G$ such that $1\tau^{-1} = E(T)$,*

(2) *T divides a semidirect product $S * G$, where S is a semilattice.*

Proof. We first prove the easy part, namely, (2) implies (1).

If T divides $S * G$ there exists by Proposition 1.2 an injective relational morphism $\tau: T \to S * G$. Let $\pi: S * G \to G$ be the morphism defined by $(s, g)\pi = g$. Then $\tau\pi: S \to G$ is a relational morphism. Moreover $1\pi^{-1} = \{(s, 1) \mid s \in S\} = E(S * G)$ and, by Proposition 1.3, $(E(S * G))\tau^{-1} = E(T)$. Thus $1(\tau\pi)^{-1} = E(T)$ as required.

The proof that (1) implies (2) is more involved and requires Simon's theorem. Let $\tau: T \to G$ be a relational morphism such that $1\tau^{-1} = E(T)$. Define a graph Γ as follows. The set of vertices is G and the set of edges is $E = \{(g, t, h) \in G \times T \times G \mid g^{-1}h \in t\tau\}$. Of course the edge (g, t, h) has g as origin and h as end. Let C be the free category over Γ. Recall that the morphisms of C are just the paths of Γ. Then G acts on C as follows. The action of G on $\mathrm{Ob}(C) = G$ is just the multiplication in G (on the left) and if $g \in G$ and if $p = (g_0, t_1, g_1) + (g_1, t_2, g_2) + \cdots + (g_{n-1}, t_n, g_n)$ is a path, then $gp = (gg_0, t_1, gg_2) + \cdots + (gg_{n-1}, t_n, gg_n)$. Finally, if $p = O_u$, we set $gp = O_{gu}$.

Let $\pi: E \to T$ be the surjective function defined by $(g, t, h)\pi = t$. Since C is the free category over Γ, π can be extended in a unique way to a surjective function $\pi: \mathrm{Mor}(C) \to T$ satisfying $(p+q)\pi = (p\pi)(q\pi)$ for all consecutive paths p and q. Notice that if $p \in \mathrm{Mor}(g, h)$, that is, if p is a path from g to h, then $g^{-1}h \in p\pi\tau$. Then we have:

LEMMA 2.4. *Let p and q be two coterminal paths. If $p\sigma = q\sigma$, then $p\pi = q\pi$.*

Define a relation $\sim$ on C by setting $p \sim q$ iff p and q are coterminal and $p\pi = q\pi$. Then $\sim$ is a congruence. Moreover if p, q are loops over the same vertex g, then $1 = g^{-1}g \in p\pi\tau$ and $1 \in q\pi\tau$. It follows that $p\pi, q\pi \in 1\tau^{-1} =$

$E(T)$. Since $E(T)$ is a semilattice we then have $p+p \sim p$ and $p+q \sim q+p$. The lemma now follows from Simon's Theorem 1.4. ▮

Let 2^E be the semilattice of subsets of E under union. If $g \in G$ and $X \in 2^E$, set $gX = \{(gh, t, gk) \mid (h, t, k) \in X\}$. This defines a left action of G on 2^E and we thus have the semidirect product $2^E * G$. Let R be the subset of $2^E \times G$ consisting of all pairs $(p\sigma, g)$, where p is a path from 1 to g. Then R is a subsemigroup of $2^E * G$. Indeed if $(p\sigma, g)$ and $(q\sigma, h)$ are in R, we have $(p\sigma, g)(q\sigma, h) = (p\sigma \cup g(q\sigma), gh) = ((p+gq)\,\sigma, gh)$ since p and gq are consecutive paths.

Next define a function $\gamma\colon R \to T$ by setting $(p\sigma, g)\,\gamma = p\pi$. Lemma 2.4 shows that γ is well defined, since if $p, q \in \mathrm{Mor}(1, g)$ satisfy $p\sigma = q\sigma$, then $p\pi = q\pi$. γ is surjective because if $g \in t\tau$, then $(1, t, g)\,\sigma = \{(1, t, g)\}$ and $(\{(1, t, g)\}, g)\,\gamma = t$. Finally, we claim that γ is a morphism. Indeed if $p \in \mathrm{Mor}(1, g)$ and $q \in \mathrm{Mor}(1, h)$ then $(p+gq)\,\pi = (p\pi)(gq)\,\pi = (p\pi)(q\pi)$. Therefore $((p\sigma, g)(q\sigma, h))\gamma = (p\sigma \cup g(q\sigma), gh)\gamma = ((p+gq)\sigma, gh)\gamma = (p+gq)\,\pi = (p\pi)(q\pi) = (p\sigma, g)\,\gamma(q\sigma, h)\,\gamma$, proving the claim. Thus T is a quotient of R and hence T divides $2^E * G$. ▮

COROLLARY 2.5. *For any variety of groups* $\mathbf{H}$, $(\mathbf{J}_1)_{\mathrm{S}}^{-1}\,\mathbf{H} = \mathbf{J}_1 * \mathbf{H}$.

Proof. Let $T \in \mathbf{J}_1 * \mathbf{H}$. Then T divides a semidirect product where S is a semilattice and $G \in \mathbf{H}$. Now the morphism $\pi\colon S * G \to G$ defined by $(s, g)\,\pi = g$ is a $(\mathbf{J}_1)_{\mathrm{S}}$-morphism since $1\pi^{-1}$ is isomorphic to S. Thus $S * G \in (\mathbf{J}_1)_{\mathrm{S}}^{-1}$ and $T \in (\mathbf{J}_1)_{\mathrm{S}}^{-1}\,\mathbf{H}$.

Conversely if $T \in (\mathbf{J}_1)_{\mathrm{S}}^{-1}\,\mathbf{H}$, there exists a relational morphism $\tau\colon T \to G$ such that $G \in \mathbf{H}$ and $1\tau^{-1}$ is a semilattice. Now $1\tau^{-1} \subset E(T)$ since τ is a $(\mathbf{J}_1)_{\mathrm{S}}$-morphism and for all $e \in E(T)$, $1 \in e\tau$ since $e\tau$ is a subsemigroup of G. Therefore $1\tau^{-1} = E(T)$ and thus by Theorem 2.3, T divides a semidirect product $S * G$, where $S \in \mathbf{J}_1$. It follows that $T \in \mathbf{J}_1 * \mathbf{H}$. ▮

Let us summarize the various descriptions of **Inv** we have obtained so far.

THEOREM 2.6. *The following equalities hold*:

$$\mathbf{Inv} = \mathbf{J}_1 * \mathbf{G} = \mathbf{G} *_{\mathrm{r}} \mathbf{J}_1 = \diamond(\mathbf{G}, \mathbf{G}) = \diamond(\mathbf{G}, \mathbf{I}) = \diamond(\mathbf{I}, \mathbf{G}) = (\mathbf{J}_1)_{\mathrm{S}}^{-1}\,\mathbf{G}.$$

3. LANGUAGES

Denote by A^* the free monoid over the set A. We shall use in this section the terminology of language theory. A is an *alphabet*, elements of A are *letters*, elements of A^* are *words*, and subsets of A^* are *languages*. The unit of A^* is the *empty word*, denoted by 1. Given a set $\mathscr{S}$ of languages of A^*, the *boolean closure of* $\mathscr{S}$ is the smallest set $\mathscr{C}$ of languages A^* such that:

(1) $\mathscr{S}$ is contained in $\mathscr{C}$.

(2) $\varnothing \in \mathscr{C}$.

(3) If $L \in \mathscr{C}$, then $A^* \backslash L \in \mathscr{C}$.

(4) If $L_1, L_2 \in \mathscr{C}$, then $L_1 \cup L_2 \in \mathscr{C}$.

A language L of A^* is called *recognizable* if there exists a monoid morphism $\phi: A^* \to M$ from A^* into a finite monoid M such that $L = L\phi\phi^{-1}$. In this case we say that M *recognizes* L. We refer the reader to the books by Eilenberg [2] and Lallement [5] for further information on the theory of recognizable languages.

If $\mathbf{V}$ is a variety of finite monoids and A is a finite alphabet, then we denote by $A^*\mathscr{V}$ the class of all recognizable languages in A^* that are recognized by a monoid of $\mathbf{V}$. One can show [2, Chap. 7] that $\mathbf{V} \subset \mathbf{W}$ if only and only if $A^*\mathscr{V} \subset A^*\mathscr{W}$ for every (finite) alphabet A. This enables us to show that two varieties of monoids are equal by showing that, for every alphabet A, the corresponding sets of recognizable languages are equal.

We now describe the operations on languages corresponding to the operations $\mathbf{V} \to \mathbf{J}_1 * \mathbf{V}$, $\mathbf{V} *_r \mathbf{J}_1$ and $(\mathbf{V}, \mathbf{W}) \to \diamond(\mathbf{V}, \mathbf{W})$ on varieties of monoids. The following theorem summarizes the work of [14].

THEOREM 3.1. *Let* $\mathbf{V}$ *and* $\mathbf{W}$ *be varieties of monoids and let* A *be an alphabet*:

(1) $\mathbf{J}_1 * \mathbf{V}$ *corresponds to the boolean closure of all languages of the form* L *or* LaA^*, *where* $L \in A^*\mathscr{V}$ *and* $a \in A$;

(2) $\mathbf{V} *_r \mathbf{J}_1$ *corresponds to the boolean closure of all languages of the form* L *or* A^*aL, *where* $L \in A^*\mathscr{V}$ *and* $a \in A$;

(3) $\diamond(\mathbf{V}, \mathbf{W})$ *corresponds to the boolean closure of all languages of the form* L, K *or* LaK, *where* $L \in A^*\mathscr{V}$, $K \in A^*\mathscr{W}$ *and* $a \in A$.

We may now prove the following result of [14].

COROLLARY 3.2. *For any variety of monoids,* $\mathbf{J}_1 * \mathbf{V} = \diamond(\mathbf{V}, \mathbf{I})$ and $\mathbf{V} *_r \mathbf{J}_1 = \diamond(\mathbf{I}, \mathbf{V})$.

Proof. For any alphabet A, the set of recognizable languages associated to the variety $\mathbf{I}$ is $\{\varnothing, A^*\}$. Therefore it follows from Theorem 3.1 that the sets of recognizable languages associated to $\mathbf{J}_1 * \mathbf{V}$ and to $\diamond(\mathbf{V}, \mathbf{I})$ are equal. Thus $\mathbf{J}_1 * \mathbf{V} = \diamond(\mathbf{V}, \mathbf{I})$. The proof for $\mathbf{V} *_r \mathbf{J}_1 = \diamond(\mathbf{I}, \mathbf{V})$ is similar. ∎

A recognizable language is called a *group-language* if it is recognized by a group. We can now describe, for each alphabet A, the set $A^*\mathscr{I}nv$ of languages corresponding to the variety of monoids **Inv**.

THEOREM 3.3. *Let A be an alphabet and let L be a language of A^*. Then the following conditions are equivalent*:

(1) $L \in A^*\mathscr{I}nv$.

(2) *L is in the boolean closure of languages of the form K or KaA^*, where K is a group-language and $a \in A$.*

(3) *L is in the boolean closure of languages of the form K or A^*aK, where K is a group-language and $a \in A$.*

(4) *L is in the boolean closure of languages of the form K or KaK', where K and K' are group-languages and $a \in A$.*

The results above were obtained by viewing inverse monoids as Schützenberger products of groups. There have been alternate descriptions of the languages corresponding to **Inv** and various subvarieties by viewing inverse monoids as monoids of partial one-to-one maps [3, 6, 7, 11]. These descriptions utilize the theory of codes. Here we extend a result of [3].

We first review some terminology. $A^+ = A^* \setminus \{1\}$ denotes the free semigroup over A. A subset X of A^+ is a *code* if X^*, the submonoid of A^* generated by X, is free with base X. X is a *prefix code* if, for all $u, v \in A^*$, $u, uv \in X$ implies $v = 1$. Dually, X is a *suffix code* if, for all $u, v \in A^*$, $u, vu \in X$ implies $v = 1$. A *biprefix code* is a set that is both a prefix and a suffix code. Notice that, as suggested by the terminology, a prefix (resp. suffix, biprefix) code is a code.

If L is a recognizable language, we denote by $M(L)$ the *syntactic monoid* of L. $M(L)$ is the quotient of A^* under the congruence $\sim_L$ defined by $u \sim_L v$ iff for all $x, y \in A^*$, $xuy \in L \Leftrightarrow xvy \in L$. $M(L)$ is also the smallest monoid recognizing L, where "smallest" refers to the cardinality or to the division ordering as well. Algebraic properties of syntactic monoids often reflect combinatorial properties of languages. For example, it is known [4] that if X is a finite prefix code and if $M(X^*)$ is an inverse monoid, then X is a biprefix code. The following result shows that any syntactic monoid can be, in some sense, approximated by a syntactic monoid of the form $M(P^*)$, where P is a finite prefix code.

PROPOSITION 3.4 [7]. *Let M be a monoid. Then there is an (effectively constructible) finite prefix code P such that*

(1) *M divides $M(P^*)$,*

(2) *there is an aperiodic relational morphism τ: $M(P^*) \to M$.*

In [7] the same construction is used to prove

PROPOSITION 3.5. *Let $M \in \mathbf{Inv}$ be a monoid. Then there is an (effectively constructible) finite biprefix code P such that*

(1) *M divides $M(P^*)$,*

(2) *$M(P^*) \in \mathbf{Inv}$,*

(3) *there is an aperiodic relational morphism $\tau: M(P^*) \to M$.*

Now let $\mathbf{H}$ be a variety of groups and let $\bar{\mathbf{H}}$ be the variety of monoids all of whose subgroups lie in $\mathbf{H}$. We combine the above results to obtain

THEOREM 3.6. *Let $M \in \bar{\mathbf{H}} \cap \mathbf{Inv}$ be a monoid. Then there is an (effectively constructible) finite biprefix code P such that*

(1) *M divides $M(P^*)$,*

(2) *$M(P^*) \in \bar{\mathbf{H}} \cap \mathbf{Inv}$,*

(3) *there exists an aperiodic relational morphism $\tau: M(P^*) \to M$.*

Proof. Let P be the finite biprefix code given by Proposition 3.5. Then conditions (1) and (3) are satisfied and $M(P^*) \in \mathbf{Inv}$. We thus need only show that $M(P^*) \in \bar{\mathbf{H}}$. But $M \in \bar{\mathbf{H}}$ by hypothesis and there is an aperiodic relational morphism $\tau: M(P^*) \to M$. Therefore $M(P^*) \in \mathbf{A}^{-1}\bar{\mathbf{H}}$ and thus $M(P^*) \in \bar{\mathbf{H}}$ since $\mathbf{A}^{-1}\bar{\mathbf{H}} = \bar{\mathbf{H}}$ (see [2], for example). ∎

We say that a variety of monoids $\mathbf{V}$ is *described* by a class $\mathscr{C}$ of codes if $\mathbf{V}$ is the variety generated by the class $\{M(P^*) \mid P \in \mathscr{C}\}$. In particular we say that $\mathbf{V}$ is described by its finite prefix (resp. biprefix) codes if $\mathbf{V}$ is described by the class of all finite prefix (resp. biprefix) codes P such that $M(P^*) \in \mathbf{V}$. We can now state

COROLLARY 3.7. *For any variety of groups $\mathbf{H}$, the variety $\bar{\mathbf{H}} \cap \mathbf{Inv}$ is described by its finite biprefix codes.*

In particular we have

COROLLARY 3.8 [3]. *The variety of monoids $\mathbf{Inv}$ is described by its finite biprefix codes.*

In [3], Hall shows that given a finite set Q, the monoid $I(Q)$ is isomorphic to a submonoid of an *inverse* monoid of the form $M(P^*)$, where P is a finite biprefix code. It follows from the Vagner–Preston theorem that every inverse monoid is isomorphic to a submonoid of an inverse monoid of the form $M(P^*)$ for some finite biprefix code P. However, the Hall construction does not preserve the subgroup structure of M.

4. A Conjecture on Inverse Monoids

In Section 2 we have given a number of descriptions of the variety of monoids **Inv** that are summarized in Theorem 2.6. However, none of these descriptions gives a criterion for the membership problem for **Inv**. That is, given the multiplication table of a monoid M, decide whether $M \in \mathbf{Inv}$ or not. We conjecture that such a criterion exists and moreover that there is a very simple criterion. (See note added in proof.)

Conjecture. Let M be a monoid. Then $M \in \mathbf{Inv}$ if and only if the idempotents of M commute.

It is easy to see that the class of monoids whose idempotents commute is a variety, denoted by **Ecom**. Since idempotents commute in an inverse monoid, we have $\mathbf{Inv} \subset \mathbf{Ecom}$ and thus the conjecture is equivalent to show that **Ecom** is contained in **Inv**.

In this section we emphasize the importance of this conjecture by showing its connection with E-unitary monoids. Next we give some evidence for this conjecture by proving a weaker result—Theorem 4.4—and we conclude the section by some examples that show why the conjecture is non-trivial, if true.

Let us first prove a useful result about monoids whose idempotents commute.

Proposition 4.1. *Let M be a monoid whose idempotents commute. Then the minimal ideal of M is a group G. Moreover M divides $M/G \times G$.*

Proof. Let G be the minimal ideal of M. Then $E(M) \cap G$ is a subsemilattice of $E(M)$ that is also a simple semigroup. Therefore $E(M) \cap G$ is trivial, that is, G contains exactly one idempotent e. Thus G is a group with unit e. Let π: $M \to M/G$ be the natural surjective morphism and let ϕ: $M \to M/G \times G$ be the function defined by $m\phi = (m\pi, em)$. Then ϕ is a morphism since for all $m, n \in M$, $(em)(en) = e(me)\, n = e(em)\, n = emn$. Moreover ϕ is injective. Indeed let m, n be two distincts elements of M. If $m \in M \backslash G$ or $n \in M \backslash G$ then $m\pi \neq n\pi$. Now if $m, n \in G$ then $em = m$, $en = n$ and thus $m\phi \neq n\phi$. Therefore M is isomorphic to a submonoid of $M/G \times G$. ∎

We now give a slightly different version of a result that was discussed in length in our article on infinite inverse semigroups [8].

PROPOSITION 4.2. *A monoid M is E-unitary iff there exists a morphism $\phi: M \to G$ into a group such that $1\phi^{-1}$ is a semilattice. Moreover, in this case $1\phi^{-1} = E(M)$.*

Proof. For the convenience of the reader we give a self-contained proof. Suppose there is a morphism $\phi: M \to G$ into a group such that $1\phi^{-1}$ is a semilattice. Then $1\phi^{-1}$ is contained in $E(M)$. Now since $e\phi = 1$ for all $e \in E(M)$ it follows that $1\phi^{-1} = E(M)$ and $E(M)$ is a semilattice. If $em = f$ for some $e, f \in E(M)$ and $m \in M$, then $(e\phi)(m\phi) = (f\phi)$ and thus $m\phi = 1$. Consequently $m \in 1\phi^{-1} = E(M)$. Similarly $me = f$ implies $m \in E(M)$ and thus M is E-unitary.

Conversely let M be an E-unitary monoid. Then by Proposition 4.1 the minimal ideal of M is a group G with unit e. Let $\phi: M \to G$ be the function defined by $m\phi = em$. Then clearly ϕ is a morphism and since M is E-unitary, $1\phi^{-1} = \{m \in M \mid em = e\}$ is a semilattice. ∎

We use this last result to give an equivalent statement for the conjecture.

THEOREM 4.3. *The conjecture holds iff every monoid whose idempotents commute is a quotient of an E-unitary monoid.*

Proof. Assume that the conjecture holds and let $M \in \mathbf{Ecom}$. Then by assumption $M \in \mathbf{Inv}$ and thus $M \in (\mathbf{J}_1)_{\mathbf{S}}^{-1}\,\mathbf{G}$ by Theorem 2.6. It follows that there is a relational morphism $\tau: M \to G$ into a group G such that $1\tau^{-1}$ is a semilattice. Let $N = \{(m, g) \in M \times G \mid g \in m\tau\}$ and let $\alpha: N \to M$ and $\beta: N \to G$ be the projections defined by $(m, g)\,\alpha = m$ and $(m, g)\,\beta = g$. Since τ is a relational morphism, N is a submonoid of $M \times G$. Furthermore, α is a surjective morphism, β is a morphism, and $1\beta^{-1} = \{(m, 1) \mid m \in 1\tau^{-1}\}$ is isomorphic to the semilattice $1\tau^{-1}$. It follows by Proposition 4.1 that N is E-unitary. Therefore M is a quotient of an E-unitary monoid.

Conversely assume that every monoid M whose idempotents commute is a quotient of an E-unitary monoid N. Then by Proposition 4.1, there is a morphism $\phi: N \to G$ into a group such that $1\phi^{-1}$ is a semilattice. It follows that $N \in (\mathbf{J}_1)_{\mathbf{S}}^{-1}\,\mathbf{G}$ and hence $N \in \mathbf{Inv}$ by Theorem 2.6. Since M is a quotient of N, we also have $M \in \mathbf{Inv}$ and the conjecture holds. ∎

We consider now the variety $\mathbf{V}$ consisting of all monoids M whose idempotents are in the center of M, that is, such that $em = me$ for all $m \in M$ and $e \in E(M)$. Clearly $\mathbf{V}$ is a subvariety of $\mathbf{Ecom}$. It was proved in [15, 17] that the variety consisting of all *aperiodic* monoids whose idempotents are in the center of M is generated by all monoids of the form S^1, where S is a nilpotent semigroup. We prove here a similar result for $\mathbf{V}$. If M is a monoid, we denote by $U(M)$ the group of units of M. Then we can state:

THEOREM 4.4. *The variety* $\mathbf{V}$ *is generated by the monoids* M *such that* $M \setminus U(M)$ *is a nilpotent semigroup.*

Proof. The proof mimics the proof given in [15]. First of all if $M \setminus U(M)$ is a nilpotent semigroup, then either M is a group or M contains exactly two idempotents 1 and 0. In both cases it is clear that $M \in \mathbf{V}$. It follows that $\mathbf{V}$ contains the variety $\mathbf{W}$ generated by all monoids M such that $M \setminus U(M)$ is nilpotent.

Conversely let $M \in \mathbf{V}$. Then by Proposition 4.1, the minimal ideal of M is a group G and M divides $G \times (M/G)$. Since $G \in \mathbf{W}$ it suffices to show that $N = M/G$ is in $\mathbf{W}$. We prove this last result by induction on the number n of idempotents of M. If $n = 1$, N is trivial and thus $N \in \mathbf{W}$. If $n = 2$, then $N \setminus U(N)$ is a nilpotent semigroup and thus $N \in \mathbf{W}$. Finally, if $n > 2$, then N contains an idempotent e distinct from 1 and 0, the zero of N. Since the idempotents are in the center of M, $eN = NeN$ is a proper ideal of N. Let π: $N \to N/eN$ be the natural surjective morphism. Then the function ϕ: $N \to (N/eN) \times eN$ defined by $m\phi = (m\pi, em)$ is clearly a morphism. Furthermore, ϕ is injective. Indeed let m, n be two distinct elements of N. If $m \in N \setminus eN$ or $n \in N \setminus eN$ then $m\pi \neq n\pi$ and if $m, n \in eN$ then $em = m$ and $en = n$. In both cases $m\phi \neq n\phi$. Therefore N divides $(N/eN) \times eN$ and since N/eN and eN contain $(n-1)$ idempotents and have a zero, we have by induction $N/eN \in \mathbf{W}$. Therefore $N \in \mathbf{W}$ and hence $M \in \mathbf{W}$. ∎

Next we prove:

THEOREM 4.5. *The variety* $\mathbf{V}$ *is contained in* $\mathbf{Inv}$.

Proof. By Theorem 4.4 it suffices to show that if M is a monoid such that $S = M \setminus U(M)$ is a nilpotent semigroup, then $M \in \mathbf{Inv}$. Define a left action of $U = U(M)$ on S^1 by setting $g \cdot s = gsg^{-1}$. A short calculation shows that this is really an action and thus we have the semidirect product $S^1 * U$. Let ϕ: $S^1 * U \to M$ be the function defined by $(s, g)\,\phi = sg$. Then ϕ is onto because if $s \in S$, $(s, 1)\,\phi = s$ and if $s \in G$, $(1, s)\,\phi = s$. Moreover ϕ is a morphism since

$$((s, g)(t, h))\,\phi = (s + gtg^{-1}, gh)\,\phi = sgth = (s, g)\,\phi(t, h)\,\phi.$$

Therefore M divides $S^1 * U$. Since $U \in \mathbf{G}$ it suffices to show that $S^1 \in \mathbf{Inv}$. Indeed by Theorem 2.6 we would have $S^1 \in \mathbf{J}_1 * \mathbf{G}$ and thus $S^1 * U \in (\mathbf{J}_1 * \mathbf{G}) * \mathbf{G} = \mathbf{J}_1 * (\mathbf{G} * \mathbf{G}) = \mathbf{J}_1 * \mathbf{G}$ by [2, Chap. 5].

Set $S = \{s_0, s_1, ..., s_n\}$, where s_0 is the zero of S, let $k = n^2 + 1$, and let Z_k be the cyclic group of order k. Define a relation τ: $S^1 \to Z_k$ by setting

$$s\tau = \begin{cases} \{(i_1 + \cdots + i_r) \mid s_{i_1} \cdots s_{i_r} = s\} & \text{if} \quad s \in S \\ 0 & \text{if} \quad s = 1. \end{cases}$$

We claim that τ is a relational $(\mathbf{J}_1)_S$-morphism. We first prove the relation

$$(s\tau)(t\tau) \subset (st)\,\tau. \qquad (*)$$

If $s = t = 1$ the relation is clear. Next assume $s = 1$ and $t \in S$. If $s_{i_1} \cdots s_{i_r} = t$ then $0 + (i_1 + \cdots + i_r) = i_1 + \cdots i_r \in t\tau$. Thus $(*)$ holds in this case. The proof is similar if $s \in S$ and $t = 1$. Finally, assume $s, t \in S$. If $s_{i_1} \cdots s_{i_r} s_{j_1} \cdots s_{j_p} = st$ then $i_1 + \cdots + i_r + j_1 + \cdots + j_p \in (st)\,\tau$. Therefore τ is a relational morphism.

Now suppose that $0 \in s\tau$. Then either $s = 1$ or $s \in S$ and there exists $i_1, \ldots, i_r$ such that $s_{i_1} \cdots s_{i_r} = s$ and $i_1 + \cdots + i_r \equiv 0 \bmod k$. If one of the i_j's is equal to 0, then $s = s_0 = 0$. Otherwise, by the choice of k, we certainly have $r > n$ and thus $s \in S^{n+1}$. Since S is nilpotent $S^{n+1} = \{0\}$ and therefore $s = 0$. It follows that $O\tau^{-1} = \{0, 1\}$ and the claim holds. Therefore $M \in (\mathbf{J}_1)_S^{-1}\,\mathbf{G}$ and $M \in \mathbf{Inv}$ by Theorem 2.6. ∎

The proof of Theorem 4.5 can be easily adapted to show that $\mathbf{V} \cap \bar{\mathbf{H}}$ is contained in $\mathbf{J}_1 * \mathbf{H}$ for any variety of groups $\mathbf{H}$ containing all solvable groups. This suggests imposing some conditions on group in our conjecture by trying to prove $\mathbf{Ecom} \cap \bar{\mathbf{H}} = \mathbf{Inv} \cap \bar{\mathbf{H}}$. However, a difficulty arises when we try to extend the results of Section 2. Indeed we have shown that $\mathbf{J}_1 * \mathbf{H} = (\mathbf{J}_1)_S^{-1}\,\mathbf{H}$ for any variety of groups $\mathbf{H}$, and $\mathbf{J}_1 * \mathbf{H}$ is certainly contained in $\mathbf{Inv} \cap \bar{\mathbf{H}}$, but we conjecture that $\mathbf{J}_1 * \mathbf{H}$ is *not* equal to $\mathbf{Inv} \cap \bar{\mathbf{H}}$ as soon as $\mathbf{H}$ is not the variety of all groups. For instance, if $\mathbf{H} = \mathbf{I}$, then $\bar{\mathbf{H}} = \mathbf{A}$, $\mathbf{J}_1 * \mathbf{I} = \mathbf{J}_1$, but there exist aperiodic inverse monoids that are not idempotent and commutative, so $\mathbf{J}_1 * \mathbf{H} \neq \mathbf{Inv} \cap \bar{\mathbf{H}}$ in this case. Similarly if $\mathbf{H} = (Z_n)$, the variety generated by the cyclic group of order n, it is not difficult to see that every monoid M in $\mathbf{J}_1 * \mathbf{H}$ satisfies $x^n = x^{2n}$ for all $x \in M$. However, one can find monoids in $\mathbf{Inv} \cap \bar{\mathbf{H}}$ that do not fulfill this condition, for instance, the cyclic aperiodic monoid of order $n + 2$.

In fact one really needs non-commutative groups to decompose an inverse monoid M, even if the $\mathscr{J}$-classes of M are trivial.

PROPOSITION 4.6. *There exists a monoid in* **Inv** *whose* $\mathscr{J}$*-classes are trivial, which is not in* $\mathbf{J}_1 * \mathbf{Gcom}$.

The proof is based on the following lemma.

LEMMA 4.7. *Let M be an aperiodic monoid of order n in* $(\mathbf{J}_1)_S^{-1}\,\mathbf{Gcom}$. *Then for all $a, b \in M$, ab^naba^nb is idempotent.*

Proof. Since $M \in (\mathbf{J}_1)_S^{-1}\,\mathbf{Gcom}$, there exists a commutative group G (denoted additively) and a relational morphism $\tau\colon M \to G$ such that $O\tau^{-1}$ is a semilattice. Let $a, b \in M$. Then since τ is a relational morphism and since G is commutative, we have

$$(a\tau + a\tau + a^n\tau) + (b\tau + b\tau + b^n\tau) \subset (ab^n aba^n b)\,\tau. \qquad (*)$$

Now since M is an aperiodic monoid of order n, $a^n = a^{n+1}$ and $b^n = b^{n+1}$. Therefore a^n is idempotent and $a^n\tau$ is a subgroup H of G. Furthermore, $a\tau + H = a\tau + a^n\tau \subset a^{n+1}\tau = a^n\tau = H$. It follows that $g + H \subset H$ for any $g \in a\tau$ and hence $g + H = H$ since H is a finite group. Consequently $a\tau + a^n\tau = a\tau + H = H = a^n\tau$ and thus we have, by $(*)$, $(a^n\tau) + (b^n\tau) \subset (ab^n aba^n b)\,\tau$. Now $0 \in a^n\tau + b^n\tau$ and therefore $ab^n aba^n b \in O\tau^{-1}$. Since $O\tau^{-1}$ is a semilattice, $ab^n aba^n b$ is idempotent. ∎

We now prove Proposition 4.6. Let M be the syntactic monoid of the language $L = ab^*aba^*b$ over the alphabet $\{a, b\}$. If $Q = \{1, 2, 3, 4, 5\}$, M is the submonoid of $I(Q)$ generated by the partial functions a and b given by

$$1a = 2, \qquad 2a = 3, \qquad 4a = 4$$

$$2b = 2, \qquad 3b = 4, \qquad 4b = 5.$$

Thus $M \in \mathbf{Inv}$ and a calculation (or an argument of language theory, because the language L is "piecewise testable"; see [2, 5, 13]) shows that the $\mathcal{J}$-classes of M are trivial. Now since $1ab^k aba^k b = 5$ for all $k > 0$, $ab^k aba^k b$ is not idempotent and thus $M \notin (\mathbf{J}_1)_{\mathrm{S}}^{-1}\,\mathbf{Gcom}$ by the lemma. It follows that $M \notin \mathbf{J}_1 * \mathbf{Gcom}$ by Corollary 2.5. ∎

Finally, let us evoke a last unsuccessful attempt to solve the conjecture. A monoid belongs to **Inv** if it divides an inverse monoid N. Therefore it is natural to first study quotients and submonoids of inverse monoids. As is well known, quotients of inverse monoids are inverse monoids and submonoids of inverse monoids are characterized by a theorem of Schein [1] that can be formulated as follows. Let P be a subset of a monoid M. Just like for languages, the syntactic monoid of P in M is the quotient of M by the congruence $\sim_P$ defined by

$$m \sim_P n \text{ iff for all } x, y \in M,\ xmy \in P \Leftrightarrow xny \in P.$$

If $a \in M$, we set $a^{-1}P = \{x \mid ax \in P\}$. P is *strong* if for all $a, b \in M$, $a^{-1}P \cap b^{-1}P \neq \varnothing$ implies $a^{-1}P = b^{-1}P$. Then we have:

PROPOSITION 4.8. *Let P be a strong subset of M. Then the syntactic monoid of P in M is a submonoid of $I(Q)$, where $Q = \{a^{-1}P \mid a \in M$ and $a^{-1}P \neq \varnothing\}$.*

Proof. Each element m of M defines a partial function on Q by

$(a^{-1}P)\,m = (am)^{-1}\,P$ if $(am)^{-1}\,P \neq \emptyset$. As is well known, S, the syntactic monoid of P in M, is generated by those partial functions. Now if P is strong, the partial functions are (partially) one-to-one. Indeed assume that $(a^{-1}P)\,m = (b^{-1}P)\,m \neq \emptyset$. Then $(am)^{-1}\,P = (bm)^{-1}\,P \neq \emptyset$, that is, there exists $x \in M$ such that $amx \in P$ and $bmx \in P$. It follows that $mx \in a^{-1}P \cap b^{-1}P$ and thus $a^{-1}P = b^{-1}P$ since P is strong. Therefore S is a submonoid of $I(Q)$. ∎

Let $\sim$ be the congruence on M defined by $m \sim n$ iff $m \sim_P n$ for all strong subsets P of M. Then Schein's theorem can be stated as follows:

THEOREM 4.9 [17]. *A monoid M is a submonoid of an inverse monoid iff the congruence $\sim$ is the equality.*

Therefore we have

COROLLARY 4.10. *A monoid of order n is a submonoid of an inverse monoid iff it is a submonoid of $I(Q)$, where* Card $Q = n2^n$.

Proof. Let M be a submonoid of an inverse monoid and let $n = \text{Card}\, M$. Then by Theorem 4.9, $M = M/\sim$. Since $\sim$ is the intersection of all congruences $\sim_P$ such that P is strong, $M/\sim$ is a submonoid of $N = \prod_{P\ \text{strong}} M/\sim_P$. Now by Proposition 4.8, $M/\sim_P$ is a submonoid of $I(Q)$, where Card $Q \leqslant n$. Moreover if Q_1 and Q_2 are disjoint sets, $I(Q_1) \times I(Q_2)$ is a submonoid of $I(Q_1 \cup Q_2)$. It follows that N is a submonoid of $I(Q)$, where

$$\text{Card}\, Q \leqslant n\, \text{Card}\{P \mid P \text{ is strong}\} \leqslant n2^n. \quad ∎$$

Corollary 4.10 shows that one can decide whether a monoid is a submonoid of an inverse monoid. Unfortunately, this result does not suffice to solve the decision problem for **Inv**.

PROPOSITION 4.11. *There exists a monoid in* **Inv** *that is not a submonoid of an inverse monoid.*

Proof. Let M be the syntactic monoid of the language $L = \{aa, aba\}$ on the alphabet $\{a, b\}$. Then M is generated by the partial functions of $\{1, 2, 3, 4\}$ given by $1a = 2$, $2a = 3a = 4$, and $2b = 3$, and a short calculation (or, as usual, an argument of language theory [2]) shows that $M = S^1$, where S is a nilpotent semigroup. Thus $M \in \mathbf{V}$ and $M \in \mathbf{Inv}$ by Theorem 4.5. Assume that M is a submonoid of an inverse monoid. Then M is a submonoid of $I(Q)$ for some finite set Q. Since we have in M, $aa = aba \neq abab$, there exists $q \in Q$ such that $qaa = qaba \neq qabab$. Therefore $qaa = qaba \neq \emptyset$

(otherwise $qabab = \varnothing = qaba$) and hence $qa = qab \neq \varnothing$. It follows that $qaba = qabab$, a contradiction. ∎

Note added in proof. C. J. Ash has proved the main conjecture of this paper: a monoid M is in **Inv** if and only if idempotents of M commute. (Finite semigroups with commuting idempotents, *J. Austral. Math. Soc. Ser. A*, to appear.)

References

1. A. H. Clifford and G. B. Preston, "The Algebraic Theory of Semigroups," Mathematical Survey 7, Amer. Math. Soc., Providence, RI. Vol. 1 (1961), Vol. 2 (1967).
2. S. Eilenberg, "Automata, Languages and Machines," Vol. B, Academic Press, New York. 1976.
3. T. E. Hall, Injective automata, inverse semigroups and prefix codes, *Theoret. Comput. Sci.* **32** (1984), 201–213.
4. M. Keenan and G. Lallement, On certain codes admitting inverse semigroups as syntactic monoids, *Semigroup Forum* **8** (1974), 312–331.
5. G. Lallement, "Semigroups and Combinatorial Applications," Wiley, New York, 1979.
6. S. W. Margolis, On the syntactic transformation semigroup of a language generated by a finite biprefix code, *Theoret. Comput. Sci.* **21** (1982), 225–230.
7. S. W. Margolis and J. E. Pin, On varieties of rational languages and variable-length code, II, *J. Pure Appl. Algebra* **41** (1986), 233–253.
8. S. W. Margolis and J. E. Pin, Inverse semigroups and extensions of groups by semilattices. *J. Algebra* **110** (1987), 277–297.
9. S. W. Margolis and J. E. Pin, Expansions, free inverse semigroups, and Schützenberger product, *J. Algebra* **110** (1987), 298–305.
10. S. W. Margolis and J. E. Pin, Languages and inverse semigroups (Proceedings, 11th ICALP), *Lecture Notes Comput. Sci.* **172** (1984), 337–345.
11. J. F. Perrot, Codes de Brandt, *in* "Actes de l'Ecole de Printemps sur la théorie des codes" (D. Perrin, Ed.), Jougne, 1979.
12. J. E. Pin, Variétés de langages et monoïde des parties, *Semigroup Forum* **20** (1980), 11–47.
13. J. E. Pin, "Varieties of formal languages," Masson, Paris, 1984, North Oxford, London and Plenum, New York, 1986.
14. J. E. Pin, Hiérarchies de concaténation, *RAIRO Inform. Théor.* **18** (1984), 23–46.
15. J. E. Pin, Semigroupe des parties et relations de Green, *Canad. J. Math.* **36** (1984), 327–343.
16. Ch. Reutenauer, Une topologie du monoïde libre, *Semigroup Forum* **18** (1979), 33–49.
17. H. Straubing, The variety generated by finite nilpotent monoids, *Semigroup Forum* **24** (1982), 25–38.