ISRAEL JOURNAL OF MATHEMATICS **176** (2010), 139–155
DOI: 10.1007/s11856-010-0023-z

MAXIMAL SUBGROUPS OF THE MINIMAL IDEAL OF A FREE PROFINITE MONOID ARE FREE

BY

Benjamin Steinberg*

School of Mathematics and Statistics, Carleton University
1125 Colonel By Drive, Ottawa, Ontario K1S 5B6, Canada
e-mail: bsteinbg@math.carleton.ca

ABSTRACT

We answer a question of Margolis from 1997 by establishing that the maximal subgroup of the minimal ideal of a finitely generated free profinite monoid is a free profinite group. More generally, if $\mathbf{H}$ is variety of finite groups closed under extension and containing $\mathbb{Z}/p\mathbb{Z}$ for infinitely may primes p, the corresponding result holds for free pro-$\overline{\mathbf{H}}$ monoids.

1. Introduction

Margolis asked in 1997 whether the maximal subgroup of the minimal ideal of a finitely generated free profinite monoid is a free profinite group; this question first appeared in print (to the best of our knowledge) in our paper with Rhodes [13]. The question was prompted by the discovery of free profinite subgroups by Almeida and Volkov [4], who subsequently characterized those free profinite subgroups which are retracts [5]. Recently, Almeida has shown that not all maximal subgroups of finitely generated free profinite monoids are free profinite groups, although he has provided a large class of examples that are free profinite [3]. His fascinating technique involves a correspondence between symbolic dynamical systems in X^{ω} and certain $\mathscr{J}$-classes of the free profinite monoid $\widehat{X^*}$. In particular, his methods apply best to *maximal* infinite $\mathscr{J}$-classes, which correspond to *minimal* dynamical systems. The minimal ideal

* The author was supported in part by NSERC.
Received December 19, 2007 and in revised form June 30, 2008

corresponds to the full shift X^{ω} and so Almeida's approach does not yet apply to studying this maximal subgroup.

The author and Rhodes recently established that closed subgroups of free profinite monoids are projective profinite groups [14]. This answered a question raised by several people including Almeida, Margolis and Lubotzky. Projectivity is a necessary, but far from sufficient, condition for freeness [16]. In this paper we answer Margolis's question in the affirmative. We also prove the analogous result relative to certain varieties of finite groups. Recall that if $\mathbf{H}$ is a variety of finite groups, that is a class of finite groups closed under taking direct products, subgroups and quotient groups, then the class $\overline{\mathbf{H}}$ of monoids whose subgroups belong to $\mathbf{H}$ is a variety of finite monoids (a notion defined analogously to that of a variety of finite groups). Our main result is then:

Theorem 1: *Let $\mathbf{H}$ be a variety of finite groups closed under extension, which contains $\mathbb{Z}/p\mathbb{Z}$ for infinitely may primes p. Then the maximal subgroup of the minimal ideal of a finitely generated (but not procyclic) free pro-$\overline{\mathbf{H}}$ monoid is a free pro-$\mathbf{H}$ group of countable rank.*

Of course if the minimal ideal of a non-procyclic free pro-$\overline{\mathbf{H}}$ monoid were a free pro-($\overline{\mathbf{H}} \cap \mathbf{CS}$) semigroup (where $\mathbf{CS}$ denotes the variety of simple semigroups), then the above theorem would be immediate, but this is not the case as was shown by Rhodes and the author [13, Theorem 17.11].

If $\mathbf{V}$ is a variety of finite monoids, then $\widehat{F}_{\mathbf{V}}(X)$ denotes the free pro-$\mathbf{V}$ monoid generated by X. The natural projection $\pi\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to \widehat{F}_{\mathbf{H}}(X)$ restricts to an epimorphism on the maximal subgroup G of the minimal ideal of $\widehat{F}_{\overline{\mathbf{H}}}(X)$ [4,13]. Our second result describes the kernel of the epimorphism $G \twoheadrightarrow \widehat{F}_{\mathbf{H}}(X)$.

Theorem 2: *Let $\mathbf{H}$ be a variety of finite groups closed under extension, containing $\mathbb{Z}/p\mathbb{Z}$ for infinitely may primes p, and let X be a finite set of cardinality at least two. Let $\varphi\colon G \twoheadrightarrow \widehat{F}_{\mathbf{H}}(X)$ be the canonical epimorphism, where G is the maximal subgroup of the minimal ideal of $\widehat{F}_{\overline{\mathbf{H}}}(X)$. Then $\ker\varphi$ is a free pro-$\mathbf{H}$ group of countable rank.*

It seems likely that our results hold for any non-trivial extension-closed variety of finite groups. The hypothesis on primes is entirely of a technical nature and should not really be essential. For example, since projective pro-p groups are free pro-p [16], Theorems 1 and 2 are valid for $\mathbf{H}$ the variety of finite p-groups. We further propose the following conjecture.

Conjecture 3: *Under the hypotheses of Theorem 1 the maximal subgroup of the closed subsemigroup generated by the idempotents of the minimal ideal of a finitely generated (non-procyclic) free pro-*$\overline{\mathbf{H}}$ *monoid is a free pro-*$\mathbf{H}$ *group of countable rank.*

In fact, we suspect a slight variation of the construction used to prove Theorem 1 already suffices to prove the conjecture, the remaining issues being purely technical. The proof of Theorem 1 relies on a criterion for freeness, due to Iwasawa [9], and extensive usage of wreath products. In spirit the proof draws from the following sources: our previous work with Rhodes [14], the synthesis theorem [1] and the classical construction embedding any countable group as a maximal subgroup of a two-generated monoid consisting of a cyclic group of units and a completely simple minimal ideal, cf. [11].

2. Minimal ideals

In this section we collect a number of standard facts concerning minimal ideals in finite and profinite semigroups, which can be found, for instance, in [7, 10, 15]. If S is a semigroup, then $E(S)$ denotes the set of idempotents of S. For an idempotent $f \in E(S)$, the group of units G_f of the monoid fSf is called the **maximal subgroup** of S at f.

We recall for the convenience of the reader Green's relations [7, 10, 15]. Two elements s, t of a semigroup are said to be $\mathscr{J}$-related if they generate the same two-sided ideal; they are $\mathscr{L}$-related if they generate the same left ideal and $\mathscr{R}$-related if they generate the same right ideal.

The first fact we require is that every profinite monoid M has a unique minimal ideal I. It is necessarily closed and if $x \in I$, then $I = MxM$. Since every compact semigroup contains an idempotent, it follows that I contains an idempotent e. Compact semigroups are stable [15], so Green–Rees structure theory [7, 10, 15] implies that the maximal subgroup G_e is eIe and furthermore is a closed subgroup (and hence a profinite group), which is independent of the choice of e up to isomorphism.

Proposition 4: *Let* $\varphi\colon S \twoheadrightarrow T$ *be a continuous onto homomorphism of profinite monoids. Let* I *be the minimal ideal of* S *and* J *be the minimal ideal of* T*. Then* $\varphi(I) = J$ *and moreover, if* $e \in E(I)$*, then* $\varphi(G_e)$ *is the maximal subgroup of* J *at* $\varphi(e)$*.*

Proof. Clearly $\varphi^{-1}(J)$ is an ideal of S so $I \subseteq \varphi^{-1}(J)$, i.e. $\varphi(I) \subseteq J$. On the other hand $\varphi(I)$ is an ideal of T since φ is onto. Thus $\varphi(I) = J$ by minimality. Now $\varphi(G_e) = \varphi(eIe) = \varphi(e)\varphi(I)\varphi(e) = \varphi(e)J\varphi(e) = G_{\varphi(e)}$, completing the proof. ∎

In particular, every profinite group image of a profinite monoid M is an image of the maximal subgroup of its minimal ideal.

Every monoid acts on the left and right of its minimal ideal, so we are led to consider transformation monoids. By a transformation monoid (X, M) we mean a monoid M acting faithfully by transformations on the right of X with the identity acting as an identity. If (X, M) is a transformation monoid, then $\overline{(X, M)}$ denotes the augmented transformation monoid obtained by adjoining to M the constant maps on X.

Let us briefly recall the wreath product of transformation monoids [8,10,15]; our notation follows [15]. The **wreath product** $(X, M) \wr (Y, N)$ of transformation monoids (X, M) and (Y, N) is $(X \times Y, M^Y \rtimes N)$, where N acts on M^Y by $y^n f = ynf$ and the action on $X \times Y$ is given by putting $(x, y)(f, n) = (x(yf), yn)$. The wreath product is associative at the level of transformation monoids [8]. We denote by $M \wr (Y, N)$ the semidirect product $M^Y \rtimes N$.

A semigroup is called **simple** if it has no proper ideals. There is a complete description of finite simple semigroups up to isomorphism in terms of Rees matrix semigroups [7,10,15]. The minimal ideal I of a finite monoid M is a simple semigroup, and hence isomorphic to a Rees matrix semigroup $\mathscr{M}(G, A, B, C)$ where $C\colon B \times A \to G$ is the sandwich matrix [7,10,15]. Fix $a_0 \in A$ and $b_0 \in B$. Then without loss of generality we may assume that each entry of row b_0 and of column a_0 of C is the identity of G [10, 15]. We may identify G with the maximal subgroup $a_0 \times G \times b_0$.

Recall that B can be identified with the set of $\mathscr{L}$-classes of I [15]. There is a natural action of M on the right of B, as $\mathscr{L}$ is a right congruence. Let $(B, \mathsf{RLM}_I(M))$ be the associated faithful transformation monoid. Notice that each element of I acts on B as a constant map and that all constant maps on B arise from elements of I.

The Schützenberger representation [7, 10, 15] gives a wreath product representation $\rho\colon M \to G \wr (B, \mathsf{RLM}_I(M))$. An element $s = (a, g, b) \in I$ is sent to the element $(f_s, \overline{b})$ where $b' f_s = C_{b'a} g$ and $\overline{b}$ is the constant map to b. In particular, if $s = (a_0, g, b_0)$ is an element of our maximal subgroup, then $b' f_s = g$

all $b' \in B$. Consequently, the Schützenberger representation is faithful on the maximal subgroup G. It follows from the results of [15, Chapter 4, Section 7] that the Schützenberger representation of $\rho(M)$ on its minimal ideal $\rho(I)$ is faithful, a fact that is used without comment just before we state Lemma 6 below.

We recall that the finite simple semigroups form a variety of finite semigroups denoted $\mathbf{CS}$. It is well known [2,15] that $\mathbf{CS} = \mathbf{G} * \mathbf{RZ}$, that is, it consists precisely of divisors of wreath products of finite groups and right zero semigroups (semigroups satisfying the identity $xy = y$). In fact, we shall need the following more explicit lemma.

Lemma 5: *Let $S = G \wr (B, \overline{B})$ where G is a finite group and $\overline{B}$ is the semigroup of constant maps on the set B. Then S is simple and the maximal subgroup of S is isomorphic to G. More precisely, if $e = (f, \overline{b})$ is an idempotent then the map $\psi\colon eSe \to G$ given by $\psi(f', \overline{b}) = bf'$ is an isomorphism.*

Proof. We have already observed that S is simple (this can also be verified by direct computation). Let $e = (f, \overline{b})$ be an idempotent of S. We must show ψ defined as above is an isomorphism. First we verify ψ is a homomorphism. Indeed, $(f', \overline{b})(f'', \overline{b}) = (f'^{\overline{b}}f'', \overline{b})$ and $b(f'^{\overline{b}}f'') = bf'bf''$. In particular, we have $1 = \psi(e) = bf$.

To see ψ is injective, note that $(f', \overline{b}) \in G_e$ implies $(f', \overline{b}) = (f, \overline{b})(f', \overline{b}) = (f^{\overline{b}}f', \overline{b})$ and so $b'f' = b'fbf'$ all $b' \in B$. Thus f' is determined by $bf' = \psi(f', \overline{b})$ and so ψ is injective. Finally, to verify ψ is onto, let $g \in G$ and consider $(f', \overline{b}) = e(\overline{g}, \overline{b})e$ where $\overline{g}$ is the constant map $B \to G$ taking all of B to g. Then $bf' = (bf)(b\overline{g})(bf) = g$ since $bf = 1$. Thus $\psi(f', \overline{b}) = g$, establishing ψ is onto. ∎

3. The proofs of Theorems 1 and 2

In this section we prove Theorems 1 and 2 modulo a technical lemma. Fix a variety of finite groups $\mathbf{H}$ closed under extension and containing $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p. Denote by $\overline{\mathbf{H}}$ the variety of finite monoids whose subgroups belong to $\mathbf{H}$.

Proof of Theorem 1. Let $X = \{x_1, \ldots, x_n\}$ be a finite set of cardinality at least two. Denote by I the minimal ideal of $\widehat{F}_{\overline{\mathbf{H}}}(X)$. Choose an idempotent $e \in I$.

Recall that if x is an element of a profinite semigroup, then $x^\omega = \lim x^{n!}$ is the unique idempotent in the closed subsemigroup generated by x [2,15]. Without loss of generality we may assume $x_1^\omega e = e = ex_2^\omega$; if not, replace e with $(x_1^\omega e x_2^\omega)^\omega$. Let G_e be the maximal subgroup at e. Our goal is to show that G_e is free pro-**H** on a countable set of generators converging to the identity (that is, free of countable rank).

Recall that a subset Y of a profinite group G converges to the identity if each neighbourhood of the identity contains all but finitely many elements of Y. A pro-**H** group F is free pro-**H** on a subset Y converging to the identity if, given any map $\tau\colon Y \to H$ with H pro-**H** and $\tau(Y)$ converging to the identity, there is a unique continuous extension of τ to F. Any free pro-**H** group on a profinite space has a basis converging to the identity [16].

It is well-known $\widehat{F}_{\overline{\mathbf{H}}}(X)$ is metrizable [2,15], and hence so is G_e. Thus the identity e of G_e has a countable basis of neighbourhoods. We shall use a well-known criterion, going back to Iwasawa [9], to establish G_e is free pro-**H** of countable rank. An **embedding problem** for G_e is a diagram

$$\begin{tikzcd} & G_e \arrow[d, two heads, "\varphi"] \\ H \arrow[r, two heads, "\alpha"] & K \end{tikzcd} \tag{3.1}$$

with $H \in \mathbf{H}$ and φ, α epimorphisms (φ continuous). A **solution** to the embedding problem (3.1) is a continuous **epimorphism** $\widetilde{\varphi}\colon G_e \to H$ making the diagram

$$\begin{tikzcd} & G_e \arrow[dl, "\widetilde{\varphi}"'] \arrow[d, two heads, "\varphi"] \\ H \arrow[r, two heads, "\alpha"] & K \end{tikzcd}$$

commute. (The terminology "embedding problem" comes from Galois theory.) According to [16, Corollary 3.5.10], to prove G_e is free pro-**H** of countable rank it suffices to show that every embedding problem (3.1) for G_e has a solution. We proceed via a series of reductions on the types of embedding problems we need to consider. The initial reductions are nearly identical to those in [14].

So let us suppose that we have an embedding problem for G_e as per (3.1). The reader is referred to [15, Chapter 3, Section 1] for basic properties of profinite monoids and projective limits; see also [16] for the analogous results in the context of profinite groups. Let $\{M_i\}_{i\in D}$ be the inverse quotient system of all finite continuous images of $\widehat{F}_{\overline{\mathbf{H}}}(X)$. Then $\widehat{F}_{\overline{\mathbf{H}}}(X) = \varprojlim_{i\in D} M_i$. The projection $\pi_i\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to M_i$ is onto as we are dealing with an inverse quotient system. Since G_e is a closed subgroup of $\widehat{F}_{\overline{\mathbf{H}}}(X)$, it follows from basic properties of profinite spaces that $G_e = \varprojlim_{i\in D} \pi_i(G_e)$ (see [16, Corollary 1.1.8]). Since φ is an onto continuous map to a finite group it follows that φ factors through $\pi_i|_{G_i}$ for some $i \in D$ (i.e. $\ker \pi_i|_{G_e} \subseteq \ker \varphi$) [16, Lemma 1.1.16]. Setting $M' = M_i$ and $\varphi' = \pi_i$, we conclude there exists a continuous onto homomorphism $\varphi'\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \twoheadrightarrow M'$ with M' a finite monoid in $\overline{\mathbf{H}}$ such that $\ker \varphi'|_{G_e} \subseteq \ker \varphi$.

Set $K' = \varphi'(G_e)$ and let $\rho\colon K' \twoheadrightarrow K$ be the canonical projection. Defining H' to be the pullback of α and ρ, that is

$$H' = \{(h, k') \in H \times K' \mid \alpha(h) = \rho(k')\},$$

yields a commutative diagram

$$\begin{tikzcd}
 & & G_e \arrow[dl, two heads, "\varphi'"'] \arrow[ddl, two heads, "\varphi"] \\
H' \arrow[r, two heads, "\alpha'"] \arrow[d, two heads, "\rho^*"'] & K' \arrow[d, two heads, "\rho"] & \\
H \arrow[r, two heads, "\alpha"] & K &
\end{tikzcd}$$

where ρ^* is the projection to H. It is easily verified that all the arrows in the diagram are epimorphisms. So to solve our original embedding problem, it suffices to solve the embedding problem

$$\begin{tikzcd}
 & G_e \arrow[d, two heads, "\varphi'"] \\
H' \arrow[r, two heads, "\alpha'"] & K'
\end{tikzcd} \tag{3.2}$$

as the composition of a solution to (3.2) with ρ^* yields a solution to (3.1). In other words, reverting back to our original notation, we may assume in the embedding problem (3.1) that the map φ is the restriction of a continuous onto homomorphism $\varphi\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \twoheadrightarrow M$ with $M \in \overline{\mathbf{H}}$.

Let J be the minimal ideal of M; so $J = \varphi(I)$ and the group $K = \varphi(G_e)$ is the maximal subgroup of J by Proposition 4. As mentioned in Section 2, the right Schützenberger representation of M on J is faithful when restricted to K. Possibly replacing M by its image under the Schützenberger representation, we may assume that the right Schützenberger representation of M on J is faithful. Therefore, we may view M as embedded in the wreath product $K \wr (B, \mathsf{RLM}_J(M))$. The existence of a solution to (3.1) is then a consequence of the following technical lemma whose proof we defer to Section 4.

Lemma 6: *Let $\varphi\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \twoheadrightarrow M$ be a continuous surjective morphism, with M finite, such that $\varphi(G_e) = K$ and the (right) Schützenberger representation of M on its minimal ideal J is faithful. Let $\alpha\colon H \twoheadrightarrow K$ be an epimorphism. Then there is an X-generated finite monoid $M' \in \overline{\mathbf{H}}$ such that if $\eta\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to M'$ is the continuous projection, then:*

1. *there is an isomorphism $\theta\colon G_{\eta(e)} \to H$ where $G_{\eta(e)}$ is the maximal subgroup at $\eta(e)$ of the minimal ideal of M';*
2. *φ factors through η as $\rho\eta$ where $\rho\colon M' \twoheadrightarrow M$ satisfies $\rho\theta^{-1} = \alpha$.*

Assuming the lemma, our desired solution to the embedding problem (3.1) is $\widetilde{\varphi} = \theta\eta|_{G_e}\colon G_e \to H$. Indeed, $\eta|_{G_e}\colon G_e \to G_{\eta(e)}$ is an epimorphism by Proposition 4 and hence $\widetilde{\varphi}$ is an epimorphism. Moreover, $\alpha\widetilde{\varphi} = \rho\theta^{-1}\theta\eta|_{G_e} = \varphi|_{G_e}$ and so $\widetilde{\varphi}$ is indeed a solution to the embedding problem (3.1). This completes the proof of Theorem 1. ∎

Now we turn to the proof of Theorem 2.

Proof of Theorem 2. Let $\pi\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to \widehat{F}_{\mathbf{H}}(X)$ be the canonical projection and set $\varphi = \pi|_G$ where G is the maximal subgroup of the minimal ideal I of $\widehat{F}_{\overline{\mathbf{H}}}(X)$. Let $N = \ker\varphi$. We shall use a criterion due to Mel'nikov to prove that N is free pro-$\mathbf{H}$. We first need to recall the notion of S-rank [16]. If S is a finite simple group and G is a profinite group, denote by $M_S(G)$ the intersection of all open normal subgroups N of G such that $G/N \cong S$. It is known [16, Chapter 8.2] that $G/M_S(G) \cong \prod_A S$, a direct product of copies of S indexed by a set A. The cardinality of A is called the **S-rank** of G, and is denoted $r_S(G)$. One property of S-rank that we shall need is part of [16, Lemma 8.2.5].

Lemma 7: *Suppose H is a continuous image of G; then $r_S(H) \leq r_S(G)$.*

Mel'nikov's criterion for freeness of a normal subgroup [16, Theorem 8.6.8] is then:

Theorem 8 (Mel'nikov): *Let $\mathbf{H}$ be a variety of finite groups closed under extension and let F be a free pro-$\mathbf{H}$ group of countably infinite rank. A non-trivial closed normal subgroup N of infinite index in F is free pro-$\mathbf{H}$ (of countable* *rank) if and only if the S-rank $r_S(N)$ is infinite for each finite simple group $S \in \mathbf{H}$.*

In our context, since G/N is a free profinite group of rank $|X|$ clearly N has infinite index. So it suffices to show that N has infinite S-rank for all finite simple groups $S \in \mathbf{H}$. By Lemma 7 it suffices to show S^n is a continuous image of N for all $n \geq 1$ (as $r_S(S^n) = n$). Notice that $\pi(E(I)) = 1$ and so $\langle E(I)\rangle \cap G \leq N$ (one can in fact show that N is the closed normal subgroup generated by $\langle E(I)\rangle \cap G$, but we shall not need this). The desired result is then an immediate consequence of the following classical lemma, which is a essentially a piece of semigroup folklore.

Lemma 9 (Folklore): *Let S be a finite monoid and let $n \geq |S|$. Then S can be embedded in a finite monoid M with the following properties:*

(1) *The group of units $U(M)$ of M is a cyclic group of order n generated by z;*
(2) *M is generated by z and a non-identity idempotent e;*
(3) *$M \setminus U(M)$ is a Rees matrix semigroup (without zero) over S;*
(4) *$M \setminus U(M)$ is generated by its idempotents.*

The first variation of this lemma seems to be due to B. Neumann, who used a wreath product construction to embed any finite semigroup into a two-generated finite semigroup [12]. His version, however, does not have the property we need of having $M \setminus U(M)$ generated by idempotents. A version having all the properties stated above (although the last property of the lemma is not explicitly verified) can be found in [11]. Margolis commented (private communication) that the construction using Rees matrices probably goes back to J. Rhodes; a wreath product variant can be found in the paper of Arbib [6]. This lemma was motivation for why Margolis thought that G should be free: it implies that G maps onto any finite group.

From Lemma 9 we conclude every group in $\mathbf{H}$ is a continuous image of N, yielding Theorem 2. Indeed, let $A \in \mathbf{H}$ and $n \geq |A|$ with $\mathbb{Z}/n\mathbb{Z} \in \mathbf{H}$. Let M be as in the lemma where $S = A$; so $M \setminus U(M)$ is the minimal ideal J of M. As $|X| \geq 2$, M can be generated by X and if $\psi\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to M$ is the canonical surjection, then $\psi(E(I)) = E(\psi(I))$ and so, since M is finite,

$$\psi(\overline{\langle E(I)\rangle}) = \psi(\langle E(I)\rangle) = \langle \psi(E(I))\rangle = \langle E(J)\rangle = J$$

as $J = \psi(I)$ by Proposition 4 and so $E(J) = \psi(E(I))$. The idempotent-generated subsemigroup of a finite simple semigroup is simple (as simple semigroups form a variety of finite semigroups); hence the closed subsemigroup generated by the idempotents of a simple profinite semigroup is simple. Proposition 4 applied to the surjective continuous map $\psi\colon \overline{\langle E(I)\rangle} \to J$ then easily yields $\psi(N)$ is A, the maximal subgroup of J. ∎

4. The proof of Lemma 6

The proof of Lemma 6 relies heavily on the wreath product and forms the technical core of this paper. To ease notation, we shall find it convenient to use the familiar formulation of wreath products in terms of row monomial matrices. Let S be a semigroup. Then $RM_n(S)$ denotes the monoid of all $n \times n$ row monomial matrices with entries in S; in other words it consists of all matrices over $S \cup \{0\}$ such that each row has exactly one non-zero entry. The binary operation is usual matrix multiplication. It is well-known [10, 15] that $RM_n(S) \cong S \wr ([n], T_n)$, where T_n is the full transformation monoid of degree n and $[n] = \{1, \ldots, n\}$. An element (f, a) corresponds to the matrix M with $M_{i,ia} = if$, $1 \leq i \leq n$, and all other entries zero. In particular, if a is a constant map to j, then M has all its non-zero entries in column j.

From this viewpoint, an iterated wreath product $S \wr (B, T) \wr (A, U)$ can be viewed as $|A| \times |A|$ block row monomial matrices where the blocks are $|B| \times |B|$ row monomial matrices over S. The term **block entry** shall refer to a matrix from $S \wr (B, T)$ while the term **entry** shall always mean an element of the semigroup $S \cup \{0\}$. In general matrices, and in particular block entries, shall be denoted by capital letters.

Having dispensed with the preliminaries, we turn to the proof of Lemma 6. For the convenience of the reader, we restate here the lemma. In what follows recall that the idempotent e from the minimal ideal has been chosen so that $x_1^{\omega} e = e = e x_2^{\omega}$ where $X = \{x_1, \ldots, x_n\}$.

Lemma: *Let $\varphi\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \twoheadrightarrow M$ be a continuous surjective morphism, with M finite, such that $\varphi(G_e) = K$ and the (right) Schützenberger representation of M on its minimal ideal J is faithful. Let $\alpha\colon H \twoheadrightarrow K$ be an epimorphism. Then there is an X-generated finite monoid $M' \in \overline{\mathbf{H}}$ such that if $\eta\colon \widehat{F}_{\overline{\mathbf{H}}}(X) \to M'$ is the continuous projection, then:*

(1) *there is an isomorphism $\theta\colon G_{\eta(e)} \to H$ where $G_{\eta(e)}$ is the maximal subgroup at $\eta(e)$ of the minimal ideal of M';*
(2) *φ factors through η as $\rho\eta$ where $\rho\colon M' \twoheadrightarrow M$ satisfies $\rho\theta^{-1} = \alpha$.*

Proof. Let B be the set of $\mathscr{L}$-classes of J. Denote by $\mathsf{RLM}_J(M)$ the quotient of M by the kernel of its action on the right of B; note that $\mathsf{RLM}_J(M)$ contains all the constant maps. Since the Schützenberger representation of M on I is faithful, we can view M as a monoid of $b \times b$ row monomial matrices over K where $b = |B|$. Moreover, the discussion in Section 2 shows that the row monomial matrix associated to an element k of the maximal subgroup K at $\varphi(e)$ has k in every entry of the first column and 0 in the remaining columns. For $x \in \widehat{F}_{\overline{\mathbf{H}}}(X)$, denote by M_x the row monomial matrix associated to $\varphi(x)$. We shall distinguish formally between M_x and $\varphi(x)$, although $M_x = M_y$ if and only if $\varphi(x) = \varphi(y)$.

Let $N = \ker\alpha$ and choose a set-theoretic section $\sigma\colon K \to H$. Then $H = N\sigma(K)$. Denote by M_x^σ the row monomial matrix over H obtained from M_x by applying σ entry-wise. Let $n = |N|$ and let m be a positive integer such that $(M_{x_1}^\sigma)^m$ is idempotent. Choose a prime $p > \max\{m, n^b\}$ so that $\mathbb{Z}/p\mathbb{Z} \in \mathbf{H}$; such a prime exists by our assumption on $\mathbf{H}$. Denote by C_p the cyclic group of order p generated by the permutation $(1\ 2 \cdots p)$. Our monoid M' will be a certain submonoid of the iterated wreath product

$$W = H \wr (B, \mathsf{RLM}_J(M)) \wr \overline{([p], C_p)}.$$

Observe that $W \in \overline{\mathbf{H}}$ since $\mathbf{H}$ closed under extension implies that $\overline{\mathbf{H}}$ is closed under wreath product [8, 15].

We begin our construction of M' by defining

$$\widetilde{x}_1 = \begin{bmatrix} 0 & M_{x_1}^\sigma & 0 & \cdots & 0 \\ 0 & 0 & M_{x_1}^\sigma & 0 & \cdots \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 0 & M_{x_1}^\sigma \\ M_{x_1}^\sigma & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

In other words $\widetilde{x}_1$ acts on the $[p]$-component by the cyclic permutation $(1\ 2\ \cdots p)$ and each block entry of $\widetilde{x}_1$ from $H \wr (B, \mathsf{RLM}_J(M))$ is $M_{x_1}^\sigma$. Set $\ell = n^b$; so $p > \ell$ by choice of p. Let $1 = N_1, N_2, \ldots, N_\ell$ be the distinct elements of N^b. We identify N^b with the group of diagonal $b \times b$ matrices over N. In particular,

N^b is a subgroup of $H \wr (B, \mathsf{RLM}_J(M))$, as M is a monoid. In fact, there is a natural onto homomorphism

$$\overline{\alpha}\colon H \wr (B, \mathsf{RLM}_J(M)) \to K \wr (B, \mathsf{RLM}_J(M))$$

induced by $\alpha\colon H \to K$; the map $\overline{\alpha}$ simply applies α entry-wise. Moreover, it is straightforward to verify that $\overline{\alpha}(U) = \overline{\alpha}(V)$ if and only if $U = N_jV$, some $1 \leq j \leq \ell$. Indeed, if we denote by u_i (respectively v_i) the non-zero entry of row i of U (respectively V), then $\overline{\alpha}(U) = \overline{\alpha}(V)$ implies $\alpha(u_i) = \alpha(v_i)$ for all i and so we can find $n_i \in N$ such that $u_i = n_iv_i$, all i. We may then take $N_j = \operatorname{diag}(n_1, n_2, \ldots, n_b)$. Dually, $U = VN_k$, some k.

Next let us define, for $i = 2, \ldots, n$, a $p \times p$ block row monomial matrix by

$$\widetilde{x}_i = \begin{bmatrix} M^\sigma_{x_i} & 0 & \cdots & 0 \\ N_2M^\sigma_{x_i} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ N_\ell M^\sigma_{x_i} & 0 & \cdots & 0 \\ M^\sigma_{x_i} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ M^\sigma_{x_i} & 0 & \cdots & 0 \end{bmatrix}$$

so $\widetilde{x}_i$ has all its block entries in the first column. The j-th block entry of the first column is $N_jM^\sigma_{x_i}$ if $j \leq \ell$ and otherwise is $M^\sigma_{x_i}$. Then $\widetilde{x}_1, \ldots, \widetilde{x}_n \in W$ and we have a map $X \to W$ given by $x_i \mapsto \widetilde{x}_i$. Extend this to a continuous morphism $\eta\colon \widehat{F_{\overline{\mathbf{H}}}}(X) \to W$ and set $M' = \eta(\widehat{F_{\overline{\mathbf{H}}}}(X))$. Our goal is to show M' is the desired monoid. We begin by verifying that φ factors through η.

Proposition 10: *Let $u \in \widehat{F_{\overline{\mathbf{H}}}}(X)$. Then each $U \in H\wr(B, \mathsf{RLM}_J(M))$ appearing as a block entry of $\eta(u)$ satisfies $\overline{\alpha}(U) = M_u$. As a consequence $\eta(u) = \eta(u')$ implies $\varphi(u) = \varphi(u')$ and so φ factors through η as $\rho\eta$ where $\rho\colon M' \to M$ takes $\eta(u)$ to $\overline{\alpha}(U)$ where U is any block entry of $\eta(u)$.*

Proof. The second statement follows from the first since $\eta(u) = \eta(u')$ then implies $M_u = M_{u'}$ and so $\varphi(u) = \varphi(u')$.

We prove the first statement for words $u \in X^*$ by a simple induction on length, the case $|u| = 0$ being trivial. If $w = x_1u$, then the definition of $\widetilde{x}_1$ implies the block entries of $\eta(w)$ are of the form $M^\sigma_{x_1}U$ where U runs over the block entries of $\eta(u)$ and the result follows by induction as $\overline{\alpha}(M^\sigma_{x_1}U) = M_{x_1}\overline{\alpha}(U)$. The case $w = x_iu$, $2 \leq i \leq n$, is similar only the block entries of

$\eta(w)$ are now of the form $N_jM^\sigma_{x_i}U$ with U the block entry of $\eta(u)$ in the first row and $\overline{\alpha}(N_jM^\sigma_{x_i}U) = M_{x_i}\overline{\alpha}(U)$. If $u \in \widehat{F}_{\overline{\mathbf{H}}}(X)$, then since X^* is dense in $\widehat{F}_{\overline{\mathbf{H}}}(X)$ and $\eta^{-1}\eta(u), \varphi^{-1}\varphi(u)$ are open, there exists a word $w \in X^*$ such that $\eta(u) = \eta(w)$ and $\varphi(u) = \varphi(w)$, whence $M_u = M_w$. The result now follows from the case of words. ∎

Our next goal is to show that if u is a word whose support contains some letter other than x_1, then every preimage of M_u under $\overline{\alpha}$ is a block entry of $\eta(u)$. This will be crucial in showing that the maximal subgroup of the minimal ideal of M' is isomorphic to H. To effect this we shall need the following lemma. Notice that if U is any preimage of M_u, then the complete set of preimages of M_u is $\{N_1U, \ldots, N_\ell U\} = \{UN_1, \ldots, UN_\ell\}$.

Lemma 11: *Let $u, w \in \widehat{F}_{\overline{\mathbf{H}}}(X)$ and suppose $W_1, \ldots, W_\ell$ are the preimages of M_w under $\overline{\alpha}$ and U is a fixed preimage of M_u under $\overline{\alpha}$. Then $W_1U, \ldots, W_\ell U$, respectively $UW_1, \ldots, UW_\ell$, are all the preimages of M_wM_u, respectively M_uM_w, under $\overline{\alpha}$.*

Proof. The preimages of M_w under $\overline{\alpha}$ are $W_i = N_iM^\sigma_w$, $1 \leq i \leq \ell$. But as M^σ_wU is an $\overline{\alpha}$-preimage of M_wM_u, it follows that

$$\{W_iU \mid 1 \leq i \leq \ell\} = \{N_iM^\sigma_wU \mid 1 \leq i \leq \ell\}$$

is the complete set of preimages of M_wM_u under $\overline{\alpha}$, as required. For the preimages of M_uM_w, note that $UW_i = UN_iM^\sigma_w$ and $UN_1, \ldots, UN_\ell$ are the $\overline{\alpha}$-preimages of M_u. Therefore, the previous case applies to prove that the UW_i, $1 \leq i \leq \ell$, form the complete set of preimages of M_uM_w. ∎

Observe that if $w \in X^*$ and the support of w is not contained in $\{x_1\}$, then by definition of $\widetilde{x}_2, \ldots, \widetilde{x}_n$, the block entries of $\eta(w)$ form a single column, that is the $\overline{([p], C_p)}$-component of $\eta(w)$ is a constant map. We can now prove the aforementioned fact concerning preimages.

Proposition 12: *Let $w \in X^*$ have support not contained in $\{x_1\}$. Then each preimage of M_w under $\overline{\alpha}$ appears as a block entry of $\eta(w)$.*

Proof. Let S be the set of words in X^* with support containing an element outside of $\{x_1\}$. We proceed by induction on $|w|$ for $w \in S$. If $|w| = 1$, then the proposition follows from the definition of $\widetilde{x}_2, \ldots, \widetilde{x}_n$.

Suppose it is true for words in S of length n and let $w \in S$ have length $n+1$. If the first letter of $w \neq x_1$, then $w = ux_i$ with $u \in S$, some i; else $w = x_1u$ where $u \in S$. In the case $w = x_1u$ the block entries of $\eta(w)$ are precisely the products of the form $M^{\sigma}_{x_1}U$ where U runs over the block entries of $\eta(u)$. By induction and Lemma 11 it follows that the block entries of $\eta(w)$ run over all the preimages of M_w under $\overline{\alpha}$. In the case $w = ux_i$, the block entries of $\eta(u)$ are in a single column, say column j. Let V be the block entry in row j of $\widetilde{x}_i$; by construction it is an $\overline{\alpha}$-preimage of M_{x_i}. Then the block entries of $\eta(w)$ are all products of the form UV where U is a block entry of $\eta(u)$. As U runs over all preimages of M_u by induction, Lemma 11 yields that each $\overline{\alpha}$-preimage of M_w is a block entry of $\eta(w)$. This completes the proof. ∎

A continuity argument allows us to extend the above result beyond words.

Corollary 13: *If $w \in I$, then the block entries of $\eta(w)$ are in a single column and each preimage under $\overline{\alpha}$ of M_w appears as a block entry of $\eta(w)$.*

Proof. Since $\overline{\mathbf{H}}$ contains the free semilattice $(P(X), \cup)$ it follows that if $\{w_r\}$ is a sequence of words in X^* converging to w, then there exists $R > 0$ such that, for $r \geq R$, the word w_r has support X. The monoid M' is finite so there exists $s \geq R$ with $\eta(w) = \eta(w_s)$ by continuity of η. Remembering that $\varphi = \rho\eta$, this implies that $\varphi(w) = \varphi(w_s)$, or equivalently that $M_w = M_{w_s}$. Since w_s has full support, the corollary now follows from Proposition 12 and the remark preceding that proposition applied to w_s. ∎

By Corollary 13 if $w \in I$, then the $\overline{([p], C_p)}$-component of $\eta(w)$ is a constant map, that is the block entries of $\eta(w)$ appear in a single column. Moreover, Proposition 10 shows that each block entry of $\eta(w)$ is a preimage of M_w under $\overline{\alpha}$. But $\varphi(w)$ belongs to the minimal ideal of M and so M_w has the shape of a constant map, i.e. it has only one non-zero column. Hence $\eta(w)$ has all its entries in a single column, that is, the $(B, \mathsf{RLM}_J(M)) \wr \overline{([p], C_p)}$-component of $\eta(w)$ is a constant map. Since $\eta(I)$ is the minimal ideal J' of M' (Proposition 4), we conclude $J' \subseteq M' \cap H \wr (B \times [p], \overline{B \times [p]})$. By Lemma 5 the semigroup $H \wr (B \times [p], \overline{B \times [p]})$ is simple and hence (recalling that simple semigroups form a variety of finite semigroups) $M' \cap H \wr (B \times [p], \overline{B \times [p]})$ is simple. Therefore, we in fact have $J' = M' \cap H \wr (B \times [p], \overline{B \times [p]})$ (since J' is an ideal of M' and hence of any subsemigroup of M'). It remains to construct an isomorphism $\theta\colon G_{\eta(e)} \to H$ such that $\rho\theta^{-1} = \alpha$.

First note that since $ex_2^\omega = e$, it must be the case that $\eta(e)$ is a block matrix with each block entry in the first column. Also, the discussion in Section 2 indicates M_e is a matrix whose only non-zero column is the first column and whose non-zero entries are comprised by the identity of K. Since the block entries of $\eta(e)$ are preimages of M_e under $\overline{\alpha}$ (Proposition 10), we deduce that all the non-zero entries of $\eta(e)$ are in the first column and belong to N. Lemma 5 says the map $\Theta\colon H \wr (B \times [p], \overline{B \times [p]}) \to H$ selecting the $1,1$ entry is an isomorphism from the maximal subgroup at $\eta(e)$ of $H \wr (B \times [p], \overline{B \times [p]})$ to H. In particular, $\eta(e)_{11}$ is the identity of H. We shall show that the restriction θ of Θ to $G_{\eta(e)}$ is onto and $\rho\theta^{-1} = \alpha$. This will require a little preparation.

Proposition 14: *If $u \in G_e$, then $\varphi(u) = \alpha(\eta(u)_{11})$.*

Proof. Corollary 13 implies that all the block entries of $\eta(u)$ are in a single column. In fact, they are all in the first column since we just saw that this is the case for $\eta(e)$ and $\eta(u) = \eta(u)\eta(e)$. Proposition 10 implies that M_u is the matrix obtained by choosing any block entry of $\eta(u)$ and applying $\overline{\alpha}$. In particular, M_u is the result of applying α entry-wise to the $1,1$ block entry of $\eta(u)$ and so $[M_u]_{11} = \alpha(\eta(u)_{11})$.

Now if $k \in K$, then according to first paragraph of the proof of Lemma 6 the row monomial matrix associated to k has all its non-zero entries in the first column and each of these entries is k. As $\varphi(u) \in K$, it follows that M_u has $\varphi(u)$ in all its entries of the first column; in particular, $[M_u]_{11} = \varphi(u)$. The last statement of the previous paragraph then yields $\varphi(u) = \alpha(\eta(u)_{11})$, as required. ∎

The proposition admits the following corollary.

Corollary 15: *The equality $\alpha\theta = \rho$ holds.*

Proof. Recalling that θ selects the $1,1$ entry of an element of $G_{\eta(e)}$, Proposition 14 shows that $\varphi = \alpha\theta\eta$ as maps from G_e to K. By definition of ρ there is a factorization $\varphi = \rho\eta$ and hence, in fact, $\rho\eta = \alpha\theta\eta\colon G_e \to K$. But $\eta|_{G_e}$ is onto, so we conclude that $\rho = \alpha\theta$ as was to be proved. ∎

Since θ is injective, being a restriction of the isomorphism Θ, Corollary 15 immediately yields that if θ is onto, then $\alpha = \rho\theta^{-1}$. Thus we are left with proving θ is onto. Since ρ must take $G_{\eta(e)}$ onto K (Proposition 4), it follows from Corollary 15 that α maps $\theta(G_{\eta(e)})$ onto K. Setting $\ker\alpha = N$, it follows

$H = N\theta(G_{\eta(e)})$ and so to complete the proof it suffices to establish that N is contained in the image of θ.

Recall that our prime p was chosen so that $p > m$ where $(M^{\sigma}_{x_1})^m = (M^{\sigma}_{x_1})^{\omega}$. We can thus find a positive integer r so that $1 \equiv rm \bmod p$. Then

$$\widetilde{x}_1^{mr} = \begin{bmatrix} 0 & (M^{\sigma}_{x_1})^{\omega} & 0 & \cdots & 0 \\ 0 & 0 & (M^{\sigma}_{x_1})^{\omega} & 0 & \cdots \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 0 & (M^{\sigma}_{x_1})^{\omega} \\ (M^{\sigma}_{x_1})^{\omega} & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Set $C = \widetilde{x}_1^{mr}$. Then C^j has the block form of the permutation matrix corresponding to $(1\ 2\ \cdots p)^j$ and each block entry of C^j is $(M^{\sigma}_{x_1})^{\omega}$. In particular, the effect of multiplying a matrix D on the left by C^j is to permute the rows of D according to the permutation $(1\ 2\ \cdots p)^j$ and to multiply each row of D on the left by $(M^{\sigma}_{x_1})^{\omega}$.

Corollary 13 tells us that each preimage of M_e under $\overline{\alpha}$ appears as a block entry U of $\eta(e)$. From the assumption that $x_1^{\omega}e = e$, it is immediate that $M^{\omega}_{x_1}M_e = M_e$. Since $\overline{\alpha}((M^{\sigma}_{x_1})^{\omega}) = M^{\omega}_{x_1}$, it follows from Lemma 11 and the first sentence of this paragraph that the elements of the form $(M^{\sigma}_{x_1})^{\omega}U$, where U runs over the block entries of $\eta(e)$, yield all the preimages of M_e under $\overline{\alpha}$ (with perhaps some repetition). Each such matrix is the $1,1$ block entry of a product $C^j\eta(e)$ for a correctly chosen j as $(1\ 2\ \cdots p)$ acts transitively on $\{1,\ldots,p\}$ and all the block entries of $\eta(e)$ are in the first column.

Since M_e is a matrix whose first column consists entirely of the identity of K (and the remaining columns are zero columns) it follows that the $\overline{\alpha}$-preimages of M_e are precisely those matrices with first column having entries from $N = \ker\alpha$ and whose remaining columns consist of zeroes. Consequently any element of N can be the $1,1$ entry of an $\overline{\alpha}$-preimage of M_e and so every element $h \in N$ is $[C^j\eta(e)]_{11}$ for some j. Since $\eta(e)_{11}$ is the identity of H, it follows $\eta(e)C^j\eta(e)$ is an element of $G_{\eta(e)}$ with $1,1$ entry h and so $\theta(\eta(e)C^j\eta(e)) = h$. Thus $\theta(G_{\eta(e)})$ contains N as required. This completes the proof of Lemma 6, thereby establishing Theorems 1 and 2. ∎

Acknowledgments. I am grateful to the referee for a number of helpful suggestions that have improved the readability of this paper.

References

[1] D. Allen, Jr. and J. Rhodes, *Synthesis of classical and modern theory of finite semigroups.* Advances in Mathematics **11** (1973), 238–266.

[2] J. Almeida, *Finite semigroups and universal algebra*, Volume 3 of *Series in Algebra.* World Scientific Publishing Co. Inc., River Edge, NJ, 1994. Translated from the 1992 Portuguese original and revised by the author.

[3] J. Almeida, *Profinite groups associated with weakly primitive substitutions*, Fundamental'naya i Prikladnaya Matematika **11** (2005), 13–48. Translation in Journal of Mathematical Sciences (N.Y.) **144** (2007), 3881–3903.

[4] J. Almeida and M. V. Volkov, *Profinite identities for finite semigroups whose subgroups belong to a given pseudovariety*, Journsl of Algebra and its Applications **2** (2003), 137–163.

[5] J. Almeida and M. V. Volkov. *Subword complexity of profinite words and subgroups of free profinite semigroups*, International Journal of Algebra and Computation **16** (2006), 221–258.

[6] M. Arbib, *The automata theory of semigroup embeddings*, Journal of the Australian Mathematical Society **8** (1968), 568–570.

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

[8] S. Eilenberg, *Automata, Languages, and Machines. Vol. B*, Academic Press, New York, 1976. With two chapters ("Depth decomposition theorem" and "Complexity of semigroups and morphisms") by Bret Tilson, Pure and Applied Mathematics, Vol. 59.

[9] K. Iwasawa, *On solvable extensions of algebraic number fields*, Annals of Mathematics (2) **58** (1953), 548–572.

[10] K. Krohn, J. Rhodes and B. Tilson, in *Algebraic Theory of Machines, Languages, and Semigroups* (Michael A. Arbib, ed.) With a major contribution by Kenneth Krohn and John L. Rhodes. Academic Press, New York, 1968, Chapters 1, 5–9.

[11] S. Margolis, *Maximal pseudovarieties of finite monoids and semigroups*, Izvestiya Vysshikh Uchebnykh Zavedeniĭ Matematika (1) (1995), 65–70. Translation in Russian Math. (Iz. VUZ) **39** (1995), 60–64.

[12] B. H. Neumann, *Embedding theorems for semigroups*, Journal of the London Mathematical Society **35** (1960), 184–192.

[13] J. Rhodes and B. Steinberg, *Profinite semigroups, varieties, expansions and the structure of relatively free profinite semigroups*, International Journal of Algebra and Computation **11** (2001), 627–672.

[14] J. Rhodes and B. Steinberg, *Closed subgroups of free profinite monoids are projective profinite groups*, The Bulletin of the London Mathematical Society **40** (2008), 375–383.

[15] J. Rhodes and B. Steinberg, *The $\mathfrak{q}$-Theory of Finite Semigroups*, Springer Monographs in Mathematics, Springer, New York, 2009.

[16] L. Ribes and P. Zalesskii, *Profinite Groups*, Volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*, Springer-Verlag, Berlin, 2000.