RATIONAL CODES AND FREE PROFINITE MONOIDS

JORGE ALMEIDA AND BENJAMIN STEINBERG

Abstract. It is well known that clopen subgroups of finitely generated free profinite groups are again finitely generated free profinite groups. Clopen submonoids of free profinite monoids need not be finitely generated nor free. Margolis, Sapir and Weil proved that the closed submonoid generated by a finite code (which is in fact clopen) is a free profinite monoid generated by that code. In this note we show that a clopen submonoid is free profinite if and only if it is the closure of a rational free submonoid. In this case its unique closed basis is clopen, and is in fact the closure of the corresponding rational code. More generally, our results apply to free pro-$\overline{\mathbf{H}}$ monoids for $\mathbf{H}$ an extension-closed pseudovariety of groups.

1. Introduction

Reiterman [15] showed that pseudovarieties of finite algebras can be defined by pseudoidentities, which are formal equalities between elements of free profinite algebras. In order to fruitfully use the language of pseudoidentities, it becomes important to understand free profinite algebras. Intensive research on profinite monoids began in the late 1980s and has not let up since, see for instance [1–6, 10, 16, 17, 20, 22].

It is well known that clopen subgroups of finitely generated free profinite groups are again finitely generated free profinite groups [19, 23]. In general, the closed subgroups of such groups are precisely the projective profinite groups [19, 23]. It is then natural to ask about the situation for finitely generated free profinite monoids. Since not all submonoids of free monoids are free, one cannot expect all clopen submonoids of free profinite monoids to be free.

The first author asked in his book [1] whether a free profinite monoid on two generators contains a copy of a free profinite monoid on an arbitrary finite number of generators. This was answered positively by Koryakov [11], who showed that the prefix code $C_n = \{y, xy, \ldots, x^{n-1}y\}$ freely generates

Date: Version of May 24, 2008.

Key words and phrases. free profinite monoids, profinite topologies, codes, automata, wreath products.

The first author was partially supported by the Centro de Matemática da Universidade do Porto, financed by FCT through the programmes POCTI and POSI, with Portuguese and European Community structural funds, and by the FCT project PTDC/MAT/65481/2006. The second author gratefully acknowledges the support of an NSERC discovery grant.

a free (clopen) profinite submonoid of $\widehat{\{x,y\}^*}$. Margolis, Sapir and Weil showed more generally [13] that if A is a finite set, then any finite code in A^* freely generates a free profinite (clopen) submonoid of $\widehat{A^*}$. Here we recall that a subset of a free monoid is called a code if it is a basis for a free submonoid.

On the other hand, it is easy to see that $\{x^2, x^3\}$ generates a clopen submonoid of $\widehat{\{x\}^*}$ that is not free (or even projective) since it is commutative and not one-generated. Our results will imply that the infinite prefix code x^*y generates a free profinite submonoid of $\widehat{\{x,y\}^*}$ that is not finitely generated, nor is it freely generated by the discrete set x^*y.

Our main result is a complete characterization of free clopen submonoids of finitely generated free profinite monoids. They are shown to be precisely the closures of free rational submonoids and their unique closed free generating sets are the closures of the associated rational codes. More generally, our results hold for free pro-$\overline{\mathbf{H}}$ monoids where $\mathbf{H}$ is an extension-closed pseudovariety of groups. Our original motivation for this work was to try and establish that every closed subgroup of a free profinite monoid is a projective profinite group. This has recently been proved by Rhodes and the second author [17].

Our techniques generalize those of the case of free groups [19, 23], properly reinterpreted, and the case of finite codes [13]. The key new ingredients are due to topological considerations. The paper is organized as follows. First we review some background material on codes, automata and monoids. We also establish a new result about rational codes and unambiguous automata, generalizing a result of Le Rest and Le Rest [12], which may be of independent interest. Next we recall the pro-$\mathbf{V}$ uniformity on a monoid for a pseudovariety $\mathbf{V}$. We then show how wreath products can be used to give a simple conceptual proof of the result about clopen subgroups of free profinite groups. In the final section we prove our main theorem.

2. Codes, automata and monoids

We briefly recall some basic facts about free monoids. Proofs and details can be found in Berstel-Perrin [7]. If A is a set, A^* denotes the free monoid generated by A; we shall use ε to denote the empty string. If $X \subseteq A^*$, then — abusively — X^* denotes the submonoid of A^* generated by X. When possible confusion could arise we shall write $X^* \leq A^*$ to emphasize that X^* is taken within A^*. The operation $X \mapsto X^*$ is called the *Kleene star*.

A subset R of A^* is called *rational* if it can be built up from the finite subsets of A^* by finitely many applications of the operations of union, (set-wise) product and Kleene star. Equivalently, these are the subsets recognized by finite automata [7, 9]. A *finite automaton* $\mathscr{A} = (Q, A, \delta, \iota, F)$ over the alphabet A consists of a finite set Q of states, an initial state $\iota \in Q$, a subset $\delta \subseteq Q \times A \times Q$ and a set of final states $F \subseteq Q$. One views an automaton as a labelled directed graph with vertex set Q. There is an edge $q \xrightarrow{a} q'$

from q to q' labelled by a if $(q, a, q') \in \delta$. The subset of A^* *recognized* (or *accepted*) by $\mathscr{A}$ is the set of all words labelling a path from ι to an element of F. Sometimes we write $(q, a, q') \in \mathscr{A}$ to mean that $(q, a, q') \in \delta$.

An automaton is termed *deterministic*[1] if each vertex has exactly one edge labelled by each letter of A emanating from it. In this case, given any state $q \in Q$ and word $w \in A^*$, there is a unique state, denoted qw, that can be reached from q by a path labelled by w. An automaton is called *unambiguous* if each pair of states p, q and each word $w \in A^*$, there is at most one path labelled by w from p to q. Clearly deterministic automata are unambiguous, but not conversely. Every rational subset of A^* is recognized by a unique minimal deterministic finite automaton [7, 9]. An automaton is called *trim* if every state is accessible from the initial state and every state can reach a final state. The *trim part* of an automaton is the automaton obtained by first removing all inaccessible states and then removing all states that cannot reach a final state.

Let Q be a finite indexing set and let $M_Q(\mathbb{Q})$ denote the monoid of $Q \times Q$-matrices over the rational numbers. A submonoid M of $M_Q(\mathbb{Q})$ is called an *unambiguous matrix monoid* if it consists of $0, 1$-matrices such that additions are never performed when multiplying two elements of M. For instance the group of permutation matrices is unambiguous, as is the monoid of row monomial matrices. A matrix representation of a monoid is called *unambiguous* if its image is an unambiguous matrix monoid. Of course any unambiguous matrix monoid is finite. The notion of an unambiguous matrix monoid and its relationship with free monoids is due to Schützenberger; see [7].

If $\mathscr{A} = (Q, A, \delta, \iota, F)$ is an automaton, then the associated matrix representation of A^* is the homomorphism $\rho : A^* \to M_Q(\mathbb{Q})$ given on $a \in A$ by

$$(\rho(a))_{p,q} = \begin{cases} 1 & \exists p \xrightarrow{a} q \in \mathscr{A} \\ 0 & \text{else.} \end{cases}$$

It is well known [7] that $\mathscr{A}$ is unambiguous if and only if the associated matrix representation is unambiguous. In this case, for a general word, $w \in A^*$, $(\rho(w))_{p,q} = 1$ if w labels a path from p to q and is 0 otherwise. The image of ρ is a finite unambiguous submonoid of $M_Q(\mathbb{Q})$, denoted $M(\mathscr{A})$, and called the *transition monoid* of $\mathscr{A}$.

If $L \subseteq A^*$ is a rational language, then there is a finite monoid $M(L)$ and a surjective homomorphism $\eta_L : A^* \to M(L)$ such that:

- $\eta_L^{-1}(\eta_L(L)) = L$;
- if $\psi : A^* \to M$ is any surjective homomorphism to a monoid M such that $\psi^{-1}(\psi(L)) = L$, then $\eta_L = \alpha\psi$ for a unique (necessarily surjective) homomorphism $\alpha : M \to M(L)$.

[1]Some authors use the word deterministic to mean that at most one edge labelled by each letter of A emanates from each vertex.

One calls $M(L)$ the *syntactic monoid* of L and it is the quotient of A^* by the congruence identifying x and y if, for all $u, v \in A^*$,

$$uxv \in L \iff uyv \in L \tag{2.1}$$

see [7, 9] for details. In particular, if L is accepted by an unambiguous automaton $\mathscr{A}$ with associated matrix representation ρ, then $\eta_L = \alpha\rho$ for a unique surjective homomorphism $\alpha : M(\mathscr{A}) \to M(L)$.

A monoid M is said to *divide* a monoid N, written $M \prec N$, if M is a quotient of a submonoid of N. By a subgroup of a monoid M, we mean a subsemigroup which is algebraically a group (we allow the subgroup to have a different identity than M). It is well known that any group divisor of a monoid M divides a subgroup of M [9, 18]. A *pseudovariety* $\mathbf{V}$ of monoids is a class of finite monoids closed under direct product such that $N \in \mathbf{V}$ and $M \prec N$ implies $M \in \mathbf{V}$. If $e \in M$ is an idempotent (meaning $e^2 = e$), then the group of units G_e of the monoid eMe is called the *maximal subgroup* of M at e; it is the largest subgroup of M with identity e. If $\mathbf{H}$ is a pseudovariety of groups (that is a pseudovariety of monoids consisting entirely of groups), then the class $\overline{\mathbf{H}}$ of all monoids whose subgroups belong to $\mathbf{H}$ is a pseudovariety. For instance, when $\mathbf{H}$ is the trivial pseudovariety, then $\overline{\mathbf{H}}$ is the pseudovariety of aperiodic monoids; if $\mathbf{G}$ is the pseudovariety of all group, then $\overline{\mathbf{G}}$ is the pseudovariety $\mathbf{M}$ of all finite monoids. A group G is said to be an *extension* of a group K by a group H if K is a normal subgroup of G and $G/K \cong H$. A pseudovariety of groups $\mathbf{H}$ is said to be *extension-closed* if whenever G is an extension of K by H with $K, H \in \mathbf{H}$, then $G \in \mathbf{K}$.

If $\mathbf{V}$ is a pseudovariety of monoids, then a rational subset $L \subseteq A^*$ is said to be $\mathbf{V}$-*recognizable* if $M(L) \in \mathbf{V}$. The collection of $\mathbf{V}$-recognizable subsets of A^* is a Boolean algebra [9]. A subset is rational if and only if it is $\mathbf{M}$-recognizable.

If $M \subseteq M_Q(\mathbb{Q})$ is an unambiguous matrix monoid and S is a monoid, then the *unambiguous wreath product* $S \wr M$ is the monoid of all $Q \times Q$-matrices over S obtained from matrices in M by replacing non-zero entries by elements of S. Because M is unambiguous, no additions are required when multiplying these matrices and so $S \wr M$ is well defined. See [14, 21] for details on this construction.

It is known that a pseudovariety of groups $\mathbf{H}$ is extension-closed if and only if it is closed under wreath products [9, 18]. More generally, if $\mathbf{H}$ is extension-closed and $S, M \in \overline{\mathbf{H}}$, then $S \wr M \in \overline{\mathbf{H}}$; see [21].

A subset $C \subseteq A^*$ is called a *code* if $C^* \leq A^*$ is a free submonoid of A^* with basis C. In general, a submonoid $M \leq A^*$ has unique minimal generating set, denoted $\min(M)$, namely $(M \setminus \varepsilon) \setminus (M \setminus \varepsilon)^2$. One has that M is free if and only if $\min(M)$ is a code [7]. Notice that a submonoid M of A^* is rational if and only if $\min(M)$ is rational; in particular, free rational submonoids are precisely the submonoids generated by rational codes. This last remark relies on the fact that rational subsets are closed under taking

complements [7, 9]. If $\mathbf{V}$ is a pseudovariety of monoids, then we shall call a code C a $\mathbf{V}$-*code* if C^* is $\mathbf{V}$-recognizable. Notice that if C is a $\overline{\mathbf{H}}$-code for an extension-closed pseudovariety of groups $\mathbf{H}$, then C is also $\overline{\mathbf{H}}$-recognizable. Indeed, it is well known that the collection of $\overline{\mathbf{H}}$-recognizable sets is closed under concatenation [9, 18]. Since any finite set is $\overline{\mathbf{H}}$-recognizable, it follows that if $M \subseteq A^*$ is any $\overline{\mathbf{H}}$-recognizable submonoid, then $\min(M)$ is also $\overline{\mathbf{H}}$-recognizable.

The simplest example of a code is a prefix code. A subset $P \subseteq A^*$ is a *prefix code* if no two elements of P are comparable in the prefix order. It is immediate to verify that prefix codes are indeed codes. The codes C_n considered in the introduction are finite prefix codes, while x^*y is an infinite rational prefix code. One can show that a submonoid M of A^* is freely generated by a rational prefix code if and only if A^* acts on the right of a finite set X with M the stabilizer of a point [7]. More generally, a submonoid M of A^* is freely generated by a rational code if and only if there is an unambiguous representation $\varphi : A^* \to M_Q(\mathbb{Q})$ such that there is an element $q \in Q$ with the property that $M = \{w \in A^* \mid (\rho(w))_{q,q} = 1\}$ [7].

We shall make use of a well-known construction [7, Chapter IV] for recognizing submonoids generated by codes. Let $\mathscr{A} = (Q, A, \delta, \iota, F)$ be an unambiguous automaton recognizing a code C. Now define

$$\mathscr{B} = (Q \cup \{\Phi\}, A, \Delta, \Phi, \{\Phi\})$$

where $\Phi \notin Q$. The set Δ of edges of $\mathscr{B}$ are those from $\mathscr{A}$ together with:

- $\mathscr{I} = \{\Phi \xrightarrow{a} q \mid \iota \xrightarrow{a} q \in \mathscr{A}, a \in A\}$;
- $\mathscr{T} = \{q \xrightarrow{a} \Phi \mid q \xrightarrow{a} t \in \mathscr{A}, a \in A, t \in F\}$;
- $\mathscr{O} = \{\Phi \xrightarrow{a} \Phi \mid a \in A \cap C\}$.

We set $\mathscr{A}^*$ equal to the trim part of $\mathscr{B}$. One obtains from [7, Chapter IV, Propositions 1.4 and 1.5] that $\mathscr{A}^*$ is an unambiguous automaton recognizing C^* provided that, for each $c \in C$, there is a *unique* state $t \in F$ such that c labels a path from ι to t. This is the case, for instance, when $\mathscr{A}$ is deterministic.

The following technical theorem generalizes a result of Le Rest and Le Rest on finite codes [12]. It seems likely to be of interest in its own right.

Theorem 2.1. *Let $\mathscr{A} = (Q, A, \delta, \iota, F)$ be a finite unambiguous automaton recognizing a rational code C such that, for each $c \in C$, there is a unique state $t \in F$ so that c labels a path from ι to t. Then each subgroup of $M(\mathscr{A}^*)$ is an extension of a divisor of a direct power of $M(\mathscr{A})$ by a subgroup of $M(C^*)$.*

Proof. Let $\alpha : M(\mathscr{A}^*) \to M(C^*)$ be the canonical projection. Let e be an idempotent of $M(\mathscr{A}^*)$ and put $K = \ker \alpha|_{G_e}$. We show that K divides a power of $M(\mathscr{A})$. Recall that $M(\mathscr{A}^*) \subseteq M_X(\mathbb{Q})$ is an unambiguous matrix monoid where X is the set of states of $\mathscr{A}^*$. Set

$$S = \mathrm{Fix}(e) = \{q \in X \mid e_{q,q} = 1\}.$$

By [7, Proposition 3.4] G_e acts faithfully by permutations of S by setting $sg = t$ if $g_{s,t} = 1$ for $s, t \in S$ and $g \in G_e$. We denote by ρ the projection $A^* \to M(\mathscr{A}^*)$; notice that $\eta_{C^*} = \alpha\rho$.

Claim 1. The set $S \setminus \{\Phi\}$ is invariant under the action of K.

Proof. If $\Phi \notin S$, then there is nothing to prove. So assume $\Phi \in S$. Let us suppose $s \in S\setminus\{\Phi\}$ and $sg = \Phi$ some $g \in K$. Choose $v, w \in A^*$ with $\rho(v) = e$ and $\rho(w) = g$. Then $s\rho(v) = se = s$, $\Phi\rho(v) = \Phi e = \Phi$ and $s\rho(w) = sg = \Phi$. (The reader should draw a picture.) Choose $u \in A^*$ with $\rho(u) = g^{-1}$. Then $\Phi\rho(u) = \Phi g^{-1} = sgg^{-1} = s$ and so $\Phi\rho(uw) = \Phi$, from which we conclude $uw \in C^*$. But $\alpha(e) = \alpha(g)$ implies $\eta_{C^*}(v) = \eta_{C^*}(w)$ and so $uw \in C^*$ implies $uv \in C^*$ by the definition of the syntactic congruence, see (2.1). It follows that $\rho(uv)_{\Phi,\Phi} = 1$ since $\mathscr{A}^*$ accepts C^*. But $\rho(uv) = g^{-1}e = g^{-1}$ and hence, since $\Phi, s \in S$, we have $s = \Phi g^{-1} = \Phi\rho(uv) = \Phi$. This contradiction establishes the claim. □

Let $\mathscr{O}_1, \ldots, \mathscr{O}_s$ be the orbits of K on S and let K_i be the quotient of K by the kernel of its action on $\mathscr{O}_i$. Since K acts faithfully on S, it is immediate that K is a subdirect product of the K_i. Therefore, to prove the theorem it suffices to show that each K_i divides $M(\mathscr{A})$. Since the orbit of Φ is trivial if $\Phi \in S$ (by Claim 1), it suffices to consider the other orbits. For the remainder of this proof we write $q \xrightarrow{u} q'$ to indicate $\rho(u)_{q,q'} = 1$.

Claim 2. Suppose $\mathscr{O}_i \neq \{\Phi\}$ is an orbit of K such that some element $g \in K_i$ is of the form $\rho(u)$ with $u \in A^*$ such that there are $s, s' \in \mathscr{O}_i$ with $sg = s'$ and a factorization $u = u'u''$ with $s \xrightarrow{u'} \Phi \xrightarrow{u''} s'$. Then K_i is trivial.

Proof. First we establish that there is a word $w \in A^*$ with $\rho(w) = e$ such that for all $q \in \mathscr{O}_i$ we can factor $w = w'_q w''_q$ where $q \xrightarrow{w'_q} \Phi \xrightarrow{w''_q} q$. Indeed, fixing q choose $h \in K_i$ such that $qh = s$ and let $v_q \in A^*$ with $\rho(v_q) = h$. Then we have

$$q \xrightarrow{v_q} s \xrightarrow{u'} \Phi \xrightarrow{u''} s' \tag{2.2}$$

with $\rho(v_q u'u'') = \rho(v_q u) = hg \in K_i$. Choose $x \in A^*$ so that $\rho(x) = (hg)^{-1}$. Then from $s'(hg)^{-1} = q(hg)(hg)^{-1} = qe = q$, we obtain $s' \xrightarrow{x} q$. Let $w_q = v_q u x$. Then $\rho(w_q) = e$ and the circuit at q labelled by w_q in $\mathscr{A}^*$ goes through Φ by (2.2). Since $q'e = q'$ for all $q' \in S$, it follows from the unambiguity of $\mathscr{A}^*$ that the word $w = w_{q_1} \cdots w_{q_m}$, where $\mathscr{O}_i = \{q_1, \ldots, q_m\}$, has the desired property.

We now use w to show that, in fact, K_i is trivial. Let $g \in K_i$ and suppose $\rho(v) = g$. Then $\eta_L(v) = \alpha(g) = \alpha(e) = \eta_L(w)$. Suppose now that $p \in \mathscr{O}_i$ and put $q = pg$. We must show that $p = q$. Since $\rho(wvw) = ege = g$, it follows that wvw labels a path from p to q in $\mathscr{A}^*$. Since $pe = p$ and $qe = q$, there are paths $p \xrightarrow{w} p$ and $q \xrightarrow{w} q$. Also we have $p \xrightarrow{v} q$. So by unambiguity of $\mathscr{A}^*$, the path from p to q labelled by wvw is the composition

$p \xrightarrow{w} p \xrightarrow{v} q \xrightarrow{w} q$. By choice of w, we can factor $w = w_1w_2$ and $w = w_3w_4$ so that

$$p \xrightarrow{w_1} \Phi \xrightarrow{w_2} p \quad \text{and} \quad q \xrightarrow{w_3} \Phi \xrightarrow{w_4} q.$$

(Again the reader should draw a picture.) Then $\Phi \xrightarrow{w_2} p \xrightarrow{v} q \xrightarrow{w_3} \Phi$ and so $w_2vw_3 \in C^*$. But we have $\eta_L(v) = \eta_L(w)$ and so $w_2ww_3 \in C^*$ by (2.1). Therefore, there is a loop in $\mathscr{A}^*$ at Φ labelled w_2ww_3, i.e. $\Phi \xrightarrow{w_2ww_3} \Phi$. There results a path $p \xrightarrow{w_1} \Phi \xrightarrow{w_2ww_3} \Phi \xrightarrow{w_4} q$. Since $w_1w_2ww_3w_4 = w^3$ and $\rho(w^3) = \rho(w)^3 = e^3 = e$, it follows that $pe = q$ and hence $p = q$. As $p \in \mathscr{O}_i$ was arbitrary, this shows that g is trivial. Thus K_i is trivial, completing the proof of the claim. □

Claim 3. Let $\mathscr{O}_i$ be an orbit of K such that, for all $g \in K_i$, there does not exist $u \in A^*$ such that $\rho(u) = g$ with $u = u'u''$ and $s \xrightarrow{u'} \Phi \xrightarrow{u''} s'$ where $s, s' \in \mathscr{O}_i$ (and so in particular $\Phi \notin \mathscr{O}_i$. Then $K_i \prec M(\mathscr{A})$.

Proof. Let $\gamma : A^* \to M(\mathscr{A})$ be the canonical projection. Our hypotheses says that if $\rho(u) \in K_i$ and $s, s' \in \mathscr{O}_i$, then $\rho(u)_{s,s'} = \gamma(u)_{s,s'}$. Indeed, any path labelled by u between vertices of $\mathscr{O}_i$ cannot visit Φ. Hence we have $\rho(u)_{s,s'} \leq \gamma(u)_{s,s'}$ for $s, s \in \mathscr{O}_i$. On the other hand, if u reads a path from s to s' in $\mathscr{A}$, then since s, s' are not trimmed when forming $\mathscr{A}^*$, it follows that any vertex visited by u on this path is also not trimmed when forming $\mathscr{A}^*$ and so $\gamma(u)_{s,s'} \leq \rho(u)_{s,s'}$. It follows that there is a well-defined surjective homomorphism $\widetilde{\rho} : \gamma(\rho^{-1}(K_i)) \to K_i$ given by $\widetilde{\rho}(\gamma(u)) = \rho(u)$. As $\gamma(\rho^{-1}(K_i))$ is a submonoid of $M(\mathscr{A})$, we conclude $K_i \prec M(\mathscr{A})$. □

Putting together Claims 2 and 3 establishes the theorem. □

Corollary 2.2. *If* $\mathbf{H}$ *is an extension-closed pseudovariety of groups and* $\mathscr{A}$ *is a deterministic automaton recognizing a code* C *such that* $M(\mathscr{A}), M(C^*)$ *belong to* $\overline{\mathbf{H}}$*, then* $M(\mathscr{A}^*) \in \overline{\mathbf{H}}$.

3. Profinite metrics and uniformities

Let us begin by recalling the definition of a uniformity on a set X since this formalism will be convenient for our proofs.

Definition 3.1 (Uniformity)**.** A uniformity on X is a set $\mathscr{U}$ of reflexive relations on X such that:

(1) If $R_2 \supseteq R_1$ and $R_1 \in \mathscr{U}$, then $R_2 \in \mathscr{U}$;
(2) If $R_1, R_2 \in \mathscr{U}$, then $R_1 \cap R_2 \in \mathscr{U}$;
(3) If $R \in \mathscr{U}$, then $R^{-1} \in \mathscr{U}$;
(4) If $R \in \mathscr{U}$, then there exists $R' \in \mathscr{U}$ such that $R' \circ R' \subseteq R$.

The first two conditions say that $\mathscr{U}$ is a filter. The elements of $\mathscr{U}$ are called *entourages*. A collection $\mathscr{B}$ of reflexive relations on X is called a *fundamental system of entourages* for $\mathscr{U}$ if $\mathscr{U}$ consists of those relations on X containing an element of $\mathscr{B}$. It is easy to see that if X is a set and $\mathscr{B}$ is

a collection of equivalence relations closed under pairwise intersection, then $\mathscr{B}$ is a fundamental system of entourages for a unique uniformity on X.

If R is an entourage and $x, y \in X$, then we use the notation $d(x, y) < R$ to mean that $(x, y) \in R$. The intuition is that x, y are at least as close as R. The most natural example of a uniformity is the uniformity associated to a metric on a metric space (X, d). A fundamental system of entourages is given by the collection $\{R_\varepsilon \mid \varepsilon > 0\}$ where $R_\varepsilon = \{(x, y) \in X \times X \mid d(x, y) < \varepsilon\}$. Notice that $d(x, y) < R_\varepsilon$ if and only if $d(x, y) < \varepsilon$, whence the notation. Notice that, for condition (4), if $R = R_\varepsilon$, then we can take $R' = R_{\varepsilon/2}$.

A set X equipped with a uniformity $\mathscr{U}$ is called a *uniform space*. A topology can be placed on X by taking as a neighbourhood basis of a point $x \in X$ the sets of the form $B(x, R) = \{y \in X \mid d(x, y) < R\}$ where $R \in \mathscr{U}$. The topology is Hausdorff if and only if $\bigcap \mathscr{U} = \Delta_X$, the diagonal.

A *Cauchy net* in a uniform space X is a net (x_α) such that for all $R \in \mathscr{U}$, there exists γ such that, for all $\alpha, \beta \geq \gamma$, $d(x_\alpha, x_\beta) < R$. A uniform space is *complete* if each Cauchy net converges. Every uniform space has a Hausdorff completion $\widehat{X}$ and every uniformly continuous function from X to a complete Hausdorff uniform space extends uniquely to $\widehat{X}$ [8]. Here a function $f : X \to Y$ between uniform spaces is *uniformly continuous* if, for each entourage R on Y, there is an entourage R' on X so that, for all $x, y \in X$ with $d(x, y) < R'$, one has $d(f(x), f(y)) < R$.

Let $\mathbf{V}$ be a pseudovariety of monoids. A monoid M is said to be *residually* $\mathbf{V}$ if it has enough homomorphisms to elements of $\mathbf{V}$ to separate points. For example a monoid is residually $\mathbf{M}$ if and only if it is residually finite. Let M be a residually $\mathbf{V}$ monoid. Then the set $\mathscr{B}_{\mathbf{V}}$ of congruences R on M such that $M/R \in \mathbf{V}$ forms the fundamental system of entourages for a uniformity known as the *pro-*$\mathbf{V}$ *uniformity* on M [1]. The associated uniform space is Hausdorff precisely because M is residually $\mathbf{V}$. The multiplication on M is uniformly continuous [1] and the completion $\widehat{M}_{\mathbf{V}}$ is a profinite monoid, called the *pro-*$\mathbf{V}$ *completion* of M; in fact, it is just $\varprojlim_{R \in \mathscr{B}_{\mathbf{V}}} M/R$ and hence is a *pro-*$\mathbf{V}$ *monoid* (that is a projective limit of (finite) monoids from $\mathbf{V}$ [1,18]). The monoid $\widehat{M}_{\mathbf{V}}$ is compact Hausdorff and totally disconnected [1]. More generally if M is a monoid with a uniform structure with a fundamental system $\mathscr{B}$ of entourages consisting of finite index congruences, then the completion $\widehat{M}$ can be identified with $\varprojlim_{R \in \mathscr{B}} M/R$ and hence $\widehat{M}$ is profinite. In what follows, instead of writing pro-$\mathbf{M}$ we shall just use the term profinite and also we will omit $\mathbf{M}$ as a subscript. So we say profinite uniformity, profinite completion and write $\widehat{M}$ for the completion.

Suppose that M is a residually $\mathbf{V}$ monoid. The *pro-*$\mathbf{V}$ *metric* on M is defined in the following way. Fix a sequence $\{\lambda_k\}$ of strictly decreasing positive real numbers converging to zero. Set $\lambda_\infty = 0$. For $m, n \in M$, let $\sigma(m, n)$ be the least cardinality of a homomorphic image of M in $\mathbf{V}$

separating m from n (if $m = n$, take $\sigma(m, n) = \infty$). Define

$$d_{\mathbf{V}}(m, n) = \lambda_{\sigma(m,n)}.$$

One easily verifies that $d_{\mathbf{V}}$ is an ultrametric. In the case that M is finitely generated, it is straightforward to see that the uniformity corresponding to $d_{\mathbf{V}}$ is the pro-$\mathbf{V}$ uniformity [1]. The associated topology is termed the *pro*-$\mathbf{V}$ topology.

For example, let A be a finite set. The profinite topology on A^* is discrete. This is because if $u \in A^*$ is of length n and I is the ideal of words of length greater than n, then A^*/I is a finite monoid and the congruence class of u is the singleton $\{u\}$. Notice that the same argument applies to the pro-$\overline{\mathbf{H}}$ topology for any pseudovariety of groups $\mathbf{H}$. On the other hand, the profinite topology on the free group on A, denoted $FG(A)$, is not discrete. In fact A^* is dense in the profinite topology on $FG(A)$. Hence there is an onto homomorphism $\varphi : \widehat{A^*} \to \widehat{FG}(A)$. Since any infinite profinite group is uncountable, this shows that $\widehat{A^*}$ is uncountable (if $A \neq \emptyset$) and so the metric d has uncountably many Cauchy sequences. In particular, the profinite uniformity is quite far from being discrete (a uniformity is said to be *discrete* if Δ_X is an entourage, or equivalently it consists of all reflexive relations). One easily verifies $\widehat{A^*}$ is a free profinite monoid on A and $\widehat{FG}(A)$ is a free profinite group on A [1, 18]. More generally, if $\mathbf{V}$ is a pseudovariety of monoids, respectively groups, then $\widehat{A^*}_{\mathbf{V}}$ is a free pro-$\mathbf{V}$ monoid, respectively $\widehat{FG}(A)_{\mathbf{V}}$ is a free pro-$\mathbf{V}$ group [1, 18].

A key fact about $\widehat{A^*}_{\mathbf{V}}$, due to the first author, is that there is an isomorphism between the Boolean algebra of clopen subsets of $\widehat{A^*}_{\mathbf{V}}$ and the Boolean algebra of $\mathbf{V}$-recognizable subsets of A^* [1, Theorem 3.6.1]. More precisely, if $K \subseteq \widehat{A^*}_{\mathbf{V}}$ is clopen, then $K \cap A^*$ is $\mathbf{V}$-recognizable; conversely, if $R \subseteq A^*$ is $\mathbf{V}$-recognizable, then $\overline{R} \subseteq \widehat{A^*}_{\mathbf{V}}$ is clopen. That is to say, $\widehat{A^*}_{\mathbf{V}}$ is the Stone dual of the Boolean algebra of $\mathbf{V}$-recognizable subsets of A^*. In particular, the clopen submonoids of $\widehat{A^*}_{\mathbf{V}}$ are precisely the submonoids of the form $\overline{M}$ where M is a $\mathbf{V}$-recognizable submonoid of A^*.

A more general situation is when X is a topological space such that each point has a basis of clopen neighbourhoods. Then one can define a uniformity on X^* whose fundamental system of entourages consists of all finite index congruences R on X^* such that $X^*/R \in \mathbf{V}$ and if X^*/R is endowed with the discrete topology, then the natural map $X \to X^*/R$ is continuous. Our assumption on X implies that the associated topology on X^* is Hausdorff (assuming $\mathbf{V}$ is non-trivial) and the induced topology on X is its original topology. The completion $\widehat{X^*}_{\mathbf{V}}$ of X^* with respect to this uniformity gives the free pro-$\mathbf{V}$ monoid on X. It has the universal property that any continuous map from X into a pro-$\mathbf{V}$ monoid extends uniquely to a continuous morphism from $\widehat{X^*}_{\mathbf{V}}$.

Let's consider an example. Let X be an infinite discrete space and βX be its Stone-Czech compactification [8]. Then βX is a compact Hausdorff

totally disconnected space and it has the universal property that any continuous map from X to a compact Hausdorff space extends uniquely to βX. It follows immediately that $\widehat{X^*}_{\mathbf{V}} = \widehat{(\beta X)^*}_{\mathbf{V}}$. Now it is well known that βX is not metrizable; in fact, X is a dense subset of βX, but any convergent sequence of elements from X must be eventually constant. Indeed, let (x_n) be a sequence of elements of X that is not eventually constant. Then we can choose a function $\chi : X \to \{0, 1\}$ that takes on both values $0, 1$ infinitely often on (x_n). Since χ extends continuously to βX, it follows that (x_n) cannot converge.

As a consequence we conclude that if X is an infinite discrete set, then $\widehat{X^*}_{\mathbf{V}}$ is not metrizable and in particular cannot embed in $\widehat{A^*}_{\mathbf{V}}$ for any finite set A, as this latter monoid is metrizable.

4. The case of free profinite groups

Let $\mathbf{H}$ be an extension-closed pseudovariety of groups. In this section we give a variation on the usual proof that clopen subgroups of finitely generated free pro-$\mathbf{H}$ groups are finitely generated free pro-$\mathbf{H}$ groups [19,23]. The reason for doing this is to highlight the similarities between the group case and the monoid case, as well as to contrast the differences.

So let F be a finitely generated free group of rank n. Then it is well known [19], and not too difficult to show, that the clopen (equals open) subgroups of $\widehat{F}_{\mathbf{H}}$ are precisely the subgroups of the form $\overline{U}$ where U is an open subgroup of F in the pro-$\mathbf{H}$ topology. Moreover, this latter condition is equivalent to saying that U is a finite index subgroup of F such that $F/U^F \in \mathbf{H}$ where $U^F = \bigcap_{g \in F} gUg^{-1}$ is the intersection of all the conjugates of U. Equivalently, U^F is the kernel of the natural map $F \to S_{F/U}$ associated to the action of F on F/U [19]. By the Nielsen-Schreier theorem, U is a free group of rank $1 + [F : U](n - 1)$.

So to prove that $\overline{U}$ is a free pro-$\mathbf{H}$ group of rank $1 + [F : U](n - 1)$ it suffices to show that $\overline{U}$ is the completion of U with respect to its own pro-$\mathbf{H}$ metric. That is it suffices to show that the uniformity induced on U by the pro-$\mathbf{H}$ uniformity on F coincides with the pro-$\mathbf{H}$ uniformity on U. Our proof uses the wreath product. To compare with the monoidal context, we use the following construction of the permutational wreath product. Let $H \leq M_n(\mathbb{Q})$ be a group of $n \times n$ permutation matrices and let G be any group. Then the *(permutational) wreath product* $G \wr H$ is the group of all $n \times n$ monomial matrices over $G \cup 0$ that can be obtained by replacing non-zero elements of matrices in H by elements of G.

Theorem 4.1. *Let $FG(A)$ be a free group on a set A and let U be an open subgroup of $FG(A)$ in the pro-$\mathbf{H}$ topology. Then the pro-$\mathbf{H}$ uniformity on U is induced by the pro-$\mathbf{H}$ uniformity on $FG(A)$. In particular, the closure of U in $\widehat{FG}(A)_{\mathbf{H}}$ is a free pro-$\mathbf{H}$ group on a basis of U.*

Proof. A fundamental system of entourages $\mathscr{B}$ for the pro-$\mathbf{H}$ uniformity on $FG(A)$ consists of all finite index congruences R such that $FG(A)/R \in \mathbf{H}$. To prove the theorem it suffices to show that the restrictions of elements of $\mathscr{B}$ to U form a fundamental system of entourages for the pro-$\mathbf{H}$ uniformity on U. Clearly if R is a congruence on $FG(A)$ with quotient group in $\mathbf{H}$, then its restriction to U is a congruence on U with quotient in $\mathbf{H}$ and hence an entourage. So what we need to show is that if $\varphi : U \to G$ is a homomorphism with $G \in \mathbf{H}$, then there is a homomorphism ψ from $FG(A)$ to a member of $\mathbf{H}$ such that φ factors through $\psi|_U$. It will then follow that the entourage of U corresponding to φ contains the restriction to U of the entourage of $FG(A)$ corresponding to ψ.

Let $m = [FG(A) : U]$ and choose coset representatives $\{1 = w_1, \ldots, w_m\}$ for the right cosets of U in $FG(A)$. Let $\rho : FG(A) \to M_m(\mathbb{Q})$ be the permutation representation associated to $FG(A)$ acting on the right cosets of $FG(A)/U$. Let $H = \rho(FG(A))$; by assumption $H \in \mathbf{H}$. There is a well-known embedding, due to Kaloujnine-Krasner although in essence it goes back to Frobenius, of $FG(A)$ into $U \wr H$ defined as follows. For $a \in A$, set

$$(\tau(a))_{i,j} = \begin{cases} w_i a w_j^{-1} & \text{if } Uw_i a = Uw_j \\ 0 & \text{else.} \end{cases}$$

Then τ induces an embedding $\tau : FG(A) \to U \wr H$. Moreover, it is easy to check that if $u \in U$, then $(\tau(u))_{1,1} = u$. One can define $\alpha : U \wr H \to G \wr H$ by applying φ entry-wise to elements of $U \wr H$. Then the composition $\psi = \alpha\tau : FG(A) \to G \wr H$ has the property that $(\psi(u))_{1,1} = \varphi(u)$ for $u \in U$. Since $\mathbf{H}$ is closed under extension, ψ is our desired homomorphism from $FG(A)$ to a group in $\mathbf{H}$ with the property that φ factors through $\psi|_U$. This completes the proof. □

Our goal for monoids is to generalize the above proof scheme. The key obstacles are the following: no Nielsen-Schreier theorem and no permutation representation on cosets with which to take the wreath product. We shall end up replacing the permutation representation with an unambiguous representation. The fact that there is no Nielsen-Schreier theorem means that we must do something to show that if K is a free clopen submonoid of $\widehat{A^*}_{\mathbf{V}}$, then $K \cap A^*$ is a free abstract monoid. Margolis, Sapir and Weil were able to get around the lack of cosets for the case of a finitely generated free submonoid by using what they call the sagittal automaton [13] (called the literal automaton in [7]). This is a canonical construction for which there is a known Kaloujnine-Krasner type embedding [14]. For the case of infinitely generated free rational submonoids, there is no canonical choice of finite unambiguous automata, and topological considerations come into play.

5. Characterization of free clopen submonoids

Fix for this section an extension-closed pseudovariety $\mathbf{H}$ of groups. Let A be a non-empty finite alphabet and $C \subseteq A^*$ an $\overline{\mathbf{H}}$-code. We remind the

reader, as we pointed out earlier, that in this context both C and C^* are $\overline{\mathbf{H}}$-recognizable. Our first goal is to show that the clopen submonoid $\overline{C^*}$ of $\widehat{A^*}_{\overline{\mathbf{H}}}$ is free pro-$\overline{\mathbf{H}}$ on the profinite space $\overline{C}$. In particular when C is finite, and so $\overline{C} = C$, we obtain the result from [13].

We define a uniformity on C^*, which we call the $\overline{C}$-*uniformity*, by taking as a fundamental system of entourages $\mathscr{B}$ the set of all finite index congruences R on C^* such that $C^*/R \in \overline{\mathbf{H}}$ and the induced map $C \to C/R$ extends continuously to the closure $\overline{C}$ of C in $\widehat{A^*}_{\overline{\mathbf{H}}}$. Since the set of such congruences is closed under intersection (as this operation corresponds to the product of maps), this uniformity is well defined.

Lemma 5.1. *Let A be a finite alphabet and let $C \subseteq A^*$ be a code. Then the completion of C^* with respect to the $\overline{C}$-uniformity is the free pro-$\overline{\mathbf{H}}$ monoid on $\overline{C}$.*

Proof. Let M be the completion of C^* with respect to the $\overline{C}$-uniformity. Since $M = \varprojlim_{R \in \mathscr{U}} C^*/R$, we see that M is pro-$\overline{\mathbf{H}}$. Let $\psi : \overline{C} \to N$ be a continuous map to a monoid $N \in \overline{\mathbf{H}}$. Then $\psi|_C : C \to N$ extends continuously to $\overline{C}$ and so the induced homomorphism $\psi^* : C^* \to N$ is uniformly continuous for the $\overline{C}$-uniformity on C^*. Thus it extends uniquely to a continuous map from $M \to N$, which must be a homomorphism as its restriction to the dense submonoid C^* is a homomorphism. This shows that M is a free pro-$\overline{\mathbf{H}}$ monoid on $\overline{C}$. □

Remark 5.2. One can replace $\overline{\mathbf{H}}$ by an arbitrary pseudovariety $\mathbf{V}$ in the definition of the $\overline{C}$-uniformity and the analogue of Lemma 5.1 will remain valid.

In light of Lemma 5.1 to achieve our first goal it suffices to prove the following theorem.

Theorem 5.3. *Let $\mathbf{H}$ be an extension-closed pseudovariety of groups, A a finite set and $C \subseteq A^*$ an $\overline{\mathbf{H}}$-code. Then the uniformity on C^* induced by the pro-$\overline{\mathbf{H}}$ uniformity on A^* is the $\overline{C}$-uniformity.*

Proof. We follow the same proof scheme as Theorem 4.1. First observe that if $\varphi : A^* \to M$ is a homomorphism with $M \in \overline{\mathbf{H}}$, then φ extends to $\widehat{A^*}_{\overline{\mathbf{H}}}$ and hence $\varphi|_C$ extends continuously to $\overline{C}$. Thus $\ker \varphi|_{C^*}$ is an entourage of the $\overline{C}$-uniformity on C^*. So we are left with showing if $\varphi : C^* \to M$ is a homomorphism to a monoid in $\overline{\mathbf{H}}$ such that $\varphi|_C$ extends continuously to $\overline{C}$, then there is a homomorphism $\psi : A^* \to N$ with $N \in \overline{\mathbf{H}}$ such that $\ker \psi \cap (C^* \times C^*)$ refines $\ker \varphi$. This will show that each entourage of the $\overline{C}$-uniformity contains an entourage of the induced uniformity on C^* from the pro-$\overline{\mathbf{H}}$ uniformity on A^*.

So let $\varphi : C^* \to M$ be a homomorphism to a monoid $M \in \overline{\mathbf{H}}$ such that $\varphi|_C$ extends continuously to $\overline{C}$. This happens if and only if there is an entourage of the pro-$\overline{\mathbf{H}}$ uniformity on A^* whose restriction to C refines

$\varphi|_C$, that is, if and only if there is a homomorphism $\gamma : A^* \to N$ with $N \in \overline{\mathbf{H}}$ such that $\ker\gamma \cap (C \times C)$ is contained in $\ker\varphi \cap (C \times C)$. Indeed, if φ extends continuously (and hence uniformly continuously by compactness) to $\overline{\varphi} : \overline{C} \to M$, then there is an entourage from the uniformity on $\widehat{A^*}_{\mathbf{V}}$ whose intersection with $\overline{C} \times \overline{C}$ is contained in $\ker\overline{\varphi}$. Intersecting back to A^*, we see that there is an entourage V of the pro-$\overline{\mathbf{H}}$ uniformity on A^* whose restriction to $C \times C$ is contained in $\ker\varphi \cap (C \times C)$; this entourage V necessarily contains the kernel of a homomorphism $\gamma : A^* \to N$ with $N \in \overline{\mathbf{H}}$. Conversely, if there is an entourage V of the pro-$\overline{\mathbf{H}}$ uniformity on A^* with $V \cap (C \times C) \subseteq \ker\varphi \cap (C \times C)$, then there is a homomorphism $\gamma : A^* \to N$ with $N \in \overline{\mathbf{H}}$ and $\ker\gamma \subseteq V$. So $\ker\gamma \cap (C \times C) \subseteq \ker\varphi \cap (C \times C)$. Now γ extends uniquely to a uniformly continuous homomorphism $\overline{\gamma} : \widehat{A^*} \to N$. Let $N' = \gamma(C) = \overline{\gamma}(\overline{C})$. Then define a map $\psi : N' \to M$ by setting $\psi(n) = \varphi(\gamma|_C^{-1}(n))$; this is well defined since $\ker\gamma \cap (C \times C) \subseteq \ker\varphi \cap (C \times C)$. Then, since the topologies on N' and M are discrete, we must have that $\psi\overline{\gamma}|_{\overline{C}} : \overline{C} \to M$ is continuous. By construction $\psi\overline{\gamma}|_C = \varphi$ and so φ does extend to $\overline{C}$.

Let $\mathscr{A}_0 = (Q, A, \delta, \iota, F)$ be the minimal deterministic automaton for C. Since C is an $\overline{\mathbf{H}}$-code, $M(\mathscr{A}_0) = M(C) \in \overline{\mathbf{H}}$. Define

$$\mathscr{A} = (Q \times N, A, \delta', (\iota, 1), F \times N)$$

to be the product automaton with edges of the form $(q, n) \xrightarrow{a} (q', n')$ such that $q \xrightarrow{a} q'$ is an edge of $\mathscr{A}_0$ and $n\gamma(a) = n'$. Clearly $\mathscr{A}$ is deterministic and also accepts C. Moreover, $M(\mathscr{A}) \prec M(C) \times N$ and hence $M(\mathscr{A}) \in \overline{\mathbf{H}}$. Since C is a code and $\mathscr{A}$ is deterministic, it follows from [7, Chapter IV, Propositions 1.4 and 1.5] that $\mathscr{A}^*$ is an unambiguous automaton recognizing C^*. Moreover, $M(\mathscr{A}^*) \in \overline{\mathbf{H}}$ by Theorem 2.1 and since C is an $\overline{\mathbf{H}}$-code.

We shall need the following observation.

Lemma 5.4. *Suppose that $u, v \in A^*$ label paths from $(\iota, 1)$ to (q, n) in $\mathscr{A}$ and $(q, n) \xrightarrow{a} \Phi$ is an edge in $\mathscr{A}^*$. Then $ua, va \in C$ and $\varphi(ua) = \varphi(va)$.*

Proof. By definition of $\mathscr{A}^*$, we have $qa \in F$ and so $ua, va \in C$. Since $\gamma(u) = n = \gamma(v)$, we must have $\gamma(ua) = \gamma(va)$. But $\ker\gamma \cap (C \times C) \subseteq \ker\varphi \cap (C \times C)$, so $\varphi(ua) = \varphi(va)$. □

Denote by P the set of states of $\mathscr{A}^*$. Let $\rho : A^* \to M(\mathscr{A}^*) \subseteq M_P(\mathbb{Q})$ be the associated unambiguous representation. It is a consequence of [21, Proposition 3.4] that the monoid $M \wr M(\mathscr{A}^*) \in \overline{\mathbf{H}}$. We shall define a homomorphism $\psi : A^* \to M \wr M(\mathscr{A}^*)$ by modifying ρ as follows. For $a \in A$, define:

- $\psi(a)_{\Phi,\Phi} = \varphi(a)$ if $a \in C$;
- $\psi(a)_{(q,n),\Phi} = \varphi(c)$ where $c = ua$ with u labelling a path from $(\iota, 1)$ to (q, n) in $\mathscr{A}$ if $(q, n) \xrightarrow{a} \Phi$. (This is independent of the choice of u by Lemma 5.4.);

- For all other entries, $\psi(a)$ agrees with $\rho(a)$.

Lemma 5.5. *Let $u \in C^*$. Then $\psi(u)_{\Phi,\Phi} = \varphi(u)$.*

Proof. Let $u \in C^*$. We proceed by induction on the length of u as an element of C^*. If u is the empty word, then $\psi(u)$ is the identity matrix and so $\psi(u)_{\Phi,\Phi} = 1 = \varphi(u)$.

Suppose that the lemma is true for all words of length $n-1$ in C^* and suppose $u = c_1c_2\cdots c_n$ with each $c_i \in C$. Since C is a code and $\mathscr{A}^*$ recognizes C^*, the path from Φ to Φ labelled by c_n visits the state Φ only at the beginning and end. Let $c_n = ua$ with $a \in A$. Then u labels a path in $\mathscr{A}^*$ from Φ to some $(q,n) \in Q \times N$ that does not revisit Φ and such that $(q,n) \xrightarrow{a} \Phi$ is an edge in $\mathscr{A}^*$. By definition of $\mathscr{A}^*$, there is then a path in $\mathscr{A}$ from $(\iota, 1)$ to (q,n) labelled by u. Thus $\psi(a)_{(q,n),\Phi} = \varphi(ua) = \varphi(c_n)$. So, using the unambiguity of $M(\mathscr{A}^*)$,

$$\begin{aligned}\psi(u)_{\Phi,\Phi} &= \psi(c_1\cdots c_{n-1})_{\Phi,\Phi}\psi(u)_{\Phi,(q,n)}\psi(a)_{(q,n),\Phi}\\ &= \varphi(c_1\cdots c_{n-1})\cdot 1\cdot\varphi(c_n) = \varphi(u)\end{aligned}$$

The computation $\psi(u)_{\Phi,(q,n)} = 1$ uses that the path labelled by u from Φ to (q,n) in $\mathscr{A}^*$ does not revisit Φ. □

From Lemma 5.5, we immediately have that if $u, v \in C^*$ and $\psi(u) = \psi(v)$, then $\varphi(u) = \varphi(v)$. Thus $\ker\psi \cap (C^* \times C^*)$ refines $\ker\varphi$, completing the proof of Theorem 5.3. □

The case where C is finite gives us the following strengthening of the statement of [13, Corollary 2.2]:

Corollary 5.6. *Let $\mathbf{H}$ be an extension-closed pseudovariety of groups, A a finite alphabet and $C \subseteq A^*$ a finite $\overline{\mathbf{H}}$-code. Then the pro-$\overline{\mathbf{H}}$ metric on C^* is equivalent to the induced metric on C^* from the pro-$\overline{\mathbf{H}}$ metric on A^*.*

The following corollary, generalizing [13, Corollary 2.2] from the finite case, is immediate from Lemma 5.1 and Theorem 5.3.

Corollary 5.7. *Let $\mathbf{H}$ be an extension-closed pseudovariety of groups, A a finite alphabet and $C \subseteq A^*$ an $\overline{\mathbf{H}}$-code. Then $\overline{C^*} \subseteq \widehat{A^*}_{\overline{\mathbf{H}}}$ is a free pro-$\overline{\mathbf{H}}$ clopen submonoid of $\widehat{A^*}_{\overline{\mathbf{H}}}$ with clopen basis $\overline{C}$.*

The final result of this section establishes the converse of Corollary 5.7. We remark that if M is a free pro-$\overline{\mathbf{H}}$ monoid on a topological space X, then it is also free pro-$\overline{\mathbf{H}}$ on the closure of X in M; thus every free pro-$\overline{\mathbf{H}}$ monoid has a closed (profinite) basis.

Theorem 5.8. *Let $\mathbf{H}$ be an extension-closed pseudovariety of groups and A a finite set. Then the clopen free pro-$\overline{\mathbf{H}}$ submonoids of $\widehat{A^*}_{\overline{\mathbf{H}}}$ are precisely the closures of $\overline{\mathbf{H}}$-recognizable free submonoids of A^*. More specifically, if M is an $\overline{\mathbf{H}}$-recognizable submonoid of A^* with minimal generating set $C = \min(M)$, then $\overline{M}$ is free pro-$\overline{\mathbf{H}}$ if and only if C is a code (necessarily*

an $\overline{\mathbf{H}}$-code). Moreover, $\overline{C}$ is the unique closed basis for $\overline{M}$ (and is in fact clopen).

Proof. Suppose that P is a free pro-$\overline{\mathbf{H}}$ clopen submonoid of $\widehat{A^*}_{\overline{\mathbf{H}}}$. Then $M = P \cap A^*$ is an $\overline{\mathbf{H}}$-recognizable submonoid by [1, Theorem 3.6.1] and $P = \overline{M}$. From now on we drop the notation P and stick to $\overline{M}$. Set $C = \min(M)$; then C is also $\overline{\mathbf{H}}$-recognizable. Since each element of A^* is an isolated point of $\widehat{A^*}_{\overline{\mathbf{H}}}$, it follows that C is contained in the closed submonoid generated by a subset $X \subseteq \overline{M}$ if and only if it is contained in the submonoid generated by X. Since $\widehat{A^*}_{\overline{\mathbf{H}}} \setminus A^*$ is an ideal [1], it follows that C is in the closed submonoid generated by X if and only if it is in the submonoid generated by $X \cap A^* \subseteq M$. Since $C = \min(M)$, this means that $C \subseteq X$. In particular, taking X to be a closed basis for $\overline{M}$, we have $\overline{C} \subseteq X$.

Suppose that $\overline{C} \neq X$. Since $\overline{C}$ is clopen in $\widehat{A^*}_{\overline{\mathbf{H}}}$, and hence in X, there exists a continuous map $\varphi : X \to \{0, 1\}$ such that $\varphi(\overline{C}) = \{1\}$ and $\varphi(X \setminus \overline{C}) = \{0\}$. As $\overline{M}$ is freely generated by X, this map extends to a continuous homomorphism $\varphi : \overline{M} \to (\{0, 1\}, \cdot)$. But C topologically generates the pro-$\overline{\mathbf{H}}$ monoid $\overline{M} = \overline{C^*}$, so $\varphi(\overline{M}) \subseteq \{1\}$, a contradiction. Thus $\overline{C} = X$.

It remains to show that C is a code (we already know that it is $\overline{\mathbf{H}}$-recognizable). Clearly C is a code if and only if every finite subset of C is a code, since a relation satisfied by the elements of C involves only finitely many elements. So let $D \subseteq C$ be finite. Since free monoids are residually $\overline{\mathbf{H}}$, to show that $D^* \leq A^*$ is free, it suffices to show that any map $\varphi : D \to N$ with $N \in \overline{\mathbf{H}}$ extends to a homomorphism $\varphi^* : D^* \to N$.

Now D is clopen in $\widehat{A^*}_{\overline{\mathbf{H}}}$ and hence in $\overline{C}$. Thus $\psi : \overline{C} \to N$ given by $\psi|_D = \varphi$ and $\psi(\overline{C} \setminus D) = 1$ is continuous. Thus ψ extends to a continuous homomorphism $\overline{\psi} : \overline{M} \to N$ since $\overline{M}$ is free pro-$\overline{\mathbf{H}}$ on $\overline{C}$. The map $\overline{\psi}|_{D^*}$ is then our desired extension of φ. Thus D is a code, and as D was an arbitrary finite subset of C, we conclude that C is a code.

Conversely, if $C \subseteq A^*$ is a $\overline{\mathbf{H}}$-code, then $\overline{C^*}$ is a free pro-$\overline{\mathbf{H}}$ clopen submonoid with profinite basis $\overline{C}$ by Corollary 5.7. □

References

1. J. Almeida, "Finite Semigroups and Universal Algebra", World Scientific, Singapore, 1994.
2. J. Almeida, *Profinite groups associated with weakly primitive substitutions*, Fundam. Prikl. Mat. **1** (2005), 13–48; translation in J. Math. Sci. (N. Y.) **144** (2007), 3881–3903.
3. J. Almeida and M. V. Volkov, *Subword complexity of profinite words and subgroups of free profinite semigroups*, Internat. J. Algebra Comput. **16** (2006), 221–258.
4. J. Almeida and P. Weil, *Relatively free profinite monoids: An introduction and examples*, pp. 73–117 in: "Semigroups, Formal Languages and Groups", J. B. Fountain, ed., Kluwer, Dordrecht, 1995.
5. J. Almeida and P. Weil, *Free profinite semigroups over semidirect products* Russian Math. (Iz. VUZ) **39** (1995), 1–27.

6. J. Almeida and P. Weil, *Free profinite $\mathscr{R}$-trivial monoids*, Internat. J. Algebra Comput. **7** (1997), 625–671.
7. J. Berstel and D. Perrin, "Theory of Codes", Academic Press, New York, 1985.
8. N. Bourbaki, "Topologie Générale", Chaps 1-2, 3rd ed., Act. Sci. Ind. no. **1142**, Paris, 1960.
9. S. Eilenberg, "Automata, Languages and Machines", Academic Press, New York, Vol A, 1974; Vol B, 1976.
10. K. Henckell, J. Rhodes and B. Steinberg, *A profinite approach to stable pairs*, Internat. J. Algebra Comput., to appear.
11. I. Koryakov, *Embedding of pseudofree semigroups*, Russian Math. (Iz. VUZ) **39** (1995), 53–69.
12. E. Le Rest and M. Le Rest, *Sur le calcul du monoïde syntaxique d'un sous monoïde finiment engendré*, Semigroup Forum **21** (1980), 173–185.
13. S. Margolis, M. Sapir and P. Weil, *Irreducibility of certain pseudovarieties*, Comm. Algebra **26**, 779–792.
14. J.-E. Pin and J. Sakarovitch, *Une application de la représentation matricielle des transductions*, Theor. Comp. Science **35** (1985), 271–293.
15. J. Reiterman, *The Birkhoff theorem for finite algebras*, Algebra Universalis, **14** (1982), 227–268.
16. J. Rhodes and B. Steinberg, *Profinite semigroups, varieties, expansions and the structure of relatively free profinite semigroups*, Internat. J. Algebra Comput. **11** (2001), 627–672.
17. J. Rhodes and B. Steinberg, *Closed subgroups of free profinite monoids are projective profinite groups*, Bull. London Math. Soc. **40** (2008), 375–383.
18. J. Rhodes and B. Steinberg, The "q-theory of Finite Semigroups", Sprinter, to appear.
19. L. Ribes and P. A. Zalesskiĭ, "Profinite Groups", Springer, Berlin, 2000.
20. B. Steinberg, *On free profinite subgroups of free profinite monoids*, Preprint 2007, arXiv:0712.2254.
21. P. Weil, *Groups in the syntactic monoid of a composed code*, J. Pure Appl. Algebra **42** (1986), 297–319.
22. P. Weil, *Profinite methods in semigroup theory*, Internat. J. Algebra Comput. **12** (2002), 137–178.
23. J. S. Wilson, "Profinite groups", The Clarendon Press, Oxford Univ. Press, New York, 1998.

J. Almeida: Departamento de Matemática Pura, Faculdade de Ciências, Universidade do Porto, 4169-007 Porto, PORTUGAL
E-mail address: jalmeida@fc.up.pt

B. Steinberg: School of Mathematics and Statistics, Carleton University Ottawa, Ontario K1S 5B6, CANADA
E-mail address: bsteinbg@math.carleton.ca