BULL. AUSTRAL. MATH. SOC.
VOL. 60 (1999) [391–402]

20M35, 20E18, 20M07, 20K45

MONOID KERNELS AND PROFINITE TOPOLOGIES ON THE FREE ABELIAN GROUP

BENJAMIN STEINBERG

To each pseudovariety of Abelian groups residually containing the integers, there is naturally associated a profinite topology on any finite rank free Abelian group. We show in this paper that if the pseudovariety in question has a decidable membership problem, then one can effectively compute membership in the closure of a subgroup and, more generally, in the closure of a rational subset of such a free Abelian group. Several applications to monoid kernels and finite monoid theory are discussed.

1. INTRODUCTION

In the early 1990's, the Rhodes' type II conjecture was positively answered by Ash [2] and independently by Ribes and Zalesskii [10]. The type II submonoid, or $\mathbf{G}$-kernel, of a finite monoid is the set of all elements which relate to 1 under any relational morphism with a finite group. Equivalently, an element is of type II if 1 is in the closure of a certain rational language associated to that element in the profinite topology on a free group. The approach of Ribes and Zalesskii was based on calculating the profinite closure of a rational subset of a free group. They were also able to use this approach to calculate the $\mathbf{G}_p$-kernel of a finite monoid. In both cases, it turns out the the closure of a rational subset of the free group in the appropriate profinite topology is again rational. See [7] for a survey of the type II theorem and its motivation.

Delgado [4], taking the proof of Ribes and Zalesskii as a model, computed the $\mathbf{G}_{\text{com}}$-kernel of a monoid by determining the closure of a rational subset of the free Abelian group in the profinite topology. Again, the closure of a rational subset was rational. In this paper, we give for any pseudovariety $\mathbf{H}$ of Abelian groups, having decidable membership problem and which generates the variety of Abelian groups, an algorithm for computing the pro-$\mathbf{H}$ closure of a rational subset of a finite rank free Abelian group. Again the closure is rational. While this is a problem of independent interest, we show as a consequence that the $\mathbf{H}$-kernel, $\mathbf{H}$-liftable k-tuples, and $\mathbf{H}$-pointlike pairs are decidable for any pseudovariety of Abelian groups $\mathbf{H}$ with decidable membership problem. In

Received 9th February, 1999
The author was supported in part by Praxis XXI scholarship BPD 16306 98 and by FCT through Centro de Matemática da Universidade do Porto.

addition, we obtain several join results for pseudovarieties of monoids. The key step is to first compute the closure of a subgroup. The algorithm is based on linear algebra and the fundamental theorem of finitely generated Abelian groups. The ideas of this proof arose from Delgado's [4] and the author's [14] where a large number of cases is handled and, in fact, most of the arguments are similar to those used there.

2. Profinite Topologies

A *pseudovariety of monoids* is a class $\mathbf{V}$ of finite monoids closed under the operations of taking finite products, submonoids, and homomorphic images. Examples include the pseudovarieties of finite commutative monoids, finite groups, and finite Abelian groups. In this paper, we shall mostly be concerned with pseudovarieties of Abelian groups. We shall use the symbol $\mathbf{H}$ exclusively for pseudovarieties of groups. Let G be any group. We now define the *pro-$\mathbf{H}$ topology* on G. One takes as a basis of neighbourhoods of 1 all normal subgroups N with $G/N \in \mathbf{H}$ and makes G a topological group in the standard way. We say that G is *residually in* $\mathbf{H}$ if $\{1\}$ is closed or, equivalently, the topology is Hausdorff. For example, a group is residually finite if and only if it is residually in $\mathbf{G}$, where $\mathbf{G}$ denotes the pseudovariety of all finite groups. This topology has the following alternative description. Let $g \in G$. Then we define

$$r(g) = \min\{[G : N] \mid G/N \in \mathbf{H},\ g \notin N\}$$

with the convention that if no such N exists, then $r(g) = \infty$. Then the $\mathbf{H}$-*pseudonorm* is defined by

$$|g|_{\mathbf{H}} = 2^{-r(g)}$$

and satisfies $|g_1 g_2|_{\mathbf{H}} \leqslant \max\{|g_1|_{\mathbf{H}}, |g_2|_{\mathbf{H}}\}$. One then defines an ultrametric écart by

$$d(g_1, g_2) = |g_1 g_2^{-1}|_{\mathbf{H}}$$

and one can easily check that the pro-$\mathbf{H}$ topology is defined by this écart. Furthermore, the topology is metric (and the pseudonorm a true norm) if and only if G is residually in $\mathbf{H}$. For example, if $G = \mathbb{Z}$, and $\mathbf{H}$ is the pseudovariety of p-groups, this topology is just the usual p-adic topology and the above norm is equivalent to the usual p-adic norm. In the cases of interest, the topology will indeed be metric. We use $\mathrm{cl}_{\mathbf{H}}(X)$ to denote the closure of a subset $X \subseteq G$ in this topology. The following elementary results are due to Hall [6].

Proposition 2.1. *Let $\mathbf{H}$ be a pseudovariety of groups, G a group, and H a subgroup.*

1. *H is open if and only if $G/H_G \in \mathbf{H}$, where $H_G = \bigcap_{g \in G} g^{-1} H g$ or, equivalently, if H is closed of finite index.*

https://doi.org/10.1017/S0004972700036571 Published online by Cambridge University Press

2. $\mathrm{cl}_{\mathbf{H}}(H) = \bigcap_{\text{open } K \supseteq H} K.$

If $G = \mathrm{FG}(A)$, the free group on A, then $\mathrm{cl}_{\mathbf{H}}(\{1\})$ is the verbal subgroup (invariant under all endomorphisms) defining the variety generated by $\mathbf{H}$. We use $\mathrm{FG}_{\mathbf{H}}(A)$ to denote the relatively free group $\mathrm{FG}(A)/\mathrm{cl}_{\mathbf{H}}(\{1\})$ in this variety. For example, if $\mathbf{H} = \mathbf{G}_{\mathrm{com}}$ the pseudovariety of Abelian groups, then $\mathrm{cl}_{\mathbf{H}}(\{1\})$ is the commutator subgroup and $\mathrm{FG}_{\mathbf{G}_{\mathrm{com}}}(A) = \oplus_A \mathbb{Z}$, the free Abelian group generated by A. More generally, if G is any group, $\mathrm{cl}_{\mathbf{H}}(\{1\})$ is a normal subgroup and $G_{\mathbf{H}} = G/\mathrm{cl}_{\mathbf{H}}(\{1\})$ is the maximal, residually $\mathbf{H}$ image of G. One can of course take $\widehat{G}_{\mathbf{H}}$, the *profinite completion* of G in this topology, and in this case, $G_{\mathbf{H}}$ is the image of G under the natural map. However, we shall have no need to consider profinite completions in this paper.

PROPOSITION 2.2. *Let $\mathbf{H}$ be a pseudovariety and G a group. Then the natural projection $\varphi : G \to G_{\mathbf{H}}$ is continuous, open, and closed, where both groups are given the pro-$\mathbf{H}$ topology.*

PROOF: That the map is open and continuous follows easily from the standard isomorphism theorems. To see that the map is closed, let $X \subseteq G$ be closed. Let $y \in \mathrm{cl}_{\mathbf{H}}(X\varphi)$ and $g \in G$ be such that $\varphi(g) = y$. Let N be an open normal subgroup of G. Then N is closed as well, so $\mathrm{cl}_{\mathbf{H}}(\{1\}) \subseteq N$. Also, $K = \varphi(N)$ is an open normal subgroup of $G_{\mathbf{H}}$. So $\varphi(Ng) \cap \varphi(X) = Ky \cap \varphi(X) \neq \emptyset$. Since N contains $\ker\varphi$, we have that $Ng \cap X \neq \emptyset$. So $g \in \mathrm{cl}_{\mathbf{H}}(X) = X$ and thus, $y = \varphi(g) \in \varphi(X)$ as desired. □

3. Supernatural Numbers and Pseudovarieties of Abelian Groups

By the fundamental theorem of finitely generated Abelian groups, a pseudovariety of Abelian groups is completely determined by its cyclic members. A *supernatural number* is a formal product $\prod_{p \text{ prime}} p^{n_p}$ where $0 \leqslant n_p \leqslant \infty$. There are evident notions for supernatural numbers of divides, lcm (least common multiple), and gcd (greatest common divisor). We use $\widehat{\mathbb{N}}$ for the set of supernatural numbers, which is actually a complete lattice, ordered by the relation divides. We want to establish a lattice isomorphism between $\widehat{\mathbb{N}}$ and the lattice of pseudovarieties of Abelian groups. In this paper, we shall use $\mathbb{N}$ to denote the positive integers. Being a subset of $\widehat{\mathbb{N}}$, $\mathbb{N}$ is also a lattice under the relation divides (although no longer a complete lattice). We shall call a subset $X \subseteq \mathbb{N}$ a *filter* if $m \in X$, and $n \mid m$ implies that $n \in X$, and $n, m \in X$ implies $\mathrm{lcm}(n, m) \in X$. The set of filters is a complete lattice ordered by inclusion.

PROPOSITION 3.1. *There is a lattice isomorphism between $\widehat{\mathbb{N}}$ and the set of filters of $\mathbb{N}$.*

PROOF: To each supernatural number π, one can associate the filter N_π of all natural numbers which divide it. Conversely, to any filter X, one can associate $\mathrm{lcm}(X)$. It is easy to see that these associations are inverse lattice homomorphisms. □

https://doi.org/10.1017/S0004972700036571 Published online by Cambridge University Press

We call a supernatural number π *recursive* if N_π is a recursive set of natural numbers. Note that if $n \in \mathbb{N}$, then N_n is finite and hence recursive.

PROPOSITION 3.2. *There is a lattice isomorphism between the set of filters of $\mathbb{N}$ and the lattice of pseudovarieties of Abelian groups. Furthermore, a filter N is recursive if and only if the corresponding pseudovariety of Abelian groups has decidable membership problem.*

PROOF: Let $\mathbf{H}$ be a pseudovariety of Abelian groups. Then we let $N_{\mathbf{H}} = \{n \mid \mathbb{Z}/n\mathbb{Z} \in \mathbf{H}\}$. We show that this is a filter. Indeed, if $m \in N_{\mathbf{H}}$ and $n \mid m$, then $\mathbb{Z}/m\mathbb{Z} \in \mathbf{H}$ and m/n generates a cyclic subgroup of $\mathbb{Z}/m\mathbb{Z}$ of order n, so $n \in N_{\mathbf{H}}$. If $n, m \in N_{\mathbf{H}}$, then $\big(n/\gcd(n,m)\big) \in N_{\mathbf{H}}$ and so $\big(n/\gcd(n,m)\big)m = \operatorname{lcm}(n,m)$ is in $N_{\mathbf{H}}$ by the Chinese remainder theorem. Conversely, if N is a filter, we can associate to it the pseudovariety $\mathbf{H}_N = \langle \mathbb{Z}/n\mathbb{Z} \mid n \in N \rangle$. It is easy to show that these maps are inverse lattice homomorphisms using standard facts about products, subgroups, and quotients of cyclic groups. Suppose N is a recursive filter. Then if G is a finite Abelian group, we can effectively, from its multiplication table, decompose it into a product of cyclic groups. Since N is recursive, we can check which of these are in $\mathbf{H}_N$. Conversely, if $\mathbf{H}$ has decidable membership, one can check if $n \in N_{\mathbf{H}}$ by just checking whether $\mathbb{Z}/n\mathbb{Z} \in \mathbf{H}$. □

We have thus established a lattice isomorphism between $\widehat{\mathbb{N}}$ and the lattice of pseudovarieties of Abelian groups. If $\pi \in \widehat{\mathbb{N}}$, we use $\mathbf{H}_\pi$ to represent the pseudovariety of all finite Abelian groups whose torsion coefficients divide π. Conversely, to any pseudovariety $\mathbf{H}$ of Abelian groups we can associate $\pi_{\mathbf{H}} = \operatorname{lcm}\big(\{n \mid \mathbb{Z}/n\mathbb{Z} \in \mathbf{H}\}\big)$.

COROLLARY 3.3. *The associations $\pi \mapsto \mathbf{H}_\pi$ and $\mathbf{H} \mapsto \pi_{\mathbf{H}}$ are inverse lattice isomorphisms. Furthermore, π is recursive if and only if $\mathbf{H}_\pi$ has decidable membership problem.*

Normally, one uses supernatural numbers to represent orders of procyclic groups [5]. One can show that if $\mathbb{Z}$ is given the pro-$\mathbf{H}$ topology, then $\pi_{\mathbf{H}}$ is the order of the pro-$\mathbf{H}$ completion $\widehat{\mathbb{Z}}_{\mathbf{H}}$.

PROPOSITION 3.4. *Let $\pi \in \widehat{\mathbb{N}}$ and let A be a set of cardinality n. If $\pi \in \mathbb{N}$, then $\mathrm{FG}_{\mathbf{H}_\pi}(A) = \oplus_A(\mathbb{Z}/\pi\mathbb{Z})$. Otherwise, $\mathrm{FG}_{\mathbf{H}_\pi}(A) = \mathrm{FG}_{\mathbf{G}_{\mathrm{com}}}(A) = \oplus_A\mathbb{Z}$.*

PROOF: The first statement is obvious since if $\pi \in \mathbb{N}$, then any group in the variety generated by $\mathbf{H}$ satisfies $xy = yx$ and $x^\pi = 1$ and hence, is a $\mathbb{Z}/\pi\mathbb{Z}$-module. The second statement follows upon noting that π has arbitrarily large divisors. So if $(a_1, \ldots, a_n) \in \oplus_n\mathbb{Z}$, then by choosing a divisor m of π with $m > a_i$ all i, we see that $(a_1, \ldots, a_n) \notin m(\oplus_n\mathbb{Z})$, but $\oplus_n\mathbb{Z}/m(\oplus_n\mathbb{Z}) \in \mathbf{H}_\pi$. □

Thus we see that if $n \in \mathbb{N}$, then $\mathbf{H}_n$ is *locally finite* (that is, has a free object generated by any finite set), that the pro-$\mathbf{H}$ topology on that free object is discrete, and that membership in $\mathbf{H}$ is trivially decidable. Hence, all questions which we shall address

in this paper are either uninteresting or trivial for such pseudovarieties. So for the rest of this paper, we shall assume π is an "infinite" supernatural number.

4. Closures of Subgroups

Let A be a finite set of cardinality n, π an infinite supernatural number, and $\mathbf{H} = \mathbf{H}_\pi$. We now describe the closure of a subgroup of $F = \oplus_A \mathbb{Z}$ in the pro-$\mathbf{H}$ topology. The proof scheme generalises techniques of the author's [14]. If G is a finitely generated Abelian group, we use G_{tor} for its torsion subgroup. We shall use frequently that given a finite presentation of G, one can effectively find G_{tor}. See [9] for a proof of the fundamental theorem of finitely generated Abelian groups which shows that everything can be done effectively. In this paper, we shall write Abelian groups additively.

Lemma 4.1. *Suppose that $H \subseteq F$ is closed. Then $(F/H)_{\text{tor}} \in \mathbf{H}$.*

Proof: Since $H = \bigcap_{\text{open } K \supseteq H} K$, $F/H \subseteq \prod_{\text{open } K \supseteq H} F/K$. Let $g = (g_K)$ be an element of $(\prod F/K)_{\text{tor}}$. Then

$$\operatorname{ord}(g) = \operatorname{lcm}\big(\{\operatorname{ord}(g_K) \mid \text{open } K \supseteq H\}\big) < \infty$$

and divides π, since each $F/K \in \mathbf{H}$. □

Now, we work towards the converse of this result.

Lemma 4.2. *Suppose $H \subseteq F$ is a subgroup with $(F/H)_{\text{tor}} \in \mathbf{H}$ and $x \in F \setminus H$. Then there is an open subgroup $K \supseteq H$ such that $x \notin K$.*

Proof: By the fundamental theorem of finitely generated Abelian groups, there are a basis $\{e_1, e_2, \dots e_n\}$ for F and positive integers $a_1, \dots, a_k$ such that $\{a_1 e_1, \dots, a_k e_k\}$ is a basis for H. Since $(F/H)_{\text{tor}} \in \mathbf{H}$, the $a_i \mid \pi$. If $x = b_1 e_1 + \cdots + b_n e_n$ with $b_i > 0$ some $i > k$, choose $m > b_i$ such that $m \mid \pi$. This can be done since π is infinite. Then

$$K = \langle a_1 e_1, \dots, a_k e_k, e_{k+1}, \dots, e_{i-1}, m e_i, e_{i+1}, \dots, e_n \rangle$$

is as desired. Otherwise, if there is no such index i, then

$$K = \langle a_1 e_1, \dots, a_k e_k, e_{k+1}, \dots, e_n \rangle$$

works. □

Corollary 4.3. *Suppose $H \subseteq F$ and π is an infinite supernatural number. Then H is closed if and only if $(F/H)_{\text{tor}} \in \mathbf{H}$. In particular, if π is recursive, it is decidable whether a subgroup is closed (given a finite generating set as input).*

Proof: We have already seen that the condition is necessary for being closed. But the above lemma shows that it is sufficient, since any element of $F \setminus H$ can be separated from H by an open subgroup. The last statement follows since one can effectively compute

https://doi.org/10.1017/S0004972700036571 Published online by Cambridge University Press

the torsion coefficients of F/H via row and column operations applied to the matrix whose columns are the generators of H. □

We now compute the closure of a subgroup H of F in the pro-$\mathbf{H}$ topology. The procedure is as follows: let $e_1, \ldots, e_n$ and $a_1, \ldots, a_k$ be as in the proof of Lemma 4.2. Then the closure of H is the subgroup obtained by replacing each a_i with $b_i = \gcd(a_i, \pi)$. Of course, we must show that this works.

PROPOSITION 4.4. *Let $F = \oplus_A \mathbb{Z}$ with basis $\{e_1, \ldots, e_n\}$ and let $H = \langle a_1 e_1, \ldots, a_k e_k \rangle$. For each i, let $b_i = \gcd(a_i, \pi)$. Then $\mathrm{cl}_{\mathbf{H}}(H) = \langle b_1 e_1, \ldots, b_k e_k \rangle$.*

PROOF: By the above corollary, $K = \langle b_1 e_1, \ldots, b_k e_k \rangle$ is closed and clearly, $H \subseteq K$. To show the converse, by continuity of addition, it suffices to show that $b_i e_i \in \mathrm{cl}_{\mathbf{H}}(H)$ for each i. Let $\varphi : F \to G \in \mathbf{H}$ be a homomorphism. We show that $\varphi(b_i e_i) \in \varphi(\langle a_i e_i \rangle)$. The result will then follow. If $\varphi(e_i) = 0$, we are done. Otherwise $\langle \varphi(e_i) \rangle = \mathbb{Z}/m\mathbb{Z}$ where $m \mid \pi$. Let $a_i = m_i b_i$ with $\gcd(m_i, \pi) = 1$. Then m_i is relatively prime to m, so there exists d_i such that $d_i m_i \equiv 1 \bmod m$. So

$$\varphi(d_i a_i e_i) = d_i m_i \varphi(b_i e_i) = \varphi(b_i e_i)$$

and thus $\varphi(b_i e_i) \in \varphi(\langle a_i e_i \rangle)$ as desired. □

THEOREM 4.5. *Let A be a finite set, $F = \oplus_A \mathbb{Z}$, π a recursive, infinite supernatural number, $\mathbf{H} = \mathbf{H}_\pi$, and $X \subseteq F$ a finite subset. Then one can effectively compute a basis for and membership in $\mathrm{cl}_{\mathbf{H}}(\langle X \rangle)$.*

PROOF: Let $H = \langle X \rangle$. By the proof of the fundamental theorem of finitely generated Abelian groups, we can effectively find a basis $\{e_1, \ldots, e_n\}$ for F and positive integers $a_1, \ldots, a_k$ such that $\{a_1 e_1, \ldots, a_k e_k\}$ is a basis for H. Furthermore, we can effectively change between this basis and the standard basis. Since π is recursive and we can effectively factor the a_i, we can effectively compute each of the $b_i = \gcd(a_i, \pi)$. So by the above proposition, $\{b_1 e_1, \ldots, b_n e_n\}$ is a basis for $\mathrm{cl}_{\mathbf{H}}(H)$. We can then effectively write this basis in terms of the original basis if we so desire. To check whether an element $x \in F$ is in $\mathrm{cl}_{\mathbf{H}}(H)$, we write it as $x = c_1 e_1 + \cdots + c_n e_n$ and determine if $b_i \mid c_i$ for $1 \leqslant i \leqslant k$ and $c_i = 0$ for $i > k$. □

Next we show that if $\mathbf{H}$ is a proper subpseudovariety of $\mathbf{G}_{\mathrm{com}}$ corresponding to an infinite supernatural number, then in general for $\mathbf{H}$-closed subgroups H and K of F, $H + K$ is not closed. Indeed, let n be an integer such that $\mathbb{Z}/n\mathbb{Z} \notin \mathbf{H}$. Let $F = \mathbb{Z} \oplus \mathbb{Z}$, $H = \langle (1, 0) \rangle$, and $K = \langle (1, n) \rangle$. Then since $F/H = F/K = \mathbb{Z}$, by Corollary 4.3, H and K are closed. But

$$H + K = \langle (1, 0), (1, n) \rangle = \langle (1, 0), (0, n) \rangle.$$

So $F/(H + K) = \mathbb{Z}/n\mathbb{Z} \notin \mathbf{H}$. Hence $H + K$ is not closed, again by Corollary 4.3. Thus the approach of [4] cannot immediately be generalised the way [11] generalises [10].

https://doi.org/10.1017/S0004972700036571 Published online by Cambridge University Press

COROLLARY 4.6. *Let A be a finite set, X a finite collection of reduced words over A, π a recursive, infinite supernatural number, and $\mathbf{H} = \mathbf{H}_\pi$. Then there is an algorithm to compute membership in $\mathrm{cl}_{\mathbf{H}}(\langle X\rangle) \subseteq \mathrm{FG}(A)$.*

PROOF: Let $H = \langle X\rangle$ and $\varphi : \mathrm{FG}(A) \to \mathrm{FG}_{\mathbf{G}_{\mathrm{com}}}(A)$ be the canonical projection. We claim $w \in \mathrm{cl}_{\mathbf{H}}(H)$ if and only if $\varphi(w) \in \mathrm{cl}_{\mathbf{H}}(\varphi(H))$. To see this, first note that Proposition 2.2 implies that $\mathrm{cl}_{\mathbf{H}}(\varphi(H)) = \varphi(cl_{\mathbf{H}}(H))$. So we just need to show that if $\varphi(w) \in \mathrm{cl}_{\mathbf{H}}(\varphi(H))$, then $w \in \mathrm{cl}_{\mathbf{H}}(H)$. Let N be an open normal subgroup of $\mathrm{FG}(A)$. Then $\varphi(N)$ is a normal open subgroup of $\mathrm{FG}_{\mathbf{G}_{\mathrm{com}}}(A)$ and so $\varphi(Nw) \cap \varphi(H) \neq \emptyset$. Since N contains $\ker\varphi$, it follow that $Nw \cap H \neq \emptyset$ and so, $w \in \mathrm{cl}_{\mathbf{H}}(H)$. □

See [**8, 15**] for some consequences of this result, although subsequent results will subsume these applications.

5. CLOSURES OF RATIONAL SUBSETS

Let M be a monoid. A subset $L \subseteq M$ is said to be *recognisable* if there exists a homomorphism $\varphi : M \to N$ with N finite and $L = \varphi^{-1}(B)$ with $B \subseteq N$. The collection of recognisable subsets is denoted $\mathrm{Rec}(M)$. If A is a set, we use A^* for the free monoid on A. If M is any monoid, and $X \subseteq M$, we use X^* for the submonoid generated by X. A subset of M is called *rational* if it is in the smallest collection of subsets of M containing the finite subsets and closed under finite unions, finite products, and the operation $X \mapsto X^*$. The collection of rational subsets of M is denoted $\mathrm{Rat}(M)$. A *rational expression* for a rational set is an expression like $\big((ab \cup c)d^*\big)^*$ which shows how to build the set up from the "rational operations". Kleene's theorem says that $\mathrm{Rat}(A^*) = \mathrm{Rec}(A^*)$ for A finite and more generally, implies that $\mathrm{Rec}(M) \subseteq \mathrm{Rat}(M)$ if M is finitely generated. It is easy to show that if $\varphi : M \to N$ is a homomorphism, then the image of a rational set is rational while the inverse image of a recognisable set is recognisable [**3**]. Let π be a recursive, infinite supernatural number and $\mathbf{H}$ the associated pseudovariety of Abelian groups. We now give an algorithm to compute the closure of a rational subset of $F = \oplus_A \mathbb{Z}$ for A a finite set. First we note that if such an algorithm exists, then π must be recursive. Indeed, the membership problem for $\mathbf{H}$ is the same as asking for A finite and N a finite index subgroup of $F = \oplus_A \mathbb{Z}$, with a given finite generating set, whether N is closed. But it is easy to see that if $g + N = g' + N$, then $g \in \mathrm{cl}_{\mathbf{H}}(N)$ if and only if $g' \in \mathrm{cl}_{\mathbf{H}}(N)$. So to verify whether N is closed, it suffices to check whether any element of a finite set of coset representatives of N in F is in $\mathrm{cl}_{\mathbf{H}}(N)$, but not in N. But if Y is a generating set of N, then $N = (Y \cup -Y)^*$ and hence is rational, so we can check this.

A subset of a monoid M is said to be *semilinear* if it is a finite union of sets of the form

$$ab_1^*b_2^* \cdots b_n^* \ (n \geqslant 0,\ b_1, \ldots, b_n \in M).$$

The following proposition is straightforward and can be found in [**4**].

https://doi.org/10.1017/S0004972700036571 Published online by Cambridge University Press

PROPOSITION 5.1. *Let M be a finitely generated commutative monoid. Then $L \in \mathrm{Rat}(M)$ if and only if it is semilinear.*

Given a finite presentation of a commutative monoid M, one can effectively place a rational subset in the above form by induction on the star height. Also note that since M is commutative, $b_1^* + \cdots + b_n^* = \{b_1, \ldots, b_n\}^*$. So we have the following corollary.

COROLLARY 5.2. *Let M be a finitely presented commutative monoid. Then any rational subset L of M can be effectively placed in the form $\bigcup_i (a_i + B_i^*)$ with $a_i \in M$, $B_i \subseteq M$ a finite subset, and the union finite.*

PROPOSITION 5.3. *Let $L = \bigcup_i (a_i + B_i^*)$ be a rational subset of F. Then $\mathrm{cl}_{\mathbf{H}}(L) = \bigcup_i (a_i + \mathrm{cl}_{\mathbf{H}}(\langle B_i \rangle))$.*

PROOF: Since the pro-$\mathbf{H}$ topology is metric, taking the closure commutes with taking finite unions. So it suffices to show that $\mathrm{cl}_{\mathbf{H}}(a + B^*) = a + \mathrm{cl}_{\mathbf{H}}(\langle B \rangle)$. Since translation by a is a continuous homomorphism, it suffices to show that $\mathrm{cl}_{\mathbf{H}}(B^*) = \mathrm{cl}_{\mathbf{H}}(\langle B \rangle)$. The inclusion from left to right is clear. By continuity of multiplication, it is easy to see that $\mathrm{cl}_{\mathbf{H}}(B^*)$ is a submonoid. So it suffices to show $-B \subseteq \mathrm{cl}_{\mathbf{H}}(B^*)$. But if $b \in B$, then

$$(n! - 1)b \to -b$$

so $-b \in \mathrm{cl}_{\mathbf{H}}(B^*)$. □

COROLLARY 5.4. *Let π be a recursive, infinite supernatural number, $\mathbf{H}$ the associated pseudovariety of Abelian groups, and F a finitely generated free Abelian group. The one can compute membership in the closure of a rational subset of F given a rational expression as input.*

Note that since any subgroup of a finite rank free Abelian group is finitely generated, and hence a rational subset, we see that the closure of a rational subset is rational. Observe that in the case of $\mathbf{G}_{\mathrm{com}}$, our results show that every subgroup is closed and hence,

$$cl_{\mathbf{G}_{\mathrm{com}}}\Big(\bigcup_i (a_i + B_i^*)\Big) = \bigcup_i \big(a_i + \langle B_i \rangle\big).$$

This result was originally obtained by Delgado [4].

6. MONOID KERNELS AND APPLICATIONS TO MONOID THEORY

We now give several applications to the theory of monoids. Let M and N be monoids. A *relational morphism* $\mu : M \multimap N$ is a relation $\mu \subseteq M \times N$ which is a submonoid projecting onto M. The most important example is the case where M and N are generated by a set A and $\mu = \{(a, a) \mid a \in A\}^*$. If $\mu : M \multimap G$ is a relational morphism with

https://doi.org/10.1017/S0004972700036571 Published online by Cambridge University Press

G a group, then $\mu^{-1}(1)$ is a submonoid of M. Fix a pseudovariety $\mathbf{H}$ of groups. Then for M finite, we let

$$K_{\mathbf{H}}(M) = \bigcap_{\mu: M \multimap G \in \mathbf{H}} \mu^{-1}(1).$$

This set is called the $\mathbf{H}$-*kernel* of M and is a submonoid containing the idempotents of M. If $\mathbf{V}$ is a pseudovariety of monoids, then the *Mal'cev product* $\mathbf{V} \textcircled{m} \mathbf{H}$ is the pseudovariety of all finite monoids M with a relational morphism $\mu : M \multimap G \in \mathbf{H}$ with $\mu^{-1}(1) \in \mathbf{V}$. A simple exercise [7] shows that $M \in \mathbf{V} \textcircled{m} \mathbf{H}$ if and only if $K_{\mathbf{H}}(M) \in \mathbf{V}$. Hence, the computability of $K_{\mathbf{H}}$ implies the decidability of membership for any pseudovariety of the form $\mathbf{V} \textcircled{m} \mathbf{H}$ with $\mathbf{V}$ having decidable membership. In the case where $\mathbf{V}$ is local in the sense of Tilson [16], one can show that $\mathbf{V} \textcircled{m} \mathbf{H} = \mathbf{V} * \mathbf{H}$ where the right hand side is the semidirect product of pseudovarieties [7].

We now show that if $\mathbf{H}$ is a decidable pseudovariety of Abelian groups, then $K_{\mathbf{H}}$ is computable. If M is an A-generated monoid, we use $[w]_M$ to denote the image of a word $w \in A^*$ in M.

PROPOSITION 6.1. *Let M be a finite monoid generated by a finite set A, π an infinite supernatural number, $\mathbf{H}$ the associated pseudovariety of Abelian groups, and $F = \oplus_A \mathbb{Z}$. For $m \in M$, let*

$$L_m = \{[w]_F \mid w \in A^* \text{ and } [w]_M = m\}.$$

Then $m \in K_{\mathbf{H}}(M)$ if and only if $0 \in \mathrm{cl}_{\mathbf{H}}(L_m)$.

PROOF: Suppose $m \in K_{\mathbf{H}}(M)$. Let N be an open normal subgroup of F. Consider the relational morphism $\mu : M \multimap F/N$ defined by

$$\mu = \{([a]_M, a + N) \mid a \in A\}^*.$$

Then since $m \in K_{\mathbf{H}}(M)$, there exists $w \in A^*$ such that $[w]_M = m$ and $[w]_F \in N$. So $N \cap L_m \neq \emptyset$. It follows that $0 \in \mathrm{cl}_{\mathbf{H}}(L_m)$.

For the converse, let $\mu : M \multimap G \in \mathbf{H}$ be a relational morphism. Choose $\widetilde{a} \in \mu([a]_M)$ for each $a \in A$. Let $\varphi : F \to G$ be the morphism associated to the map $a \mapsto \widetilde{a}$. Let $N = \ker \varphi$. Then N is an open normal subgroup and so $L_m \cap N \neq \emptyset$. Thus, there exists $w \in A^*$ such that $[w]_M = m$ and $[w]_F \in N$. But by definition of φ, $\varphi([w]_F) \in \mu(m)$. So $m \in \mu^{-1}(0)$. It follows that $m \in K_{\mathbf{H}}(M)$. ∎

THEOREM 6.2. *Let $\mathbf{H}$ be a pseudovariety of Abelian groups with decidable membership. Then $K_{\mathbf{H}}$ is computable.*

PROOF: If $\mathbf{H}$ is locally finite, the result is trivial. So suppose $\mathbf{H}$ corresponds to a recursive, infinite supernatural number. Let M be a finite A-generated monoid. For $m \in M$, the set of words $w \in A^*$ with $[w]_M = m$ is a rational subset and one can effectively compute a rational expression for it by Kleene's algorithm. Hence, L_m is a

https://doi.org/10.1017/S0004972700036571 Published online by Cambridge University Press

rational subset of F and one can effectively obtain a rational expression for it. So by Corollary 5.4, one can decide whether $0 \in \mathrm{cl}_{\mathbf{H}}(L_m)$. Hence by the above proposition, $K_{\mathbf{H}}$ is computable. □

COROLLARY 6.3. *Let* $\mathbf{V}$ *be a pseudovariety of monoids and* $\mathbf{H}$ *a pseudovariety of Abelian groups, each with decidable membership problem. Then* $\mathbf{V} \textcircled{m} \mathbf{H}$ *has decidable membership problem.*

A related algorithmic problem is the following. Let M be a finite monoid and $\mathbf{H}$ a pseudovariety of groups. Then $(m_1, \ldots, m_k) \in M^k$ is called an $\mathbf{H}$-*liftable* k-*tuple* if for every relational morphism $\mu : M \multimap G \in \mathbf{H}$, there exists $g_1, \ldots, g_k \in G$ such that $g_1 \ldots g_k = 1$ and $g_i \in \mu(m_i)$ for all i. For instance, an $\mathbf{H}$-liftable 1-tuple is just a member of $K_{\mathbf{H}}(M)$. One can show in a similar manner to above that if $\mathbf{H}$ is a pseudovariety of Abelian groups corresponding to an infinite supernatural number, then $(m_1, \ldots, m_k)$ is an $\mathbf{H}$-liftable k-tuple if and only if $0 \in \mathrm{cl}_{\mathbf{H}}(L_{m_1} + \cdots + L_{m_k})$. Since $L_{m_1} + \cdots + L_{m_k}$ is a rational subset, we obtain the following.

PROPOSITION 6.4. *Let* $\mathbf{H}$ *be a decidable pseudovariety of Abelian groups. Then one can compute* $\mathbf{H}$-*liftable* k-*tuples.*

If M is a finite monoid, $X \subseteq M$, and $\mathbf{V}$ a pseudovariety of monoids, then X is said to be $\mathbf{V}$-pointlike if for every relational morphism $\mu : M \multimap V \in \mathbf{V}$, one has that $X \subseteq \mu^{-1}(v)$ for some $v \in V$. For example, $K_{\mathbf{H}}(M)$ is an $\mathbf{H}$-pointlike set. One can show that $M \in \mathbf{V}$ if and only if its only $\mathbf{V}$-pointlike subsets are singletons. Hence, if $\mathbf{V}$ has decidable pointlike pairs, then $\mathbf{V}$ has decidable membership. The following is proved in the same manner as Proposition 6.1; see for instance [4].

PROPOSITION 6.5. *Let* M *be a finite monoid generated by a finite set* A *and* $\mathbf{H}$ *be a non-locally finite pseudovariety of Abelian groups. Then* $\{m, n\} \subseteq M$ *is* $\mathbf{H}$-*pointlike if and only if* $0 \in \mathrm{cl}_{\mathbf{H}}(L_m - L_n)$.

COROLLARY 6.6. *Let* $\mathbf{H}$ *be a pseudovariety of Abelian groups with decidable membership problem. Then* $\mathbf{H}$-*pointlike pairs are decidable.*

A locally finite pseudovariety $\mathbf{V}$ is said to be *order computable* if there is a computable bound on the size of the free object on any finite set (in this case the pseudovariety is necessarily decidable). Recall if $\mathbf{V}$ and $\mathbf{W}$ are pseudovarieties, then their join $\mathbf{V} \vee \mathbf{W}$ is the smallest pseudovariety containing them. The following two results are consequences of the author's [12, 13].

THEOREM 6.7. *If* $\mathbf{V}$ *is an order computable, locally finite pseudovariety and* $\mathbf{H}$ *is a pseudovariety of Abelian groups with decidable membership problem, then* $\mathbf{V} \vee \mathbf{H}$ *has decidable pointlike pairs and hence is decidable.*

For undefined terms in the following theorem, see [1, 13].

THEOREM 6.8. *Let* $\mathbf{V}$ *be a pseudovariety of* $\mathcal{J}$*-trivial monoids with a decidable word problem for its monoid of implicit operations and* $\mathbf{H}$ *a pseudovariety of Abelian groups with decidable membership problem. Then* $\mathbf{V} \vee \mathbf{H}$ *has decidable pointlike pairs and hence is decidable. In particular,* $\mathbf{J} \vee \mathbf{H}$ *is decidable, where* $\mathbf{J}$ *is the pseudovariety of all finite* $\mathcal{J}$*-trivial monoids.*

Finally, it is shown in [14] that if $\mathbf{H}$ is a pseudovariety of groups with decidable pointlike pairs, then $\mathbf{J} * \mathbf{H}$ is decidable.

THEOREM 6.9. *Let* $\mathbf{H}$ *be a pseudovariety of Abelian groups with decidable membership problem. Then* $\mathbf{J} * \mathbf{H}$ *has decidable membership problem.*

It is shown in [15], that $\mathbf{J} \textcircled{m} \mathbf{H} \neq \mathbf{J} * \mathbf{H}$ for pseudovarieties of Abelian groups, so this result is meaningful.

REFERENCES

[1] J. Almeida, *Finite semigroups and universal algebra* (World Scientific, River Edge, NJ, 1994).

[2] C.J. Ash, 'Inevitable graphs: A proof of the Type II conjecture and some related decision procedures', *Internat. J. Algebra Comput.* **1** (1991), 127–146.

[3] J. Berstel, *Transductions and context-free languages* (Teubner, Stuttgart, 1979).

[4] M. Delgado, 'Abelian pointlikes of a monoid', *Semigroup Forum* **56** (1998), 339–361.

[5] M. Freid and M. Jarden, *Field arithmetic* (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

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

[7] K. Henckell, S. Margolis, J.-E. Pin and J. Rhodes, 'Ash's type II theorem, profinite topology and Malcev products. Part I', *Internat. J. Algebra Comput.* **1** (1991), 411-436.

[8] S. Margolis, M. Sapir and P. Weil, 'Closed subgroups in pro-$\mathbf{V}$ topologies and the extension problem for inverse automata', (preprint).

[9] J.R. Munkres, *Elements of algebraic topology* (Addison-Wesley, Menlo Park, CA, 1984).

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

[11] L. Ribes and P. A. Zalesskiĭ, 'The pro-p topology of a free group and algorithmic problems in semigroups', *Internat. J. Algebra Comput.* **4** (1994), 359–374.

[12] B. Steinberg, 'On pointlike sets and joins of pseudovarieties', *Internat. J. Algebra Comput.* **8** (1998), 203–231.

[13] B. Steinberg, 'On algorithmic problems for joins of pseudovarieties', *Semigroup Forum* (1999) (to appear).

[14] B. Steinberg, 'Inevitable graphs and profinite topologies: Some solutions to algorithmic problems in monoid and automata theory stemming from group theory', *Internat. J. Algebra Comput.* (1999) (to appear).

[15] B. Steinberg, 'Finite state automata: A geometric approach', (Technical Report University of Porto, 1999).

[16] B. Tilson, 'Categories as algebra: an essential ingredient in the theory of monoids', *J. Pure Appl. Algebra* **48** (1987), 83–198.

Faculdade de Ciências
da Universidade do Porto
4099-002 Porto, Portugal
e-mail: bsteinbg@agc0.fc.up.pt