SOLVING SYSTEMS OF EQUATIONS MODULO PSEUDOVARIETIES OF ABELIAN GROUPS AND HYPERDECIDABILITY

MANUEL DELGADO*

Centro de Matemática da Universidade do Porto
Rua do Campo Alegre, 687
4169-007 Porto, Portugal
E-mail: mdelgado@fc.up.pt

ARIANE MASUDA AND BENJAMIN STEINBERG†

School of Mathematics and Statistics, Carleton University
Ottawa, Ontario, K1S 5B6, Canada
E-mail: {ariane,bsteinbg}@math.carleton.ca

Based on an algorithm to solve systems of equations modulo proper pseudovarieties of abelian groups given in this paper, we prove that decidable pseudovarieties of abelian groups are (completely) hyperdecidable. However these pseudovarieties are shown not to be reducible for the canonical signature.

1. Introduction

Recall that a pseudovariety of monoids is a class of finite monoids closed under formation of finite direct products, submonoids and homomorphic images. Generalizing the notions of pointlike sets [11] and Type I and Type II semigroups [14, 15] Almeida [1] introduced the notion of hyperdecidability for pseudovarieties. One of the nice properties of a hyperdecidable pseudovariety W is that under relatively mild hypothesis on a pseudovariety V (decidable with finite vertex rank) one can decide membership in the semidirect product pseudovariety $\mathsf{V} * \mathsf{W}$. Most proofs of hyperdecidability [4, 7, 16, 18] actually establish a somewhat stronger property called

*The first author gratefully acknowledges support of FCT through the CMUP. He also acknowledges a sabbatical grant of FCT used to visit Carleton University.
†The work of the third author was done under the auspices of an NSERC discovery grant.

tameness, introduced by Almeida and the third author [5, 6].

Let us recall the definitions. A directed *graph* is a finite set $\Gamma = V \uplus E$ endowed with two adjacency functions $\alpha, \omega : E \to V$. The disjoint sets E and V are the edge set and the vertex set of Γ respectively. The maps α, ω select respectively the initial and terminal vertices. A *labelling* of Γ by a monoid M is a function $\ell : \Gamma \to M$. The labelling is said to be *consistent* if

$$\ell(\alpha(e)) \cdot \ell(e) = \ell(\omega(e))$$

for every $e \in E$.

Let M and N be finite monoids. A relational morphism $\tau : M \multimap N$ is a map from M into the power set of N such that: $\tau(m) \neq \emptyset$, all $m \in M$; $1 \in \tau(1)$; and $\tau(m_1)\tau(m_2) \subseteq \tau(m_1 m_2)$, all $m_1, m_2 \in M$. Suppose that $\tau : M \multimap N$ is a relational morphism of monoids and let $\ell : \Gamma \to M$, $\delta : \Gamma \to N$ be labellings of Γ. We say that δ is *τ-related* to ℓ if $\delta(z) \in \tau(\ell(z))$ for every $z \in \Gamma$. Let V be a pseudovariety of monoids. The labelling $\ell : \Gamma \to M$ is said to be V-*inevitable* if, for every relational morphism $\tau : M \multimap N \in \mathsf{V}$, there is a consistent labelling $\delta : \Gamma \to N$ that is τ-related to ℓ. A pseudovariety V of semigroups is said to be *hyperdecidable* if there exists an algorithm to test whether a finite graph labelled by a finite monoid is V-inevitable.

This notion was generalized by Rhodes and the third author [13], see also Almeida [2]. Let E be a finite system of equations over an alphabet X. That is, E consists of equations $u_i = v_i$ with $u_i, v_i \in X^*$. (We remark that in $\mathfrak{q}$-theory [13] equations over free profinite monoids are also considered.) Let M be a finite monoid. If N is another monoid and $\tau : M \multimap N$ is a relational morphism, then the substitutions $\sigma : X \to M$ and $\sigma' : X \to N$ are said to be *τ-related* if $\sigma'(x) \in \tau(\sigma(x))$, for all $x \in X$. If V is a pseudovariety, then the substitution σ is said to be (V, E)-*inevitable* if, for all relational morphisms $\tau : M \multimap N \in \mathsf{V}$, there is a substitution $\sigma' : X \to N$ that is τ-related to σ and such that $\sigma' \models E$ (meaning the induced map $\sigma' : X^* \to N$ satisfies $\sigma'(u) = \sigma'(v)$ for all $u = v \in E$).

For instance, if $\Gamma = V \uplus E$ is a graph, then a labelling ℓ over M is a substitution. We take as a system of equations the set E_Γ of all equations of the form $\alpha(e)e = \omega(e)$; the system of equations obtained in this way is called the *consistency equations* of Γ. Then ℓ is V-inevitable if and only if it is (V, E_Γ)-inevitable.

We shall call V *completely hyperdecidable* if (V, E)-inevitability is decidable for all finite systems of equations E. Completely hyperdecidable pseudovarieties are certainly hyperdecidable and hence decidable; they also have decidable pointlikes and decidable idempotent-pointlikes [13]. However, not every decidable pseudovariety is hyperdecidable [12, 8].

Both Rhodes and Steinberg [13] and Almeida [2] consider a generalized notion of tameness in this context, but we shall not deal with it here. The motivation for these more general notions of inevitability comes from dealing with other operators than the semidirect product. In Rhodes and Steinberg [13] pseudovarieties of relational morphisms are defined and shown to give rise to operators. The operator associated to a pseudovariety of relational morphisms R is denoted by Rq. Such pseudovarieties can be defined by pseudoidentities of the appropriate sort. Complete hyperdecidability of V means that if R is a decidable pseudovariety of relational morphisms with a certain finiteness condition, then RqV is decidable.

Our main result is the following:

Theorem 1.1. *Let* H *be a pseudovariety of abelian groups. Then* H *is decidable if and only if it is completely hyperdecidable. In particular, decidable pseudovarieties of abelian groups are hyperdecidable.*

This result is in some sense sharp because Auinger and the third author [8] constructed an example of a decidable pseudovariety of metabelian groups that is not hyperdecidable.

The third author [18] showed that any pseudovariety V of J-trivial monoids with decidable word problem for free pro-V monoids with finite generating sets has a hyperdecidable join with any hyperdecidable pseudovariety of groups. The same proof works without change for joins with completely hyperdecidable pseudovarieties of groups (for instance equations of the form $u_1 = \cdots = u_n = u_1^2$ were also considered there).

Corollary 1.1. *Let* $\mathsf{V} \subseteq \mathsf{J}$ *be a pseudovariety of monoids with decidable word problem for each finitely generated free pro-*V *monoid. Let* H *be any decidable pseudovariety of abelian groups. Then* $\mathsf{V} \vee \mathsf{H}$ *is completely hyperdecidable. In particular* $\mathsf{J} \vee \mathsf{H}$ *is completely hyperdecidable.*

Recall that any aperiodic pseudovariety V of commutative monoids has decidable word problem for its free pro-V monoids on finite sets and that every decidable pseudovariety of commutative monoids is a join of an aperiodic pseudovariety of commutative monoids and a decidable pseudovariety of abelian groups. Thus we obtain the following corollary.

Corollary 1.2. *A pseudovariety of commutative monoids is completely hyperdecidable if and only if it is decidable.*

However, it turns out that every proper, non-locally finite pseudovariety of abelian groups is not tame with respect to the canonical signature [5, 6]; in fact no such pseudovariety is weakly κ-reducible (see Almeida and Steinberg [5, 6] for undefined terminology). Steinberg [19] proved that the pseudovariety of p-groups, p a prime, is hyperdecidable by showing that it is weakly κ-reducible. Almeida [3] then showed that p-group pseudovarieties are tame with respect to an infinite (but recursive) implicit signature. The case of proper, non-locally finite pseudovarieties of abelian groups is the first example, as far as we know, of pseudovarieties of groups that are known to be hyperdecidable but are provably not weakly κ-reducible. Also, to the best of our knowledge there are currently no examples of hyperdecidable pseudovarieties that are not known in addition to be tame (for some implicit signature). Let us now formulate out second main result.

Theorem 1.2. *Let* H *be a proper pseudovariety of abelian groups that is not locally finite. Then* H *is not weakly* κ*-reducible.*

2. Solving systems modulo pseudovarieties of abelian groups

In this section we prove the previously announced theorems.

We begin with a lemma concerning solutions of systems of equations in a free abelian group modulo a sequence of integers. This lemma may be of interest in its own right. It builds on the same reparameterization trick used by Almeida and Delgado [4].

Recall [10] that a subset of $\mathbb{Z}^k$ is called *linear* if it can be expressed in the form $a + b_1\mathbb{N} + \cdots + b_p\mathbb{N}$ with $a, b_1, \ldots, b_p \in \mathbb{Z}^k$. The number p is called the *size* of this expression. A *semilinear* set [10] is a finite union of linear sets. If one is interested in a finite number of semilinear sets, then by taking, if necessary, some of the b_i's equal to $0 \in \mathbb{Z}^k$ we may suppose that all expressions of linear sets involved in these finitely many semilinear sets have the same size. If R is a ring, we use $M_{r,s}(R)$ to denote the set of $r \times s$ matrices with entries in R.

Lemma 2.1. *Let* $\mathcal{F}$ *be an infinite, recursive set of natural numbers closed under taking divisors and least common multiples. Let* $N = \{m_1, m_2, \ldots\} \subseteq \mathcal{F}$ *be such that* m_k *is a divisor of* m_{k+1}*, each* k*, and such that every element of* $\mathcal{F}$ *divides some* m_k*.*

Then given as input $B \in M_{r,st}(\mathbb{Z})$*,* $c \in \mathbb{Z}^r$ *and, for each* $i \in \{1, \ldots, s\}$*, a semilinear subset* $L_i \subseteq \mathbb{Z}^t$ *it is decidable whether, for each* k*, there exists*

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} \in (\mathbb{Z}^t)^s \textit{ such that } x_i \in L_i \textit{ and } BX \equiv c \pmod{m_k}.$$

Proof. As observed, we may assume without loss of generality that the constraints L_i have the form $L_i = \cup_{j=1}^{r_i} L_j^{(i)}$ where

$$L_j^{(i)} = a_j^{(i)} + b_{1,j}^{(i)}\mathbb{N} + \cdots + b_{p,j}^{(i)}\mathbb{N}, \text{ and } a_j^{(i)}, b_{k,j}^{(i)} \in \mathbb{Z}^t.$$

We claim that it suffices to assume that $L_i = L_j^{(i)}$ for some j. Indeed, consider all possible instances of our algorithmic problem obtained by replacing each L_i by one of the $L_j^{(i)}$. Clearly if any of these finitely many new instances has a solution modulo m_k for all k (that is the algorithm outputs "yes" for such an instance), then the original problem has a solution modulo each m_k and hence a positive output. We show the converse by a standard compactness argument. Suppose our system with the original constraints has a solution modulo m_k for all k. Then for each k there is a vector $X_k \in (\mathbb{Z}^t)^s$ with the i^{th} component in some $L_{j_k}^{(i)}$. Since there are infinitely many k but only finitely many indices i, and for each i there are only finitely many sets of the form $L_j^{(i)}$, there must be infinitely many k such that for each i the corresponding set $L_{j_k}^{(i)}$ is the same for these k. That is we can find, for each i, a j_i such that for infinitely many k there is a solution $X = \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix}$ to $BX \equiv c \pmod{m_k}$ with $x_i \in L_{j_i}^{(i)}$, all i. Since a solution modulo m_k is also a solution modulo m_ℓ for all $\ell \leq k$, as $m_\ell \mid m_k$, we see that, for the instance of our problem where L_i is replaced by $L_{j_i}^{(i)}$, we always have a solution modulo m_k, each k. Thus an algorithm for our original problem is simply to check all of the finitely many instances that we have created. Hence we may assume that each $L_i = L_j^{(i)}$ for some j, as claimed.

Say $L_i = a^{(i)} + b_1^{(i)}\mathbb{N} + \cdots + b_p^{(i)}\mathbb{N}$. We write $L_i = a^{(i)} + B_i\mathbb{N}^p$ where $B_i = (b_1^{(i)}|b_2^{(i)}|\cdots|b_p^{(i)}) \in M_{t,p}(\mathbb{Z})$. With this reparameterization, our system with constraints is equivalent to solving modulo each m_k the system

$$B \begin{pmatrix} a^{(1)} + B_1 Y_1 \\ \vdots \\ a^{(s)} + B_s Y_s \end{pmatrix} = c,$$

where each $Y_i \in \mathbb{N}^p$. But this is equivalent to solving modulo each m_k a system of the form $DY = e$ where $D \in M_{r,ps}(\mathbb{Z})$, $e \in \mathbb{Z}^r$ and $Y \in \mathbb{N}^{ps}$.

Equivalently we want to determine whether modulo each m_k it is possible to express e as a non-negative linear combination of the columns of D; that is whether modulo each m_k, e is in the submonoid generated by the columns of D. As every submonoid of a finite group is a subgroup, our problem is equivalent to determining whether modulo each m_k, e is in the subgroup generated by the columns of D. But [17] if H is the pseudovariety of abelian groups with exponent in $\mathcal{F}$, then by the definition of N, this question is equivalent to asking whether e belongs to the pro-H closure in $\mathbb{Z}^r$ of the subgroup generated by the columns of D. Moreover, since $\mathcal{F}$ is recursive, the pseudovariety H is decidable [17]. Now, the results of the third author [17] show that it is decidable whether e belongs to the pro-H closure of the subgroup generated by the columns of D. □

Let us remark that the solvability of the system considered above depends only on $\mathcal{F}$ and not on the choice of N. We now proceed to reduce the complete hyperdecidability of H to the previous lemma. Let M be a (perhaps infinite) monoid. *A system of equations* over M with variables in X is a set E of formal equalities $u = v$ between elements of $M \star X^*$ where $\star$ denotes the free product. The system is said to be *solvable modulo a pseudovariety* V with constraints $L_x \subseteq M$, $x \in X$, if: for each homomorphism $\psi : M \to N \in \mathsf{V}$, we can choose a substitution $\sigma : X \to M$ such that $\sigma(x) \in L_x$, all x, and the map $\overline{\psi} : M \star X^* \to N$ induced from ψ and $\psi \circ \sigma$ satisfies $\overline{\psi}(u) = \overline{\psi}(v)$ for all $u = v \in E$. Solving systems of equations over A^* with rational constraints is very closely related to complete hyperdecidability. This motivates the next theorem.

Theorem 2.1. *Let* H *be a decidable pseudovariety of abelian groups. Then there is an algorithm which, given a finite alphabet* A*, a finite system of equations* E *over* A^* *with variables in* X *and given, for each variable* $x \in X$*, a rational subset* $L_x \subseteq A^*$*, determines whether* E *is solvable modulo* H *with constraints* L_x*,* $x \in X$*.*

Proof. If H is locally finite (that is, contains only finitely many A-generated groups for each finite set A), then the problem is trivial, so we suppose that this is not the case. Suppose $A = \{a_1, \ldots, a_t\}$ and $X = \{x_1, \ldots, x_s\}$. Let $\eta : A^* \to \mathbb{N}^t$ be given by $\eta(w) = (|w|_{a_1}, \ldots, |w|_{a_t})$. Denote by $\eta(E)$ the system $\{\eta(u) = \eta(v) \colon u = v \in E\}$. Then our problem is clearly equivalent to trying to solve $\eta(E)$ modulo H with the constraints

$\eta(L_x)$, $x \in X$. But since each homomorphism of $\mathbb{N}^t$ to an abelian group extends uniquely to $\mathbb{Z}^t$, our problem is equivalent to trying to solve $\eta(E)$ in $\mathbb{Z}^t$ modulo H with the constraints $\eta(L_x)$, $x \in X$ (viewed as subsets of $\mathbb{Z}^t$). We can hence use subtraction to rewrite our system $\eta(E)$ as a linear system of the form $BX = c$ with $B \in M_{r,st}(\mathbb{Z})$ subject to the constraints $\eta(L_x)$, $x \in X$. A theorem of Eilenberg and Schützenberger [10] says that $\eta(L_x)$ is a semilinear set that can be algorithmically be determined from L_x. A more efficient algorithm can be found in the work of the first author [9].

The next step is to obtain a set of positive integers as in Lemma 2.1. Let $\mathcal{F}_{\mathsf{H}} = \{n \mid \mathbb{Z}_n \in \mathsf{H}\}$; this is a recursive set closed under taking divisors and least common multiples [17]. Let us enumerate $\mathcal{F}_{\mathsf{H}}$ as a sequence in increasing order: $n_1 < n_2 < \ldots$. Since we are assuming that H is not locally finite, this sequence is infinite. We define another sequence of positive integers $(m_i)_{i\in\mathbb{N}}$ by setting $m_1 = n_1$ and $m_i = \mathrm{lcm}(m_{i-1}, n_i)$ for all $i > 1$. By construction $m_i \mid m_{i+1}$. Since $\mathcal{F}_{\mathsf{H}}$ is closed under taking least common multiples, $\{m_k\}_{k\in\mathbb{N}} \subseteq \mathcal{F}_{\mathsf{H}}$. By construction each element of $\mathcal{F}_{\mathsf{H}}$ divides some m_k.

Suppose that $\psi : \mathbb{Z}^t \to G \in \mathsf{H}$. Then if n denotes the exponent of G, we must have $n \in \mathcal{F}_{\mathsf{H}}$. Therefore $n \mid m_k$ for all sufficiently large m_k. Hence our system $\eta(E)$ has a solution modulo H if and only if $BX = c$ can be solved modulo each m_k subject to our constraints. But this can be decided according to Lemma 2.1. □

2.1. *Proof of Theorem 1.1*

Let H be a decidable pseudovariety of abelian groups. Let M be a finite monoid, E a finite system of equations in variables X. Let $\sigma : X \to M$ be a substitution. We must decide whether σ is (H, E)-inevitable. Choose a generating set A for M and consider the canonical projection $\varphi : A^* \to M$. A standard argument [13] shows that σ is (H, E)-inevitable if and only if, for all $\psi : A^* \to G \in \mathsf{H}$, there exists a substitution $\sigma' : X \to G$ such that $\sigma' \models E$ and σ' is $\psi\varphi^{-1}$-related to σ. Let $L_x = \varphi^{-1}(\sigma(x))$, for $x \in X$; by Kleene's theorem each L_x is a rational subset of A^*.

A substitution $\sigma' : X \to G$ is τ-related to σ if and only if we can choose for each $x \in X$, an element $w_x \in L_x$ such that $\psi(w_x) = \sigma'(x)$. With this in mind it is straightforward to see that σ is (H, E)-inevitable if and only if E is solvable modulo H with the constraints L_x, $x \in X$. But this can be algorithmically determined by Theorem 2.1. This establishes Theorem 1.1.

2.2. *Proof of Theorem 1.2*

In this proof we assume familiarity with the work of the third author [17] since our example is essentially from there. We will take the following definition of weak κ-reducibility for our non-locally finite pseudovariety H of abelian groups; its equivalence with the usual definition [5, 6] is a standard argument that we leave to the reader. If A is a finite alphabet, we use $\eta_A : A^* \to \mathbb{N}^{|A|}$ for the canonical projection.

Definition 2.1. A pseudovariety of groups H is *weakly κ-reducible* if given a finite alphabet A, a finite graph $\Gamma = V \uplus E$ and a rational subset $L_x \subseteq A^*$ for each $x \in \Gamma$, the following holds: the consistency equations E_Γ for Γ are solvable modulo H subject to the constraints L_x, $x \in \Gamma$, if and only if there exists for each $x \in X$ an element $w_x \in \overline{\eta_A(L_x)}$ such that $\{w_x\}_{x\in\Gamma}$ is a solution to E_Γ in $\mathbb{Z}^{|A|}$. Here $\overline{L_x}$ is the closure of L_x in the pro-H topology on $\mathbb{Z}^{|A|}$, which is the weakest topology making all homomorphisms from $\mathbb{Z}^{|A|}$ to groups in H continuous.

Let p be a prime such that $\mathbb{Z}_p \notin \mathsf{H}$. Let $A = \{a, b\}$. Set $\eta = \eta_{\{a,b\}}$. Consider the graph Γ given by

$$v_0 \xrightarrow{e} v_1 \xrightarrow{f} v_2$$

and consider the labelling

$$1 \xrightarrow{a^*} a^* \xrightarrow{(ab^p)^*} b.$$

The consistency equations are: $v_0 e = v_1$, $v_1 f = v_2$. After abelianization the equations can be written as $v_0 + e = v_1$ and $v_1 + f = v_2$ and so they have the consequence $v_0 + e + f = v_2$. The algorithm [17] shows that $\overline{\eta(a^*)} = (1,0)\mathbb{Z}$ and $\overline{\eta((ab^p)^*)} = (1,p)\mathbb{Z}$. Since $\eta(b) = (0,1)$ is not in $\langle(1,0),(1,p)\rangle$ it follows that $v_0 + e + f = v_2$ cannot be solved in $\mathbb{Z}^{|A|}$ subject to the constrains $\overline{L_x}$, $x \in \Gamma$.

But if we follow the procedure of the proof of Lemma 2.1 we see that we just need that $(0,1)$ is in the pro-H closure of $\langle(1,0),(1,p)\rangle$ for the system to be solvable modulo H with our constraints. But the algorithm [17] shows that the closure of this subgroup is all of $\mathbb{Z}^2$. So the system is solvable modulo H. Thus H is not weakly κ-reducible.

Bibliography

1. J. Almeida, *Hyperdecidable pseudovarieties and the calculation of semidirect products*, Internat. J. Algebra Comput. **9** (1999), 241–261.

2. J. Almeida, *Finite semigroups: an introduction to a unified theory of pseudovarieties*, Semigroups, algorithms, automata and languages (Coimbra, 2001), 3–64, World Sci. Publishing, River Edge, NJ, 2002.
3. J. Almeida, *Dynamics of implicit operations and tameness of pseudovarieties of groups*, Trans. Amer. Math. Soc. **354** (2002), 387–411.
4. J. Almeida and M. Delgado, *Tameness of the pseudovariety of Abelian groups*, Internat. J. Algebra Comput. **15** (2005), 327–338.
5. J. Almeida and B. Steinberg, *Iterated semidirect products with applications to complexity*, Proc. London Math. Soc. **80** (2000), 50–74.
6. J. Almeida and B. Steinberg, *Syntactic and global semigroup theory, a synthesis approach*, pp. 1–23 in: Algorithmic Problems in Groups and Semigroups, J.-C. Birget, S. Margolis, J. Meakin, M. Sapir eds., Birkhäuser, Basel 2000.
7. 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.
8. K. Auinger and B. Steinberg, *On the extension problem for partial permutations*, Proc. Amer. Math. Soc. **131** (2003), 2693–2703.
9. M. Delgado, *Commutative images of rational languages and the abelian kernel of a monoid*, Theor. Inform. Appl. **35** (2001), 419–435.
10. S. Eilenberg and M. P. Schützenberger, *Rational sets in commutative monoids*, J. Algebra **13** (1969), 173–191.
11. K. Henckell, *Pointlike sets: The finest aperiodic cover of a finite semigroup*, J. Pure Appl. Algebra **55** (1988), 85–126.
12. J. Rhodes and B. Steinberg, *Pointlike sets, hyperdecidability, and the identity problem for finite semigroups*, Internat. J. Algebra and Comput. **9** (1999), 475–481.
13. J. Rhodes and B. Steinberg, "The q-theory of finite semigroups", Springer-Verlag, to appear.
14. J. Rhodes and B. Tilson, *Lower bounds for complexity of finite semigroups*, J. Pure Appl. Algebra, **1** (1971), 79–95.
15. J. Rhodes and B. Tilson, *Improved lower bounds for the complexity of finite semigroups*, J. Pure Appl. Algebra, **2** (1972), 13–71.
16. B. Steinberg, *On pointlike sets and joins of pseudovarieties*, Internat. J. Algebra Comput. **8** (1998), 203–231.
17. B. Steinberg, *Monoid kernels and profinite topologies on the free Abelian group*, Bull. Austral. Math. Soc. **60** (1999) 391–402.
18. B. Steinberg, *On algorithmic problems for joins of pseudovarieties*, Semigroup Forum **62** (2001), 1–40.
19. 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. **11** (2001), 25–71.