COMPLETE REDUCIBILITY OF PSEUDOVARIETIES

J. ALMEIDA

Departamento de Matemática Pura, Fac. de Ciências, Universidade do Porto, Rua do Campo Alegre, 687, 4169-007 Porto, Portugal.
E-mail: jalmeida@fc.up.pt

J. C. COSTA

Centro de Matemática, Universidade do Minho, Campus de Gualtar, 4700-320 Braga, Portugal.
E-mail: jcosta@math.uminho.pt

M. ZEITOUN

LaBRI, Université Bordeaux 1 – CNRS 351 cours de la Libération, 33405 Talence Cedex, France.
E-mail: mz@labri.fr

The notion of reducibility for a pseudovariety has been introduced as an abstract property which may be used to prove decidability results for various pseudovariety constructions. This paper is a survey of recent results establishing this and the stronger property of complete reducibility for specific pseudovarieties.

1. Introduction

One of the most fruitful settings for the applications of the theory of finite semigroups in computer science has been formalized by Eilenberg in [25]. The classification of rational languages according to several natural combinatorial properties is translated in terms of the pseudovarieties of finite semigroups to which their syntactic semigroups belong. Several combinatorial constructions on rational languages correspond to algebraic operations on semigroups which have counterparts as operations on pseudovarieties. See [25, 28, 33, 1] for background and examples.

To establish decidability results for certain pseudovariety constructions, one is often led to a decision problem which consists in determining whether a system of equations of some suitable type with rational constraints admits a solution modulo every semigroup of a given pseudovariety V. A stan-

dard compactness argument allows us to transfer this problem to deciding whether the system has a solution in a fixed free pro-V semigroup $\overline{\Omega}_A\mathsf{V}$. Since such semigroups are usually uncountable, these decision problems are hard to handle directly but a successful approach has been devised by Almeida and Steinberg [12, 11]. Under mild hypotheses on V (recursive enumerability) and on the type of equations (recursive enumerability of the corresponding signature, as well as computability of its operations), it is easy to exhibit a semi-algorithm to enumerate the systems which do not have solutions. So, the question amounts to determining whether there is also a semi-algorithm to enumerate those systems that do have solutions. Since there are too many candidates for solutions, the next idea is to reduce the universe where solutions need to be sought. This leads to the reducibility property: if the system admits a solution then it admits a solution of a special type. The universe of candidates for solutions that is most often encountered consists of the smallest subsemigroup of the free profinite semigroup $\overline{\Omega}_A\mathsf{S}$ containing the free generators which is closed under unary pseudo-inversion $s \mapsto s^{\omega-1}$. If the reducibility property holds for every finite system of equations, then we say that V is completely reducible. For the method to be successful, besides this reducibility property, one needs the decidability of a word problem so as to be able to determine whether a candidate for a solution is actually a solution.

This paper is a survey of reducibility results for pseudovarieties. We also present a sketch of a proof that the pseudovariety R, of all finite $\mathcal{R}$-trivial semigroups, is completely reducible. The proof is inspired by Makanin's algorithm to decide whether a finite system of word equations with rational constraints has a solution in the free semigroup [30, 31, 29]. It suggests new connections between Finite Semigroup Theory and Combinatorics on Words which deserve further investigation. The full details of the proof will appear elsewhere [6].

2. How we are led to systems of equations

We start by illustrating with two examples how decision problems for systems of equations come up when trying to prove decidability of pseudovariety constructions through bases of pseudoidentities for such pseudovarieties.

Let Sl denote the pseudovariety $[\![x^2 = x, xy = yx]\!]$ of all finite semilattices. Given any pseudovariety V, the *Basis Theorem* for semidirect products [16][a] gives the following basis of pseudoidentities for the semidirect

[a]The proof of the Basis Theorem is known to have a gap in its full generality, although

product of Sl with V:

$$\mathsf{Sl} * \mathsf{V} = [\![wu^2 = wu,\ wuv = wvu :\ \mathsf{V} \models wu = wv = w]\!].$$

Thus, to check whether a given finite semigroup S belongs to $\mathsf{Sl} * \mathsf{V}$, it suffices to verify the following condition:

> let $\bar{w}, \bar{u}, \bar{v} \in S$ be such that at least one of the inequalities $\bar{w}\bar{u}^2 \neq \bar{w}\bar{u}$ and $\bar{w}\bar{u}\bar{v} \neq \bar{w}\bar{v}\bar{u}$ holds; then there are no elements $w, u, v \in \overline{\Omega}_A\mathsf{S}$ and evaluation of the generators A in S such that:
>
> (1) w, u, v are evaluated to $\bar{w}, \bar{u}, \bar{v}$, respectively;
> (2) $\mathsf{V} \models wu = wv = w$.

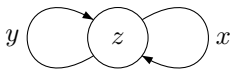
Thus, we are led to consider the system of equations $zx = zy = z$ upon whose variables x, y, z we impose constraints in the semigroup S. We would like to be able to decide whether there is some *solution of the system modulo* V in the sense that the above conditions (1) and (2) hold.

A similar example is provided by Mal'cev products. Bases of pseudoidentities for Mal'cev products have been described by Pin and Weil [34]:

$$\mathsf{Sl} \mathbin{Ⓜ} \mathsf{V} = [\![u^2 = u,\ uv = vu :\ \mathsf{V} \models u^2 = u = v]\!].$$

Here, the system consists of the equations $x^2 = x = y$. But, otherwise, the nature of the decision problem is the same: to be able to decide whether, imposing constraints for the variables in a given finite semigroup, the system admits a solution modulo every semigroup from V.

The type of equations that appear depends on the operation on pseudovarieties that one is interested in computing and on a certain parameter from the "other" pseudovariety. In the above cases, the parameter is respectively a graph[b]



upon which a basis of pseudoidentities for the global[c] gSl may be written, and the "rank" of the pseudovariety Sl, that is the minimum number of variables in a basis of pseudoidentities defining it.

its validity remains open. See [3, 42, 36] for further information.

[b] We associate a system of equations to a finite directed graph by viewing each edge and each vertex as a variable and writing the equation $xy = z$ for each edge $x \xrightarrow{y} z$.

[c] The global of a pseudovariety of semigroups is the pseudovariety of semigroupoids which it generates and the restriction under which the Basis Theorem for semidirect products is known to be valid is that the global of the first factor admit a basis of pseudoidentities over graphs with a bounded number of vertices.

In general, we are given a finite system of equations $u_i = v_i$ $(i \in I)$ over a finite set X of variables for which constraints are chosen in a given finite semigroup S: s_x $(x \in X)$. By a *solution of the system modulo* an A-generated profinite semigroup T we mean a mapping $\varphi : X \to \overline{\Omega}_A\mathsf{S}$ into the free profinite semigroup $\overline{\Omega}_A\mathsf{S}$ over the set A, together with a continuous homomorphism $\psi : \overline{\Omega}_A\mathsf{S} \to S$ such that the following conditions hold:

(1) $\forall x \in X,\ \psi(\varphi(x)) = s_x$;
(2) $\forall i \in I,\ \theta\hat{\varphi}(u_i) = \theta\hat{\varphi}(v_i)$,

where $\hat{\varphi}$ is the unique extension of φ to a continuous homomorphism $\overline{\Omega}_X\mathsf{S} \to \overline{\Omega}_A\mathsf{S}$ and $\theta : \overline{\Omega}_A\mathsf{S} \to T$ is the unique continuous homomorphism determined by the choice of generators. In case $T = \overline{\Omega}_A\mathsf{V}$, we speak of a *solution modulo* V. The problem is to decide whether such a solution exists.

There are a number of reformulations and generalizations which we proceed to present. See [3] for further details. First, it suffices to consider onto continuous homomorphisms $\psi : \overline{\Omega}_A\mathsf{S} \to S$, in which case the existence of a solution modulo V is independent of the finite set A. Second, for a fixed onto continuous homomorphism $\psi : \overline{\Omega}_A\mathsf{S} \to S$, the constraints may be lifted to constraint sets in $\overline{\Omega}_A\mathsf{S}$ which are therefore clopen subsets of $\overline{\Omega}_A\mathsf{S}$, that is closures of rational languages of the free semigroup A^+. In this form, the problem is formulated entirely as a problem in the free profinite semigroup $\overline{\Omega}_A\mathsf{S}$: the analogous problem with constraints given by clopen subsets of a fixed free profinite semigroup $\overline{\Omega}_A\mathsf{S}$, where solutions modulo V are sought, is equivalent to the original problem. It may be useful to have variables for which there is no room for choice for their values, that is they play the role of *parameters*. The equations $u_i = v_i$ may be given by pseudowords,[d] that is we may consider *pseudo-equations* instead of *word equations*.

As mentioned in the Introduction, it is not hard to obtain a semi-algorithm for non-solvability. If the system has a solution in $\overline{\Omega}_A\mathsf{S}$ modulo V then it also has a solution modulo any A-generated semigroup from V: every solution modulo V has that property. By a compactness theorem, the converse is also true. For a specific A-generated semigroup T from V, the problem of existence of solutions modulo T can be solved by checking a finite number of candidates. Thus, the existence of solutions modulo V for finite systems of word equations is (theoretically) decidable if we can

[d]Elements of $\overline{\Omega}_A\mathsf{S}$ may be called *pseudowords* when they are viewed as combinatorial entities generalizing finite words, or *implicit operations* if they are identified with such operations via their natural interpretation as operations on finite semigroups.

also exhibit a semi-algorithm that enumerates the solvable systems. The difficulty is that, $\overline{\Omega}_A\mathsf{S}$ being uncountable for every non-empty set A, there are too many candidates for solutions. Moreover, we need to be able to determine whether a candidate for a solution modulo V actually has this property, namely whether it satisfies the constraints and the equations, modulo V. The first difficulty is overcome if we can reduce the existence of solutions modulo V in $\overline{\Omega}_A\mathsf{S}$ to the existence of solutions modulo V in some recursively enumerable subset of $\overline{\Omega}_A\mathsf{S}$. A setting for performing such a reduction was proposed in [11]: a subalgebra $\Omega_A^\sigma\mathsf{S}$ of $\overline{\Omega}_A\mathsf{S}$ for an *implicit signature* σ, that is a signature consisting of binary multiplication together with some implicit operations, which have a natural interpretation in every finite semigroup. The computational requirements for such a signature are: (1) it should be recursively enumerable (so that we may enumerate the members of $\Omega_A^\sigma\mathsf{S}$); (2) its operations should be computable in finite semigroups (so that we may check the constraints); (3) the word problem for $\Omega_A^\sigma\mathsf{V}$ should be solvable (so that we may verify whether the equations hold modulo V).

We say that V is *σ-reducible* with respect to a class of equation systems if the existence of a solution modulo V of any system in the class entails the existence of a solution in σ-terms. In case the class consists of all finite systems of equations of σ-terms (with parameters also given by σ-terms), we say that V is *completely σ-reducible*. If the class consists of all systems of equations associated with finite graphs, then we say that V is *σ-reducible*.

An example of a common candidate for such a signature consists of multiplication together with the unary pseudo-inversion $x \mapsto x^{\omega-1}$. It is called the *canonical signature* and denoted κ; whether it is suitable or not depends on the pseudovariety V, as we need the word problem for $\Omega_A^\kappa\mathsf{V}$ and the appropriate κ-reducibility property. Here are some examples: the pseudovariety G of all finite groups is κ-reducible [17][e] but not completely

[e]For groups, κ-reducibility admits a different type of formulation which was originally established by Ash; the equivalence between the two formulations can be found in [11]. Ash obtained his results as a means to prove the *Rhodes Type II Conjecture*, whose history and relevance is explained in [26]. Independently and roughly at the same time, the conjecture was also proved by Ribes and Zalesskiĭ [37] through the theory of profinite groups. In turn, their result was translated into a result in Model Theory which was extended by Herwig and Lascar [27] into a deep result about the existence of extensions to automorphisms (of perhaps larger finite structures) of partial automorphisms of finite relational structures, together with a technical formulation of the same result as a property about free groups, which explains the connection with the Ribes and Zalesskiĭ Theorem. The formal equivalence of the latter with Ash's Theorem was recognized in [7, 8]. The

κ-reducible [24]; for a prime p, the pseudovariety G_p of all finite p-groups is not κ-reducible but it is σ-reducible for a certain infinite signature σ [2]; the pseudovariety Ab of all finite Abelian groups is completely κ-reducible [9]; the pseudovariety OCR of all finite orthodox completely regular semigroups is κ-reducible [13]; the pseudovariety CR of all finite completely regular semigroups is κ-reducible [14][f]; the pseudovariety LSl of all finite semigroups S whose local subsemigroups eSe are semilattices is κ-reducible [23]; the pseudovariety R is κ-reducible [5]; the pseudovariety J of all finite $\mathcal{J}$-trivial semigroups is completely κ-reducible [3]. The κ-reducibility of the pseudovariety A of all finite aperiodic semigroups was announced by J. Rhodes in 1997 but no proof has yet been published. The word problem for $\Omega_A^\kappa \mathsf{A}$ was solved by McCammond [32] and, independently, by Zhil'tsov [43].

Although the join operation is not as amenable to decidability proofs through reducibility arguments as the semidirect and Mal'cev products, there have been investigations in this direction. Both proofs of decidability of $\mathsf{J} \vee \mathsf{G}$ [4, 38], obtained independently, use some form of reducibility of G and J. The same approach has also been used to study other joins [40, 5].

3. Simplifications

There are a number of simplifications of the problem which we proceed to examine. See [6] for details.

A first simplification consists in observing that parameters may be captured by adding extra variables and constraining them suitably: σ-reducibility for systems without parameters implies σ-reducibility for systems with parameters given by σ-terms.

Say that a pseudovariety is *weakly cancellable* if, whenever it satisfies the pseudoidentity $u_1 \# u_2 = v_1 \# v_2$, where the letter $\#$ does not occur in u_1, u_2, v_1, v_2, it also satisfies the pseudoidentities $u_1 = v_1$ and $u_2 = v_2$. Many familiar pseudovarieties are weakly cancellable: A, R, J, CR, DA (finite semigroups in which regular elements are idempotent), DO (finite semigroups in which regular $\mathcal{D}$-classes are orthodox subsemigroups), DS (finite semigroups in which regular $\mathcal{D}$-classes are subsemigroups), and locally extensible pseudovarieties of groups in the sense of [22].[g] If V is weakly

connections between the two approaches to the Type II Conjecture have been extensively investigated by Steinberg, later joined by Auinger [41, 39, 20, 18, 21].

[f] As has been observed by K. Auinger in a private communication, the stronger version of κ-reducibility for G which is needed in [14] can be established using the methods of [7, 8].

[g] See the Appendix for a characterization of weak cancellability in pseudovarieties of groups.

cancellable and σ-reducible for systems consisting of just one equation of σ-terms, without any parameters, then V is completely σ-reducible.

Another simplification stems from the relationship between the canonical signature κ and the alternative signature in which the unary pseudoinversion is replaced by the ω-power operation $x \mapsto x^\omega = x^{\omega-1}x$. Since, for finite aperiodic semigroups, the two operations coincide, the following result is not surprising, although it does require a proof: if V is an aperiodic pseudovariety, then V is κ-reducible for an arbitrary system if and only if it is reducible for the same system with respect to the signature consisting of multiplication and the operation $x \mapsto x^\omega$.

4. Further simplifications for the case of R

In this paper, we pay special attention to the case of the pseudovariety R, for which there are also some specific simplifications of the reducibility problem which apply.

From the general simplifications of the preceding section, we know that, if R is κ-reducible for systems consisting of a single equation of κ-terms without parameters, then R is completely κ-reducible. In fact, it suffices to consider word equations. The idea is to express that an initial subterm t is an ω-power of u by the word equation $ut = t$. This leads to a finite system of word equations which may then be transformed into a single word equation taking into account that R is weakly cancellable.

For a pseudoword $w \in \overline{\Omega}_A\mathsf{S}$, let $c(w)$ be the set of all letters $a \in A$ which are factors of w and let $\vec{c}(w) = \{a \in A : \mathsf{R} \models wa = w\}$.

A solution δ modulo R of the equation $u = v$ is said to be R-*reduced with respect to* $u = v$ if it has the following property: for every factor xy of uv, where x and y are variables, if z is the first letter of $\delta(y)$, then $\mathsf{R} \not\models \delta(x)z = \delta(x)$. Suppose that R is κ-reducible for systems of word equations without parameters which involve one general equation $u = v$ and all other equations of the form $xy = x$, where x and y are variables, and which admit solutions modulo R which are R-reduced with respect to the equation $u = v$. Then R is completely κ-reducible. The idea here is to factorize each $\delta(x)$ as $a_1u_1a_2u_2\cdots a_{n_x}u_{n_x}$ where the a_i are letters and indicate their leftmost occurrences in $\delta(x)$. One may introduce n_x new variables $y_{x,i}$ to represent the intermediate factors u_i (depending on x) as well as variables z_a to represent the individual letters a from the alphabet. Upon the variable $y_{x,i}$ is imposed a constraint which requires that $c(y_{x,i}) \subseteq \{a_1, \ldots, a_i\}$. In turn, the variables z_a are constrained to be equal to a. In the original equation,

for each two-letter factor x_1x_2, we expand the variable x_2 according to the factorization of its value in a solution δ modulo R, replacing x_2 by the associated product $z_{a_m}y_{x_2,m}\cdots z_{a_{n_{x_2}}}y_{x_2,n_{x_2}}$, where a_m is the first letter in $\delta(x_2)$ which does not belong to $\vec{c}(\delta(x_1))$, dropping x_2 altogether at that position in the equation if $c(\delta(x_2)) \subseteq \vec{c}(\delta(x_1))$. The resulting finite system of word equations may be compressed into a single word equation by the tricks of the preceding section. To retain the information about the value of each $\vec{c}(\delta(x))$, we add the equations $y_{x,n_x}z_a = y_{x,n_x}$ whenever $a \in \vec{c}(\delta(x))$.

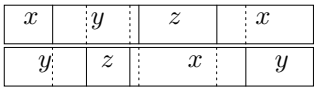
5. Complete reducibility of R

The aim of the remainder of the paper is to sketch a proof of the following result from [6]. Weaker forms were previously established in [10] and [5].

Theorem 1. *The pseudovariety* R *is completely* κ*-reducible.*

In the sequel, we try as much as possible to formulate the arguments in a more general setting, thus referring to a general pseudovariety V.

Let $u = x_1\cdots x_r$, $v = x_{r+1}\cdots x_s$, where the x_i are not necessarily distinct variables from a set X. Suppose that $\varphi : X \to \overline{\Omega}_A\mathsf{S}$ is a solution of the equation $u = v$ modulo a given pseudovariety V, satisfying prescribed constraints in a finite semigroup S. Suppose that V determines some kind of unique factorization in the free profinite semigroup $\overline{\Omega}_A\mathsf{S}$ and that we may assume that the solution is such that the resulting factorizations of u and v under the solution are of that kind. Then the two factorizations must match. For example, if we have a solution of the equation $xyzx = yzxy$, then the two factorizations of the common value of the words $xyzx$ and $yzxy$ must match, say as indicated in the following diagram:

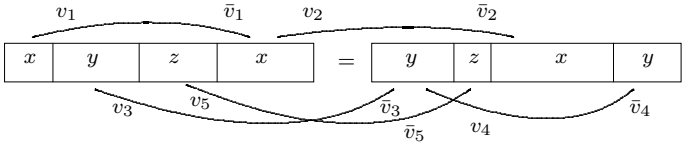


The factorizations of the value of a variable corresponding to its different occurrences in the equation must also be matched and this leads to the successive refinement of factorizations. How to manage the propagation of these factorizations which, for pseudowords, may perhaps have to be carried *ad infinitum*?

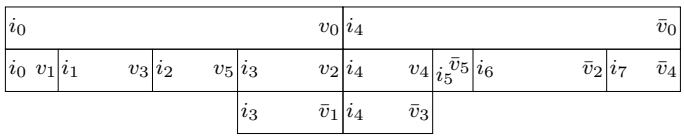
For R the propagation of factorizations has been successfully handled in [5] in the case of systems of equations associated with finite graphs. The case of arbitrary word equations is much more delicate. The management of

the propagation of factorizations is done by adapting ideas from Makanin's algorithm to decide whether a finite system of word equations with rational constraints admits a solution in the free monoid [30, 31]. There is a recent more efficient (PSPACE) algorithm, due to Plandowski [35]. Since we are concerned at present with an abstract property rather than the construction of an algorithm, there is no complexity issue for us, and so we preferred to use Makanin's ideas, with which we are more familiar, and which, perhaps therefore, seem more adjusted to the current problem.

One of the simple ideas in Makanin's algorithm is to organize the matching of factorizations by only matching a couple of factorizations of the same word at a time. For instance, for the equation $xyzx = yzxy$, the matching might be done as indicated in the following diagram:



The variables v_0 and $\bar{v}_0$ are used to match the common value of both sides of the equation. Each *box* is identified by the *position* i of its beginning (its *left*) together with the new *variable* v_k or $\bar{v}_k$ that determines it:



The *right* of a box is where it ends. A quadruple of the form $(i, v, j, \bar{v})$ is called a *boundary equation*. Each of the pairs (i, v) and $(j, \bar{v})$ that constitute it corresponds to a box in the diagram and thus to a pseudoword under the given solution of the original equation. The two pseudowords thus obtained define a pseudoidentity which is valid in V.

If we are working with finite words, as in Makanin's algorithm, when we use a boundary equation $(i, v, j, \bar{v})$ to match two segments of a solution, the words are actually equal and therefore we do not have to worry about carrying along the constraint value. For pseudowords and solutions modulo V, the situation is more complicated: under the solution, the two sides are not really equal but only equal over V. One might formulate the constraints in terms of conditions in $\overline{\Omega}_A\mathsf{V}$ but then what we get are in general only closed sets, rather than clopen sets, and thus a finiteness condition is lost which turns out to be essential in our reduction arguments.

Suppose the constraints are given by values in a finite A-generated semigroup. Although initially we only have one constraint for each pair of consecutive positions, corresponding to the value assigned to a variable under a solution of the equation modulo V, as we start refining factorizations the constraint values must be factorized accordingly, and in S the factorization will not be unique. In other words, the pseudowords coming from the solution of the original equation show that the constraining subsets must be V-*pointlike*. This leads to the following special case of κ-reducibility for R which can be found in [5] in a slightly different form.

Proposition 2. *Let $\varphi : \overline{\Omega}_A\mathsf{S} \to S$ be a continuous homomorphism and let $u_1, \ldots, u_n \in \overline{\Omega}_A\mathsf{S}$ be pseudowords such that $\mathsf{R} \models u_1 = \cdots = u_n$. Then there exist $w_1, \ldots, w_n \in \Omega_A^\kappa\mathsf{S}$ such that the following conditions hold:*

(1) $\mathsf{R} \models w_1 = \cdots = w_n$;
(2) $\varphi(u_i) = \varphi(w_i)$ $(i = 1, \ldots, n)$;
(3) $c(u_i) = c(w_i)$ $(i = 1, \ldots, n)$;
(4) $\vec{c}(u_i) = \vec{c}(w_i)$ $(i = 1, \ldots, n)$.

Unlike the case of finite words, factorizations of pseudowords may continue forever. However, due to periodicity phenomena in the constraints, one may hope to control infinite refinements through the replacement of segments in the original solution by ω-terms. In Makanin's algorithm, decidability follows from a very delicate and complicated analysis of how periodicity phenomena in S allow to compute a bound for the number of times a refinement needs to be performed. Plandowski [35] describes it as *one of the most complicated termination proofs existing in the literature*.

6. General strategy of the proof

The basic reason why appropriate factorizations exist for the pseudovariety R are the following. We say that a pseudoword is *end-marked* if it is of the form wa with $\mathsf{R} \not\models wa = w$, where a is a letter. End-marked pseudowords enjoy some important properties which we quote from [5], where further references to related literature may also be found. If ua and vb are end-marked pseudowords such that $ua\mathcal{R}vb$, then $a = b$ and $u = v$ ($\mathcal{R}$-triviality). There are no infinite ascending $\leq_{\mathcal{R}}$-chains of end-marked pseudowords over a finite alphabet (well-foundedness). Suppose that u and v are two prefixes of the same element of $\overline{\Omega}_A\mathsf{S}$. Then one of them is a prefix of the other (unambiguous $\mathcal{R}$-order). This provides another proof of the characterization of A-pseudowords over R as "reduced A-labeled ordinals" found in [15].

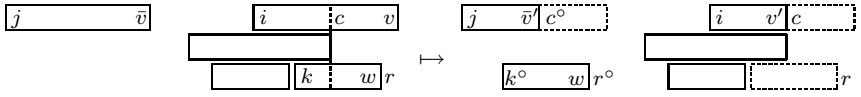
The positions in the factorizations will thus be determined by certain ordinals smaller than the ordinal of the given solution. Now, the basic strategy of the proof should be clear: to use the boundary equations to reduce the maximum of the positions which appear in boxes or the number of boxes which end at that maximum. In an ordinal, such a procedure can only be carried out a finite number of times. The difficulty is that, unlike what happens for finite words, we may very well have $\mathsf{R} \models u = v$ with u a proper suffix of v, but not a proper prefix, assuming that in all factorizations that we consider factors stop just short of the last letter of an end-marked prefix. Yet such cases lead to periodicity phenomena which we have managed to handle. A boundary equation $(i, v, j, \bar{v})$ is said to be *elastic* if it has the following form:

To proceed, we distinguish three cases which require different strategies. The description of the strategy will be essentially pictorial, which makes it somewhat imprecise. Also, we will make no further reference to the crucial detail of how the constraints need to be factorized as the factorizations for the values of each variable are merged. Full details are provided in [6].

Case A. Suppose that there is a "rightmost" boundary equation $(i, v, j, \bar{v})$ which is elastic and such that, under the given solution, not all letters which occur in the box (i, v) occur in the factor between the positions i and j. Then one may introduce a new position k which corresponds to the first letter in the box (i, v) which does not occur in the factor between the positions i and j and replace the boundary equation $(i, v, j, \bar{v})$ by $(i, v', j, \bar{v}')$:

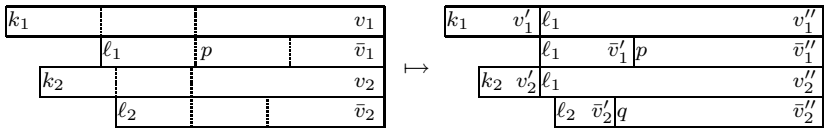
Case B. Suppose that Case A does not hold and that there is at least one boundary equation $(i, v, j, \bar{v})$ whose box (i, v) ends at a maximum position for all boxes and such that the box $(j, \bar{v})$ ends earlier. Among all such boundary equations, we may choose one such that i is minimum and, by an argument of pushing forward periods in elastic equations which is sketched in Case C, we may also assume that there are no elastic boundary equations for which one of the boxes includes the position i and ends at the same position as (i, v). Then we may proceed as in Makanin's algorithm: let c be the *critical boundary* defined by $c = \max\{c', i\}$ where $c' = \max\{\mathrm{right}(w) : \mathrm{left}(w) < i\}$. We have to transport the constraints of

the segment $(c, \mathrm{right}(v))$ to the corresponding segment $(c^\circ, \mathrm{right}(\bar{v}))$, where, as ordinals, $p^\circ - j = p - i$. These segments are then handled by Proposition 2 and can be dropped from the boundary equation $(i, v, j, \bar{v})$. Additionally, we transport all boxes (k, w) crossing c to their corresponding segment of $(j, \mathrm{right}(\bar{v}))$. The diagram of boxes might include those on the left, in which case we transform it to the one on the right:



Case C. Suppose that all boundary equations which have a box which ends at the maximum position where boxes end are elastic and that none of the previous cases hold. Under the given solution, each such boundary equation $(k_i, v_i, \ell_i, \bar{v}_i)$ $(i = 1, \ldots, m)$ determines a pseudoidentity of the form $u_i w_i = w_i$ such that $\mathsf{R} \models u_i w_i = w_i$, where, assuming that $k_i < \ell_i$, u_i corresponds to the box which starts at position k_i and ends just short of position ℓ_i, while w_i corresponds to the box $(\ell_i, \bar{v}_i)$. Since Case A does not hold, we must have $c(u_i) = c(w_i)$ and so the pseudoidentity $u_i w_i = w_i$ is equivalent, for R, to $w_i = u_i^\omega$, which forces a periodicity phenomenon. This periodicity has to be carefully combined with periodicity in the constraints.

The first step consists in synchronizing the periods of the various elastic boundary equations involved so that a similar situation is produced with all k_i equal. This can be achieved by breaking up the boxes by a process which we call *pushing forward the period* and which is depicted in the following diagram which, for simplicity, considers the case of two boundary equations:



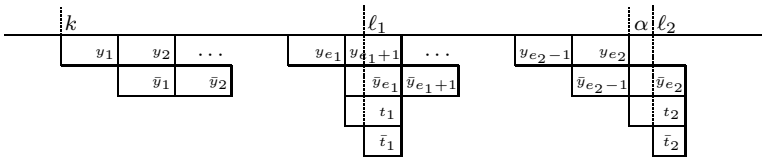
The positions p and q are such that the factors corresponding to the pairs of boxes $(k_1, v_1'), (\ell_1, \bar{v}_1')$ and $(k_2, v_2'), (\ell_2, \bar{v}_2')$ determine pseudoidentities which are valid in R. The boundary equations $(k_1, v_1, \ell_1, \bar{v}_1)$ and $(k_2, v_2, \ell_2, \bar{v}_2)$ are replaced by new boundary equations $(k_1, v_1', \ell_1, \bar{v}_1')$, $(\ell_1, v_1'', p, \bar{v}_1'')$, $(k_2, v_2', \ell_2, \bar{v}_2')$, and $(\ell_1, v_2'', q, \bar{v}_2'')$.

The same strategy works in general and hence we may assume that all k_i are equal to the same k, which implies that R satisfies all pseudoidentities of the form $u_i w_i = w_i = w_j$, so that the w_i have a value w over R which is independent of i and $\mathsf{R} \models w = u_i^\omega$ for $i = 1, \ldots, m$. To handle this

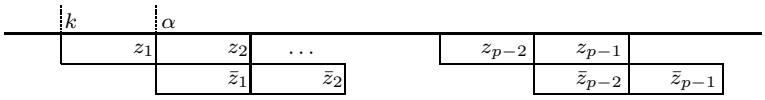
situation, we have the following multi-periodicity result.

Proposition 3. *Let $u_1, \ldots, u_m$ be pseudowords over A such that R satisfies $u_1^\omega = \cdots = u_m^\omega$. Assume that, for all i, the product $u_i u_i$ is reduced. Then, there exist $z \in \overline{\Omega}_A\mathsf{S}$, $r_i \in \overline{\Omega}_A\mathsf{S}^1$, and integers $k_i > 0$ such that R satisfies the pseudoidentities $u_i = z^{k_i} r_i$ and $z = r_i z$, for all $i = 1, \ldots, n$, where all the products and zz are reduced.*

We introduce new boundary equations to capture the refined period z given by Proposition 3, along with its periods r_i ($i = 1, 2, \ldots$):



Finally, we indicate how the constraints are used to show that a solution modulo R in κ-terms must exist if there is some solution modulo R. It is well known that, for a finite semigroup S, there are integers h and p such that $1 < h < p$ and, for all $s_1, \ldots, s_p \in S$, $s_1 \cdots s_p = s_1 \cdots s_h (s_{h+1} \cdots s_p)^\omega$. We drop the boundary elastic equations whose boxes end at the maximum position where any boxes end and we introduce new boundary equations to capture the repetition p times of the longest period encountered so far:



The proof of Theorem 1 is achieved by showing that each time we change our system of boundary equations we obtain a system which still admits a solution modulo V and, conversely, such that if the new system admits a solution in κ-terms then so does the old one.

Appendix

As has been pointed out by the anonymous referee, for pseudovarieties of groups, local extensibility is sufficient but not necessary for weak cancellability. Indeed, for a pseudovariety V of groups, the weak cancellation property may be reformulated as follows. Over V, the non-trivial pseudoidentity $u_1 \# u_2 = v_1 \# v_2$ is equivalent to one of the form $u\# = \#v$ for pseudowords u and v, with the letter $\#$ not occurring in them, such that V does not satisfy both pseudoidentities $u = 1$ and $v = 1$. Substituting u for the letter $\#$, we deduce the pseudoidentity $u^2 = uv$, so that $u = v$ holds

in V. Hence, the original pseudoidentity $u_1\#u_2 = v_1\#v_2$ is equivalent to one of the form $u\# = \#u$ over V, where $\#$ is a letter not occurring in the non-trivial pseudoword u. This shows that V is not weakly cancellable if and only if there is a finitely generated free pro-V group with a non-trivial central element which does not use all free generators. The referee further asked whether it is sufficient for non-weak cancellability of V for $\overline{\Omega}_A\mathsf{V}$ to have a non-trivial center whenever A is a non-empty finite set.

Before giving a negative answer to the preceding question, we proceed to consider a special kind of pseudovarieties of groups. Say that a group is *centerless* if its center is trivial.

Proposition 4. *Let V be a pseudovariety which is generated by some family $\mathcal{C}$ of centerless groups. Then V is weakly cancellable.*

Proof. Let u be a non-trivial element of $\overline{\Omega}_A\mathsf{V}$ which belongs to the closed subgroup generated by $A \setminus \{a\}$ for some $a \in A$. Then there is some group G in $\mathcal{C}$ and some continuous homomorphism $\varphi : \overline{\Omega}_{A\setminus\{a\}}\mathsf{V} \to G$ such that $\varphi(u) \neq 1$. Since G has trivial center, there is some $g \in G$ which does not commute with $\varphi(u)$. Now, we may extend φ to a continuous homomorphism $\psi : \overline{\Omega}_A\mathsf{V} \to G$ by letting $\psi(a) = g$ and $\psi(b) = \varphi(b)$ for $b \in A \setminus \{a\}$. Since $\psi(a)$ and $\psi(u)$ do not commute, we conclude that u is not central in $\overline{\Omega}_A\mathsf{V}$. Hence the pseudovariety V is weakly cancellable by the referee's remark. □

For an example, let S_3 denote the symmetric group on three symbols and let $\mathsf{V}(S_3)$ be the pseudovariety it generates. By Proposition 4, $\mathsf{V}(S_3)$ is weakly cancellable, while, as any locally finite pseudovariety of groups, it is not locally extensible. We claim that $\overline{\Omega}_A\mathsf{V}(S_3)$ has a non-trivial center for every non-empty finite set A, which provides a negative answer to the question raised by the referee. The claim is proved by recursively exhibiting central elements.

Lemma 5. *Let $A_n = \{x_1, \ldots, x_n\}$ and define recursively a sequence u_n by taking $u_1 = x_1$ and $u_{n+1} = (u_n x_{n+1}^3 u_n)^2$. Then u_n is a non-trivial central element in the group $G_n = \overline{\Omega}_{A_n}\mathsf{V}(S_3)$.*

Proof. Let $w \mapsto \overline{w}$ denote an arbitrary homomorphism $G_n \to S_3$. If we take $\overline{x}_2 = \cdots = \overline{x}_n = 1$, then $\overline{u}_n = \overline{x}_1^{4^{n-1}}$ so that $\overline{u}_n \neq 1$ if we choose for $\overline{x}_1$ a 3-cycle. Hence $u_n \neq 1$.

To prove that u_n is in the center of G_n, we proceed by induction on n, the case $n = 1$ being trivial. Given elements $\overline{x}_1, \ldots, \overline{x}_{n+1} \in S_3$, denote

by Z_k the center of the subgroup H_k generated by $\overline{x}_1, \ldots, \overline{x}_k$. We assume that, given $\overline{x}_1, \ldots, \overline{x}_{n+1} \in S_3$, $\overline{u}_n \in Z_n$ and we claim that $\overline{u}_{n+1} \in Z_{n+1}$. If $\overline{u}_n$ commutes with $\overline{x}_{n+1}$ then $\overline{u}_{n+1} = (\overline{u}_n \overline{x}_{n+1}^3 \overline{u}_n)^2 = \overline{u}_n^4 \overline{x}_{n+1}^6 = \overline{u}_n^4$, which shows that $\overline{u}_{n+1} \in Z_{n+1}$. Hence, we may assume that $\overline{x}_{n+1}$ does not commute with $\overline{u}_n$, which implies that $\overline{u}_n$ does not belong to the subgroup generated by $\overline{x}_{n+1}$ and, by induction hypothesis, that $\overline{x}_{n+1} \notin H_n$. We claim that, under these circumstances, $\overline{u}_{n+1} = 1$.

Indeed, if $\overline{u}_n$ is a 3-cycle, then $\overline{x}_{n+1}$ is a 2-cycle and so $\overline{u}_n \overline{x}_{n+1}^3 \overline{u}_n = \overline{x}_{n+1}$ and $\overline{u}_{n+1} = \overline{x}_{n+1}^2 = 1$. Assume next that $\overline{u}_n$ is a 2-cycle. If $\overline{x}_{n+1}$ is a 3-cycle, then $\overline{u}_{n+1} = \overline{u}_n^4 = 1$. If $\overline{x}_{n+1}$ is also a 2-cycle, then $\overline{u}_n \overline{x}_{n+1}^3 \overline{u}_n$ is again a 2-cycle and so $\overline{u}_{n+1} = 1$. □

The above lemma serves only to handle a very special example. We do not know how far it can be generalized, that is which non-trivial finite groups G have the property that the center of $\overline{\Omega}_{A_n}\mathsf{V}(G)$ is non-trivial for every $n \geq 1$. But, of course, this is a remotely marginal question for the theme of this paper.

Acknowledgments

The work of J. Almeida was (partially) supported by the *Centro de Matemática da Universidade do Porto* (CMUP), financed by FCT (Portugal) through the programmes POCTI and POSI, with national and European Community structural funds. The work of J. C. Costa was supported, in part, by FCT through the *Centro de Matemática da Universidade do Minho*. The work of M. Zeitoun was partly supported by the European research project HPRN-CT-2002-00283 GAMES.

References

1. J. Almeida, *Finite Semigroups and Universal Algebra*, World Scientific, Singapore, 1995. English translation.
2. ———, *Dynamics of implicit operations and tameness of pseudovarieties of groups*, Trans. Amer. Math. Soc. **354** (2002) 387–411.
3. ———, *Finite semigroups: an introduction to a unified theory of pseudovarieties*, in Semigroups, Algorithms, Automata and Languages, G. M. S. Gomes, J.-E. Pin, and P. V. Silva, eds., Singapore, 2002, World Scientific, 3–64.
4. J. Almeida, A. Azevedo, and M. Zeitoun, *Pseudovariety joins involving $\mathcal{J}$-trivial semigroups*, Int. J. Algebra Comput. **9** (1999) 99–112.
5. J. Almeida, J. C. Costa, and M. Zeitoun, *Tameness of pseudovariety joins involving R*, Monatsh. Math. **146** (2005) 89–111.

6. ———, *Complete reducibility of systems of equations with respect to R*. In preparation.
7. J. Almeida and M. Delgado, *Sur certains systèmes d'équations avec contraintes dans un groupe libre*, Portugal. Math. **56** (1999) 409–417.
8. ———, *Sur certains systèmes d'équations avec contraintes dans un groupe libre—addenda*, Portugal. Math. **58** (2001) 379–387.
9. ———, *Tameness of the pseudovariety of Abelian groups*, Int. J. Algebra Comput. **15** (2005) 327–338.
10. J. Almeida and P. V. Silva, *SC-hyperdecidability of* $\boldsymbol{R}$, Theor. Comp. Sci. **255** (2001) 569–591.
11. J. Almeida and B. Steinberg, *On the decidability of iterated semidirect products and applications to complexity*, Proc. London Math. Soc. **80** (2000) 50–74.
12. ———, *Syntactic and Global Semigroup Theory, a Synthesis Approach*, in Algorithmic Problems in Groups and Semigroups, J. C. Birget, S. W. Margolis, J. Meakin, and M. V. Sapir, eds., Birkhäuser, 2000, 1–23.
13. J. Almeida and P. G. Trotter, *Hyperdecidability of pseudovarieties of orthogroups*, Glasgow Math. J. **43** (2001) 67–83.
14. ———, *The pseudoidentity problem and reducibility for completely regular semigroups*, Bull. Austral. Math. Soc. **63** (2001) 407–433.
15. J. Almeida and P. Weil, *Free profinite* $\mathcal{R}$*-trivial monoids*, Int. J. Algebra Comput. **7** (1997) 625–671.
16. ———, *Profinite categories and semidirect products*, J. Pure Appl. Algebra **123** (1998) 1–50.
17. C. J. Ash, *Inevitable graphs: a proof of the type II conjecture and some related decision procedures*, Int. J. Algebra Comput. **1** (1991) 127–146.
18. K. Auinger, *A new proof of the Rhodes type II conjecture*, Int. J. Algebra Comput. **14** (2004) 551-568.
19. K. Auinger and B. Steinberg, *On the extension problem for partial permutations*, Proc. Amer. Math. Soc. **131** (2003) 2693–2703.
20. ———, *The geometry of profinite graphs with applications to free groups and finite monoids*, Trans. Amer. Math. Soc. **356** (2004) 805–851.
21. ———, *A constructive version of the Ribes-Zalesskii product theorem*, Math. Z. **250** (2005) 287-297.
22. ———, *Hall varieties of finite supersolvable groups*. To appear in Math. Ann.
23. J. C. Costa and M. L. Teixeira, *Tameness of the pseudovariety LSl*, Int. J. Algebra Comput. **14** (2004) 627–654.
24. T. Coulbois and A. Khélif, *Equations in free groups are not finitely approximable*, Proc. Amer. Math. Soc. **127** (1999) 963–965.
25. S. Eilenberg, *Automata, Languages and Machines*, vol. B, Academic Press, New York, 1976.
26. K. Henckell, S. Margolis, J.-E. Pin, and J. Rhodes, *Ash's type II theorem, profinite topology and Malcev products. Part I*, Int. J. Algebra Comput. **1** (1991) 411–436.
27. B. Herwig and D. Lascar, *Extending partial automorphisms and the profinite*

topology on free groups, Trans. Amer. Math. Soc. **352** (2000) 1985–2021.
28. G. Lallement, *Semigroups and Combinatorial Applications*, Wiley, New York, 1979.
29. M. Lothaire, *Algebraic Combinatorics on Words*, Cambridge University Press, Cambridge, UK, 2002.
30. G. S. Makanin, *The problem of solvability of equations in a free semigroup*, Mat. Sb. (N.S.) **103 (2)** (1977) 147–236. In Russian. English translation in: *Math. USSR-Sb.* 32 (1977) 128-198.
31. ———, *Equations in a free semigroup*, Amer. Math. Soc. Transl. (II Ser.) **117** (1981) 1–6.
32. J. McCammond, *Normal forms for free aperiodic semigroups*, Int. J. Algebra Comput. **11** (2001) 565–580.
33. J.-E. Pin, *Varieties of Formal Languages*, Plenum, London, 1986. English translation.
34. J.-E. Pin and P. Weil, *Profinite semigroups, Mal'cev products and identities*, J. Algebra **182** (1996) 604–626.
35. W. Plandowski, *Satisfiability of word equations with constants is in PSPACE*, J. ACM **51** (2004) 483–496.
36. J. Rhodes and B. Steinberg, *The q-theory of finite semigroups*, 2001–2004. Book under preparation. Preliminary versions available through `http://mathstat.math.carleton.ca/~bsteinbg/qtheor.html`.
37. L. Ribes and P. A. Zalesskiĭ, *On the profinite topology on a free group*, Bull. London Math. Soc. **25** (1993) 37–43.
38. B. Steinberg, *On pointlike sets and joins of pseudovarieties*, Int. J. Algebra Comput. **8** (1998) 203–231.
39. ———, *Inevitable graphs and profinite topologies: some solutions to algorithmic problems in monoid and automata theory, stemming from group theory*, Int. J. Algebra Comput. **11** (2001) 25–71.
40. ———, *On algorithmic problems for joins of pseudovarieties*, Semigroup Forum **62** (2001) 1–40.
41. ———, *Inverse automata and profinite topologies on a free group*, J. Pure Appl. Algebra **167** (2002) 341–359.
42. P. Weil, *Profinite methods in semigroup theory*, Int. J. Algebra Comput. **12** (2002) 137–178.
43. I. Y. Zhil'tsov, *On identities of finite aperiodic epigroups*. Ural State Univ., 1999.