A proof of Zhil'tsov's theorem on decidability of equational theory of epigroups

Inna Mikhaylova

HAL Id: hal-01352849
https://hal.inria.fr/hal-01352849

Submitted on 16 Aug 2016

A proof of Zhil'tsov's theorem on decidability of equational theory of epigroups

Inna Mikhailova*

Ural Federal University, Ekaterinburg, Russia

Epigroups are semigroups equipped with an additional unary operation called pseudoinversion. Each finite semigroup can be considered as an epigroup. We prove the following theorem announced by Zhil'tsov in 2000: the equational theory of the class of all epigroups coincides with the equational theory of the class of all finite epigroups and is decidable. We show that the theory is not finitely based but provide a transparent infinite basis for it.

Keywords: epigroup, finite semigroup, decidability of equational theory, finite basis problem

1   Introduction

A semigroup S is called an *epigroup* if, for every element $x \in S$, some power of x belongs to a subgroup of S. The class of all epigroups includes all periodic semigroups (i.e., semigroups in which each element has an idempotent power), all completely regular semigroups (i.e., unions of groups), and many other important classes of semigroups. See Shevrin (1994a,b) and the survey Shevrin (2005) for more examples and an introduction to the structure theory of epigroups.

It is known that, for every element x of an epigroup S, there exists a unique maximal subgroup G_x that contains all but finitely many powers of x. Let e_x stand for the identity element of G_x. Then it is known that $xe_x = e_x x$ and that the product belongs to G_x. The latter fact allows one to consider the inverse of xe_x in the group G_x; we denote this inverse by $\overline{x}$. This defines the unary operation $x \mapsto \overline{x}$ on each epigroup; we call this operation *pseudoinversion*. Thus, epigroups can be treated as unary semigroups, that is, as algebras with two operations: multiplication and pseudoinversion, and we shall adopt this meaning of the term 'epigroup' throughout. Let $\mathfrak{E}$ stand for the class of all epigroups.

A systematic study of epigroups as unary semigroups was initiated by Lev Shevrin in Shevrin (1994a,b, 2005). In particular, Shevrin suggested to investigate the collection of all unary semigroup identities holding in all epigroups, that is, the *equational theory* of $\mathfrak{E}$ as a class of unary semigroups[i]. The most fundamental questions about this theory are whether or not it is decidable and whether or not it is finitely axiomatizable.

---

*Email: inna.mikhaylova@gmail.com

[i] In order to prevent any chance of confusion, we mention here that the class $\mathfrak{E}$ does not form a variety of unary semigroups; of course, this is not an obstacle for considering the equational theory of $\mathfrak{E}$.

Yet another motivation for studying unary identities of epigroups comes from the theory of finite semigroups. Every finite semigroup can be treated as an epigroup, and the unary operation of pseudoinversion is an *implicit operation* in the sense of Jan Reiterman Reiterman (1982), that is, it commutes with the homomorphisms between finite semigroups. Therefore, for each collection Σ of unary identities of epigroups, the class of all finite semigroups satisfying Σ is a pseudovariety. In fact, many important pseudovarieties can be defined by identities involving the operation of pseudoinversion (which within the realm of finite semigroups is usually denoted by $x \mapsto x^{\omega-1}$) or the operation $x \mapsto x^\omega := \overline{x}x$; see Almeida (1995) for plentiful examples.

We denote by $\mathfrak{E}_{fin}$ the class of all finite epigroups. Along with $\mathfrak{E}$ and $\mathfrak{E}_{fin}$, among important classes of epigroups is the class $\mathfrak{A}_{fin}$ consisting of finite combinatorial (or aperiodic) semigroups. Recall that a semigroup is *combinatorial* if all its maximal subgroups are one-element.

At the end of the 1990s Ilya Zhil'tsov began to study the decidability problem for the equational theory of $\mathfrak{A}_{fin}$ (considered as a class of epigroups) along with a more general question. First results he obtained were published in Zhil'tsov (1999) and a full solution of the problem for $\mathfrak{A}_{fin}$ (found independently of Jon McCammond's solution in McCammond (2001)) was announced in Zhil'tsov (2000). The paper Zhil'tsov (2000) also contained similar results for the pseudovariety $\mathfrak{E}_{fin}$. We collect these results in the following statement:

Theorem 1 *The equational theory of the class $\mathfrak{E}$ coincides with the equational theory of the class $\mathfrak{E}_{fin}$ and is decidable. The theory is not finitely based but has the following infinite identity basis:*

$$(xy)z \approx x(yz),$$
$$\overline{(xy)}x \approx x\overline{(yx)},$$
$$\overline{x}^2 x \approx \overline{x},$$
$$x^2 \overline{x} \approx \overline{\overline{x}},$$
$$\overline{\overline{x}x} \approx \overline{x}x,$$
$$\overline{x^p} \approx \overline{x}^p \quad \text{for each prime } p.$$

Very unfortunately, soon after the announcement Zhil'tsov (2000) had appeared, Zhil'tsov died in a tragic accident and left no implementation of the statements indicated in Zhil'tsov (2000). It took us considerable effort to reconstruct all necessary steps of the proof. In Sections 2 and 3 we follow Zhil'tsov's plan outlined in Zhil'tsov (2000) quite closely while in Section 4 we choose a somewhat different way.

In Section 2 we introduce Zhil'tsov's concept of a $\mathbb{Z}$-unary word. He suggested to consider words with not just one but countably many additional unary operations. In Section 3, we consider normal forms for $\mathbb{Z}$-unary words and prove two of Zhil'tsov's propositions. First, it is possible to algorithmically construct the normal form. Second, there is an algorithm that, for two Z-words in normal form, returns their longest common prefix [suffix]. In particular, this means that there is an algorithm that decides whether the normal forms of given $\mathbb{Z}$-unary words coincide. In Section 4 we consider epigroup terms as $\mathbb{Z}$-unary words and show that an epigroup identity holds in each epigroup if and only if the normal form of the left-hand side of the identity coincides with the normal form of its right-hand side.

When the results forming this paper had already been obtained and the paper was being prepared for publication, the author learned about José Carlos Costa's preprint Costa (2013) also dealing with the equational theory of $\mathfrak{E}_{fin}$; later Costa's paper Costa (2014) was published. Let us briefly comment on the

relation between Costa (2014) and the present paper. Both papers provide algorithms to decide the equational theory of $\mathfrak{E}_{fin}$ and bases for the theory. However, the two algorithms utilize essentially different approaches and their justifications come from different sources. The bases found in Costa (2014) and in the present paper are, of course, equivalent.

2 $\mathbb{Z}$-unary words

2.1 *Basic definitions*

We fix an *alphabet* A, that is, a non-empty set which elements are referred to as *letters*. As usual, by A^+ we denote the *free semigroup* over A, that is, the set of all non-empty *words* over A which are multiplied by concatenation. We extend A^+ to a larger algebra that we denote by $Z(A)$ and call the *free Z-unary semigroup* over A, the elements of $Z(A)$ being called *Z-unary words* over A. For this we fix a symbol ω and define the notions of a $\mathbb{Z}$-unary word and of its *height* by simultaneous induction as follows:

1) the empty word is a $\mathbb{Z}$-unary word of height $-\infty$;

2) every letter from A is a $\mathbb{Z}$-unary word of height 0;

3) for every integer $q \in \mathbb{Z}$ and every $\mathbb{Z}$-unary word σ of height h, the expression $(\sigma)^{\omega+q}$ is a $\mathbb{Z}$-unary word of height $h + 1$;

4) for every pair σ_1, σ_2 of $\mathbb{Z}$-unary words of heights h_1 and respectively h_2, the expression $\sigma_1\sigma_2$ is a $\mathbb{Z}$-unary word of height $\max\{h_1, h_2\}$.

For example, the expression

$$(x^{\omega-4}yx^{\omega+30})^{\omega-1}xy^\omega$$

is a $\mathbb{Z}$-unary word over $\{x, y\}$ of height 2. This example also illustrates three natural conventions that we adopt throughout: we omit parentheses in expressions like $(\sigma)^{\omega+q}$ whenever σ is just a letter and take the liberty to write ω instead of $\omega + 0$ and $\omega - q$ instead of $\omega + (-q)$ for q being a positive integer.

We denote the height of $\sigma \in Z(A)$ by $h(\sigma)$. It is easy to verify that every $\mathbb{Z}$-unary word σ of height $h + 1$ with $h \geq 0$ can be uniquely represented as

$$\sigma = \pi_0\rho_1^{\omega+q_1}\pi_1\cdots\rho_n^{\omega+q_n}\pi_n, \tag{1}$$

where $n \geq 1$, $h(\rho_i) = h$ for all $i = 1, \ldots, n$, and $h(\pi_i) \leq h$ for all $i = 0, \ldots, n$. We call (1) the *height representation* of σ.

We define the mapping $\sigma \mapsto |\sigma|$ from the free $\mathbb{Z}$-unary semigroup $Z(A)$ into the ring $\mathbb{Z}[\omega]$ of all polynomials in ω with integer coefficients as follows:

1) $|\sigma| := 0$ if σ is the empty word;

2) $|\sigma| := 1$ whenever σ is a letter from A;

3) $|\sigma^{\omega+q}| := (\omega + q)|\sigma|$ for every integer $q \in \mathbb{Z}$ and every $\sigma \in Z(A)$;

4) $|\sigma\tau| := |\sigma| + |\tau|$ for all $\sigma, \tau \in Z(A)$.

We call $|\sigma|$ the *length* of the $\mathbb{Z}$-unary word σ. Observe that $h(\sigma)$ is just is the degree $\deg|\sigma|$ of the polynomial $|\sigma|$. For two polynomials $f, g \in \mathbb{Z}[\omega]$, we write $f \geq g$ if the leading coefficient of the polynomial $f - g$ is non-negative. Then $|\sigma| \geq 0$ for every $\sigma \in Z(A)$.

We say that a $\mathbb{Z}$-unary word τ is a *prefix* [resp. *suffix*] of $\sigma \in Z(A)$ if $\sigma = \tau\rho$ [resp. $\sigma = \rho\tau$] for some $\rho \in Z(A)$. A $\mathbb{Z}$-unary word τ is a *factor* of σ if $\sigma = \rho_1\tau\rho_2$ for some $\rho_1, \rho_2 \in Z(A)$ and it is a *power* of σ if $\tau = \sigma^n$ for some $n \geq 2$. Likewise, $\mathbb{Z}$-unary words of the form $\sigma^{\omega+q}$, where q is an integer, are called ω-*powers* of σ. Observe that the free $\mathbb{Z}$-unary semigroup $Z(A)$ considered as a semigroup is just the free monoid generated by A and all ω-powers.

2.2 Singular words

Consider the fully invariant congruence $\mathcal{S}$ on the free $\mathbb{Z}$-unary semigroup $Z(A)$ generated by the pairs

$$(x^{\omega+q}, xx^{\omega+q-1}), \tag{2}$$

$$(x^{\omega+q}, x^{\omega+q-1}x), \tag{3}$$

$$(x(yx)^{\omega+q}, (xy)^{\omega+q}x), \tag{4}$$

where q runs over $\mathbb{Z}$.

By a *singular word* or, shortly, a *sword* we mean an $\mathcal{S}$-class. The class corresponding to a given $\mathbb{Z}$-unary word σ is denoted by $\sigma^{\mathcal{S}}$. Notice that if σ is an ordinary word, that is, $\sigma \in A^+$, then $\sigma^{\mathcal{S}} = \{\sigma\}$. The quotient algebra $Z(A)/\mathcal{S}$ of all swords is denoted by $\mathrm{Sing}(A)$.

Example 1 (Zhil'tsov) *Consider the $\mathbb{Z}$-unary word $x(xyz)^{\omega-5}xy(zx)^{\omega+4}zz$ of height 1 and of length $5\omega - 2$. We can represent it by the following picture:*
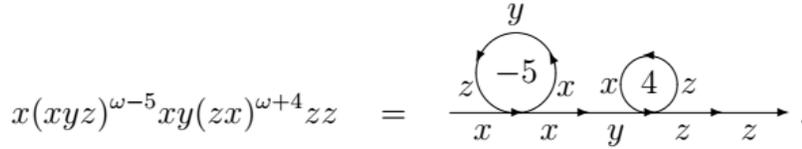

$$x(xyz)^{\omega-5}xy(zx)^{\omega+4}zz \quad = \quad$$

Fig. 1: Pictorial representation if a $\mathbb{Z}$-unary word

Here the ω-powers $(xyz)^{\omega-5}$ and $(zx)^{\omega+4}$ are represented by the circles labeled xyz and zx with encircled numbers -5 and 4 respectively. Now we draw the analogous pictures for three further $\mathbb{Z}$-unary words that belong to the same $\mathcal{S}$-class. These pictures illustrate three basic transformations that one can perform on a $\mathbb{Z}$-unary word without changing its $\mathcal{S}$-class.

- *One can "unwind" n copies of a circle to the left or the right side of the circle, simultaneously decreasing its encircled number by n — in Fig. 2 this transformation is applied to the circle labeled zx in Fig. 1 with $n = 2$. This corresponds to n applications of either (2) or (3) from left to right.*

- *One can "wind up" (if it is possible) n copies of a circle from the left or the right side of the circle, simultaneously increasing its encircled number by n — in Fig. 3 this transformation is applied to the circle labeled xyz in Fig. 2 with $n = 1$. This corresponds to n applications of either (2) or (3) from right to left.*

$$x(xyz)^{\omega-5}xyzxzx(zx)^{\omega+2}zz \quad = \quad$$

Fig. 2: Unwinding

$$x(xyz)^{\omega-4}zx(zx)^{\omega+2}zz \quad = \quad$$

Fig. 3: Winding up

$$x(xyz)^{\omega-4}z(xz)^{\omega+2}z \quad = \quad$$

Fig. 4: Rolling

- *One can "roll" a circle to the left (right) side if some suffix (resp. prefix) of the circle's label is written before (resp. after) the circle — in Fig. 4 this transformation is applied to the circle labeled zx in Fig. 3. This corresponds to an application of* (4).

Thus, any sword can be considered as an ordinary word with some attached "singularities" (ω-powers that may contain further ω-powers etc.) that can move along the word. This explains our terminology.

We refer to the basic transformations illustrated in Example 1 as *$\mathcal{S}$-transformations*. Each $\mathcal{S}$-transformation involves a certain ω-power which we call the *site* of the transformation. Clearly, two $\mathbb{Z}$-unary words belong to the same $\mathcal{S}$-class if and only if one can obtain each of these words form the other by a suitable sequence of $\mathcal{S}$-transformations.

Notice that, due to the definition of the congruence $\mathcal{S}$, the following conditions hold for all $\mathbb{Z}$-unary words σ, τ in the same $\mathcal{S}$-class:

- σ and τ have the same height;

- σ and τ have the same length.

Thus, we can well define the *height* and the *length* of a sword $\sigma^{\mathcal{S}}$ as the height and respectively the length of σ. We can also speak about a height representation of a sword; observe, however, that in contrast to $\mathbb{Z}$-unary words, a sword may have several height representations.

We say that a sword $\tau^{\mathcal{S}}$ is a *prefix* [*suffix, factor*] of a sword $\sigma^{\mathcal{S}}$ if, for some $\mathbb{Z}$-unary words τ', σ' such that $(\tau')^{\mathcal{S}} = \tau^{\mathcal{S}}$ and $(\sigma')^{\mathcal{S}} = \sigma^{\mathcal{S}}$, the $\mathbb{Z}$-unary word τ' is a prefix [resp. suffix, factor] of σ'. In the same way, the notions of a power and of an ω-power extend to swords.

As we will see, the algebra $\mathrm{Sing}(A)$ considered as a semigroup inherits several important properties from the free semigroup. Of course, there are some differences too. For instance, each sword of height more than zero has infinitely many factors. Further, for every ordinary word w and every integer t such that $0 \leq t \leq |w|$, there exists a prefix of w with length t. This is not true in general swords: for example, the sword $((x^2)^\omega)^\mathcal{S}$ has no prefix of length ω.

Lemma 1 *There is an algorithm that, given an arbitrary sword $\sigma^\mathcal{S}$ and a polynomial $f(\omega) \in \mathbb{Z}[w]$ such that the leading coefficient of $|\sigma| - f(\omega)$ is non-negative, decides whether $\sigma^\mathcal{S}$ has a prefix of length $f(\omega)$. If the answer is positive, the algorithm constructs swords $x^\mathcal{S}, y^\mathcal{S}$ such that $\sigma^\mathcal{S} = x^\mathcal{S} y^\mathcal{S}$ and $|x| = f(\omega)$.*

Proof: We induct on the height of σ. As we have noticed prior to the formulation of the lemma, its statement holds for ordinary words and hence for swords of height 0.

Let $h(\sigma) = h + 1$ and let (1) be the height representation of σ. Since $f(\omega) \leq |\sigma|$, there is an index k such that

$$|\pi_0 \cdots \rho_k^{\omega + q_k}| \leq f(\omega) \leq |\pi_0 \cdots \rho_k^{\omega + q_k} \pi_k \rho_{k+1}^{\omega + q_{k+1}}|.$$

(If $\deg f(\omega) < h + 1$, then $k = 0$ and the above inequality takes the form $0 \leq f(\omega) \leq |\pi_0 \rho_1^{\omega + q_1}|$.) Let $g(\omega) = f(\omega) - |\pi_0 \cdots \rho_k^{\omega + q_k}|$. (In the case where $k = 0$, we let $g(\omega) = f(\omega)$.) Clearly, $\sigma^\mathcal{S}$ has a prefix of length $f(\omega)$ if and only if the sword $(\pi_k \rho_{k+1}^{\omega + q_{k+1}})^\mathcal{S}$ has a prefix of length $g(\omega)$.

First suppose that $\deg g(\omega) < h + 1$. Then it is possible to choose a positive integer m such that the leading coefficient of $|\pi^k \rho_{k+1}^m| - g(\omega)$ is non-negative, and we are in a position to apply the induction hypothesis to the sword $(\pi^k \rho_{k+1}^m)^\mathcal{S}$ and the polynomial $g(\omega)$. If the answer is positive and $(\pi^k \rho_{k+1}^m)^\mathcal{S} = x_1^\mathcal{S} y_1^\mathcal{S}$ with $|x_1| = g(\omega)$, then the required swords are $x^\mathcal{S} = (\pi_0 \cdots \rho_k^{\omega + q_k} x_1)^\mathcal{S}$ and $y^\mathcal{S} = (y_1 \rho_{k+1}^{\omega + q_{k+1} - m} \cdots \pi_n)^\mathcal{S}$.

Now suppose that $\deg g(\omega) = h + 1$. It is easy to see that if the required prefix exists then it has the form $(\pi_k \rho_{k+1}^{\omega + t} \eta)^\mathcal{S}$ for some integer $t \leq q_{k+1}$ and some prefix η of the $\mathbb{Z}$-unary word ρ_{k+1}. Since $h(\pi_k) \leq h$ and $h(\eta) \leq h$, we conclude that, by the definition of the length, the leading coefficients of the polynomials $|\pi_k \rho_{k+1}^{\omega + t} \eta|$, $|\pi_k \rho_{k+1}^{\omega + q_{k+1}}|$, and $g(\omega)$ must coincide. If this holds, then we choose an integer $s < q_{k+1}$ such that the leading coefficient of the polynomial $g'(\omega) = |\pi_k \rho_{k+1}^{\omega + s}| - g(\omega)$ is non-negative. Since $\deg g'(\omega) < h + 1$, we can apply the induction hypothesis to the sword $(\rho_{k+1}^{q_{k+1} - s})^\mathcal{S}$ and the polynomial $g'(\omega)$, obtaining either a negative answer or a decomposition $(\rho_{k+1}^{q_{k+1} - s})^\mathcal{S} = x_1^\mathcal{S} y_1^\mathcal{S}$. Then the required prefix is $x^\mathcal{S} = (\pi_0 \cdots \rho_k^{\omega + q_k} \pi_k \rho_{k+1}^{\omega + s} x_1)^\mathcal{S}$. $\square$

Lemma 2   *1. $\mathrm{Sing}(A)$ is a $\mathcal{J}$-trivial cancellative semigroup;*

    2. The set of all prefixes [suffixes] of a sword is linearly ordered by right [resp. left] division.

Proof: Let us start with the proof of the cancelation property. Suppose that $\sigma^\mathcal{S} \tau_1^\mathcal{S} = \sigma^\mathcal{S} \tau_2^\mathcal{S}$. This implies $(\sigma \tau_1)^\mathcal{S} = (\sigma \tau_2)^\mathcal{S}$. Therefore there exists a sequence of $\mathbb{Z}$-unary words $\sigma \tau_1 = \eta_1, \eta_2, \ldots, \eta_n = \sigma \tau_2$ such that for each $i = 1, \ldots, n - 1$, the word η_{i+1} can be obtained from the word η_i by one of the $\mathcal{S}$-transformations: "unwinding", "winding up", or "rolling". We will construct two sequences of $\mathbb{Z}$-unary words $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ with the following properties:

   (i) $\alpha_1 = \sigma$, $\beta_1 = \tau_1$;

(ii) for each $i = 1, \ldots, n-1$, one can pass from α_i to α_{i+1} and from β_i to β_{i+1} by a sequence of $\mathcal{S}$-transformations;

(iii) for each $i = 1, \ldots, n$, the $\mathbb{Z}$-unary word $\alpha_i \beta_i$ can be obtained from η_i by applying only "unwinding" $\mathcal{S}$-transformations.

This will imply the desired conclusion $\tau_1^{\mathcal{S}} = \tau_2^{\mathcal{S}}$. Indeed, by (i) and (ii), we have $\sigma = \alpha_1 \; \mathcal{S} \; \alpha_n$ and $\tau_1 = \beta_1 \; \mathcal{S} \; \beta_n$ whence, in particular, $|\sigma| = |\alpha_n|$. By (iii), $\alpha_n \beta_n$ can be obtained from $\eta_n = \sigma \tau_2$ by "unwinding" $\mathcal{S}$-transformations only. The definition of an "unwinding" $\mathcal{S}$-transformation implies that if such a transformation is applied to a product of two $\mathbb{Z}$-unary words, its site is contained in one of the factors. Thus, we conclude that $\alpha_n \beta_n = \gamma \delta$, where γ and δ are obtained by some "unwinding" $\mathcal{S}$-transformations from σ and τ_2 respectively. In particular, $\sigma \; \mathcal{S} \; \gamma$ and $\tau_2 \; \mathcal{S} \; \delta$. Since $|\gamma| = |\sigma| = |\alpha_n|$, we have $\gamma = \alpha_n$ whence $\delta = \beta_n$. This yields $\tau_1 \; \mathcal{S} \; \beta_n = \delta \; \mathcal{S} \; \tau_2$ and $\tau_1 \; \mathcal{S} \; \tau_2$, as required.

Thus, it remains to construct the sequences $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ satisfying (i)–(iii). We proceed by induction, using (i) as the induction basis. Suppose that the $\mathbb{Z}$-unary words α_i and β_i have already been defined. If the $\mathcal{S}$-transformation Φ applied to obtain η_{i+1} from η_i is of the type "winding up", we let $\alpha_{i+1} = \alpha_i$, $\beta_{i+1} = \beta_i$. If Φ is of the type "unwinding", one of the two possibilities occur: either Φ is one of the $\mathcal{S}$-transformations employed to convert η_i into $\alpha_i \beta_i$ or not. In the former case we again let $\alpha_{i+1} = \alpha_i$, $\beta_{i+1} = \beta_i$. In the latter case, the site of Φ persists in $\alpha_i \beta_i$ and, as already mentioned, it is located within one of the factors α_i or β_i. If the site lies within α_i, we let α_{i+1} be the result of applying Φ to α_i and let $\beta_{i+1} = \beta_i$; otherwise we let $\alpha_{i+1} = \alpha_i$ and let β_{i+1} be the result of applying Φ to β_i.

Now let Φ be of the type "rolling". By symmetry, we may assume that Φ corresponds to an application of (4) from right to left, that is, the site $(xy)^{\omega+q}$ of Φ is followed by x in η_i and "rolls" to the right producing $x(yx)^{\omega+q}$ in η_{i+1}. Since $\alpha_i \beta_i$ is obtained from η_i by "unwinding" $\mathcal{S}$-transformations, $\alpha_i \beta_i$ may contain several copies of the site of Φ—for illustration, if, say, $\eta_i = (z(xy)^{\omega+q}x)^{\omega+r}$, then unwinding the external ω-power gives $\mathbb{Z}$-unary words of the form $(z(xy)^{\omega+q}x)^s (z(xy)^{\omega+q}x)^{\omega+r-s-t}(z(xy)^{\omega+q}x)^t$, with $s+t+1$ occurrences of the site. We apply Φ to all copies of $(xy)^{\omega+q}x$ that occur within α_i or β_i. Besides that, it may happen that some copies of the site have undergone unwinding themselves, resulting in a $\mathbb{Z}$-unary word of the form $\xi = (xy)^r (xy)^{\omega+q-r-s}(xy)^s x$. Whenever such a ξ lies entirely within α_i or β_i, we substitute it by $x(yx)^r (yx)^{\omega+q-r-s}(yx)^s$—clearly, this amounts to "rolling" of $(xy)^{\omega+q-r-s}$ to the right. If ξ occurs on the junction of α_i and β_i, we can basically do the same except for the only case where $(xy)^r (xy)^{\omega+q-r-s}$ is a suffix of α_i while $(xy)^s x$ is a prefix of β_i because in this case we cannot "roll" $(xy)^{\omega+q-r-s}$ to the right within α_i. In this remaining case, when passing from α_i to α_{i+1}, we substitute $(xy)^r (xy)^{\omega+q-r-s}$ by $x(yx)^r (yx)^{\omega+q-r-s-1}y$. This concludes the induction step.

Now let us show that $\mathrm{Sing}(A)$ is $\mathcal{J}$-trivial. Indeed, assume that some swords $\alpha^{\mathcal{S}}, \beta^{\mathcal{S}}$ are $\mathcal{J}$-related. Then $\alpha^{\mathcal{S}} = \sigma_1^{\mathcal{S}} \beta^{\mathcal{S}} \tau_1^{\mathcal{S}}$ and $\beta^{\mathcal{S}} = \sigma_2^{\mathcal{S}} \alpha^{\mathcal{S}} \tau_2^{\mathcal{S}}$ for some $\sigma_1, \sigma_2, \tau_1, \tau_2 \in Z(A)$. We have $\alpha^{\mathcal{S}} = \sigma_1^{\mathcal{S}} \sigma_2^{\mathcal{S}} \alpha^{\mathcal{S}} \tau_2^{\mathcal{S}} \tau_1^{\mathcal{S}}$ whence $|\sigma_1| = |\sigma_2| = |\tau_1| = |\tau_2| = 0$ and all these $\mathbb{Z}$-unary words must be empty. Hence $\alpha^{\mathcal{S}} = \beta^{\mathcal{S}}$.

The $\mathcal{J}$-triviality of the semigroup $\mathrm{Sing}(A)$ implies that the relations of right and left division are partial orders on $\mathrm{Sing}(A)$. We aim to show that their restrictions to the set of all prefixes [suffixes] of a fixed sword $\sigma^{\mathcal{S}}$ are linear orders. By symmetry, it suffices to consider right division only. Thus, suppose that $\sigma^{\mathcal{S}} = \tau_1^{\mathcal{S}} \rho_1^{\mathcal{S}} = \tau_2^{\mathcal{S}} \rho_2^{\mathcal{S}}$ and $|\tau_1| \leq |\tau_2|$. Since $\tau_1 \rho_1 \; \mathcal{S} \; \tau_2 \rho_2$, the sword $(\tau_2 \rho_2)^{\mathcal{S}}$ has a prefix of length $|\tau_1|$ that should be also a prefix of the sword $(\tau_2)^{\mathcal{S}}$. Hence, using the algorithm of Lemma 1, we can find two swords $x^{\mathcal{S}}$ and $y^{\mathcal{S}}$ such that $\tau_2^{\mathcal{S}} = x^{\mathcal{S}} y^{\mathcal{S}}$ and $|x| = |\tau_1|$.

Since $\tau_1 \rho_1 \; \mathcal{S} \; xy\rho_2$, there exists a sequence of $\mathbb{Z}$-unary words $\eta_1 = \tau_1 \rho_1, \eta_2, \ldots, \eta_n = xy\rho_2$ such that η_{i+1} can be obtained from η_i by an application of a suitable $\mathcal{S}$-transformation for each $i = 1, \ldots, n-1$.

Now we follow the proof of the cancelation property above and construct two sequences of $\mathbb{Z}$-unary words $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ such that

(i) $\alpha_1 = \tau_1$, $\beta_1 = \rho_1$;

(ii) for each $i = 1, \ldots, n - 1$, one can pass from α_i to α_{i+1} and from β_i to β_{i+1} by a sequence of $\mathcal{S}$-transformations;

(iii) for each $i = 1, \ldots, n$, the $\mathbb{Z}$-unary word $\alpha_i \beta_i$ can be obtained from η_i by applying only "unwinding" $\mathcal{S}$-transformations.

Then the same argument as the one we have utilized in the proof of the cancelation property shows that $\tau_1 = \alpha_1 \, \mathcal{S} \, \alpha_n \, \mathcal{S} \, x$ whence $\tau_1^{\mathcal{S}} = x^{\mathcal{S}}$ divides $\tau_2^{\mathcal{S}}$ on the right. $\square$

3   Normal swords

3.1   Overview

In this section we introduce a rewriting system that plays a key role for the decidability question.

Let $\mathcal{R}$ denote the rewriting system on the free $\mathbb{Z}$-unary semigroup $Z(A)$ consisting of the rules

$$x^{\omega+q} x^{\omega+r} \xrightarrow{\mathcal{R}} x^{\omega+q+r}, \tag{5}$$

$$(x^n)^{\omega+q} \xrightarrow{\mathcal{R}} x^{\omega+nq}, \tag{6}$$

$$(x^{\omega+r})^{\omega+q} \xrightarrow{\mathcal{R}} x^{\omega+rq} \tag{7}$$

for all $x \in Z(A)$, all $r, q \in \mathbb{Z}$, and all $n \geq 2$. Observe that all these rules are length-decreasing; the rule (7) is also height-decreasing while (5) and (6) do not change the height. The rewriting system $\mathcal{R}$ induces the "quotient" rewriting system $\mathcal{R}/\mathcal{S}$ on the quotient semigroup $\mathrm{Sing}(A) = Z(A)/\mathcal{S}$ as follows: $\alpha^{\mathcal{S}} \xrightarrow{\mathcal{R}/\mathcal{S}} \beta^{\mathcal{S}}$ if and only if there exist $\mathbb{Z}$-unary words σ and τ such that $\alpha^{\mathcal{S}} = \sigma^{\mathcal{S}}$, $\beta^{\mathcal{S}} = \tau^{\mathcal{S}}$, and $\sigma \xrightarrow{\mathcal{R}} \tau$. By $(\mathcal{R}/\mathcal{S})^*$ we denote the reflexive and transitive closure of $\mathcal{R}/\mathcal{S}$.

A *normal sword* (or an $\mathcal{R}/\mathcal{S}$-*irreducible sword*) is a sword $\alpha^{\mathcal{S}}$ such that there is no sword $\beta^{\mathcal{S}}$ with $\alpha^{\mathcal{S}} \xrightarrow{\mathcal{R}/\mathcal{S}} \beta^{\mathcal{S}}$. Observe that every factor of a normal sword is also normal. A sword $\alpha^{\mathcal{S}}$ is called *fully normal* if its square $(\alpha^{\mathcal{S}})^2$ is normal. It is easy to see that then $(\alpha^{\mathcal{S}})^n$ is normal for all $n \geq 2$.

Any normal sword which is $(\mathcal{R}/\mathcal{S})^*$-related to a given sword $\sigma^{\mathcal{S}}$ is said to be a *normal form* of $\sigma^{\mathcal{S}}$. We stress that at this point we claim no uniqueness nor confluence: a sword may have several normal forms.

Up to now, we have always tried to differentiate between a sword (i.e., an $\mathcal{S}$-class) and a $\mathbb{Z}$-unary word representing this $\mathcal{S}$-class. In the sequel, in order to lighten the notation, we allow ourselves to omit the superscript $^{\mathcal{S}}$ so that a sword, say, $\alpha^{\mathcal{S}}$ may be denoted by just α.

This definition of a normal sword implies that such a sword contains no factors of the forms $x^{\omega+r} x^{\omega+q}$, $(x^n)^{\omega+q}$, $(x^{\omega+r})^{\omega+q}$. Notice also that if a sword is fully normal, then it is obviously normal and cannot have the form $x^{\omega+m}$ nor $x^{\omega+r} y x^{\omega+q}$. Clearly, all ordinary words are fully normal.

The main goal of this section is to prove the two following propositions.

Proposition 1 *There exists an algorithm that, given a sword σ of height h, returns a normal form of σ.*

Proposition 2 *There exists an algorithm that, given two normal swords of height at most h, returns their longest common prefix.*

We have included the parameter h in the formulations of Propositions 1 and 2 because we are going to prove these propositions, along with Lemmas 3–7 formulated below, by simultaneous induction on h. All these statements obviously hold for swords of height 0 (i.e., for ordinary words), and we will assume that they hold true for all swords of height $h - 1$.

We will also use the following corollary of Proposition 2:

Corollary 1 *There is an algorithm that checks whether or not two given normal swords are equal.*

Proof: Let σ, τ be normal swords. Using the algorithm of Proposition 2, we find their longest common prefix ρ. Clearly, $\sigma = \tau$ if and only if $\sigma = \rho$ and $\tau = \rho$, and the two latter equalities are equivalent to the equalities $|\sigma| = |\rho|$ and respectively $|\tau| = |\rho|$ in view of Lemma 2. $\square$

3.2 Periodic normal swords

We will need two auxiliary facts similar to well-known properties of ordinary words.

Given a sword τ, a sword σ is called τ-*periodic* if σ is a power or an ω-power of τ.

Lemma 3 *Let σ, τ be non-empty normal swords of height at most h and $\tau\sigma = \sigma\tau$. Then there exists a fully normal sword π such that both τ and σ are π-periodic. If, besides that, σ and τ are fully normal, then $h(\sigma) = h(\tau) = h(\pi)$ and $\sigma = \pi^{n_1}$, $\tau = \pi^{n_2}$ for some positive integers n_1, n_2.*

Proof: By symmetry, we may assume that $|\sigma| \geq |\tau|$. Observe that since $\sigma\tau = \tau\sigma$, the sword τ is a prefix of σ by item 2 of Lemma 2. Therefore, there exists a sword σ' such that $\sigma = \tau\sigma'$ whence $\tau\sigma'\tau = \sigma\tau = \tau\sigma = \tau^2\sigma'$. Since τ^2 is a prefix of a normal sword, it is normal whence τ is fully normal. Further, by item 1 of Lemma 2, we can cancel τ in the equality $\tau\sigma'\tau = \tau^2\sigma'$, thus getting $\sigma'\tau = \tau\sigma'$.

First consider the case $h(\sigma) > h(\tau)$. Then $h(\sigma') > h(\tau)$ whence $|\sigma'| > |\tau|$. Arguing as in the preceding paragraph, we see that τ is a prefix of σ' and there exists a sword σ'' of height $h(\sigma)$ such that $\sigma''\tau = \tau\sigma''$, and so on. Therefore, for any positive integer m, the sword τ^m is a prefix of the sword σ. It is clear this is only possible if σ has some ω-power of τ as a prefix. Therefore, we may assume that $\sigma = \tau^{\omega+k}\sigma_1$ for some integer k and some sword σ_1.

Suppose that $h(\sigma_1) = h(\sigma)$. Observe that $\tau^{\omega+k}\sigma_1\tau = \sigma\tau = \tau\sigma = \tau^{\omega+k+1}\sigma_1$. Using item 1 of Lemma 2, we conclude that $\sigma_1\tau = \tau\sigma_1$, and we can repeat the same steps as before to obtain that $\sigma_1 = \tau^{\omega+\ell}\sigma_2$ for some integer ℓ and some sword σ_1. Then, however, the sword $\sigma = \tau^{\omega+k}\tau^{\omega+\ell}\sigma_2$ would not be normal, a contradiction.

Hence $h(\sigma_1) < h(\sigma)$. If σ_1 is not empty, we can apply the induction hypothesis to the swords σ_1 and τ whose height is strictly less than h. There exists a fully normal sword π such that both σ_1 and τ are π-periodic but then $\sigma = \tau^{\omega+k}\sigma_1$ could not be normal, a contradiction again. Thus, σ_1 is empty, whence $\sigma = \tau^{\omega+k}$ is an ω-power of the fully normal sword τ and the first statement of the lemma holds true.

Assume now that $h(\sigma) = h(\tau)$. Then $|\sigma| = \ell_1\omega^h + g_1(w)$, $|\tau| = \ell_2\omega^h + g_2(\omega)$, where $\deg(g_i) < h$ for $i = 1, 2$. We proceed by induction on $\max\{\ell_1, \ell_2\}$.

If $\ell_1 = \ell_2$ (in particular, if $\max\{\ell_1, \ell_2\} = 1$), the sword σ' such that $\sigma = \tau\sigma' = \sigma'\tau$ has height less than h, and this leads to the case just considered. We then obtain that there is a fully normal sword π such

that $\tau = \pi^{\omega+k}$ and $\sigma' = \pi^m$ for some integers k, m, and thus, $\sigma = \pi^{\omega+k+m}$. If $\ell_1 \neq \ell_2$, we apply the induction hypothesis to the pair σ', τ to obtain the required property.

The second statement of the lemma trivially follows from the definition of a fully normal sword.   □

Lemma 4 *Let x and y be fully normal swords. Suppose that $|x| \geq |y|$ and x^2 is a prefix [suffix] of some y-periodic sword. Then there exists a fully normal sword z such that x and y are powers of z. If, besides that, some ω-powers of x and y are prefixes [suffixes] of a normal sword, then $x = y$.*

Proof: Since x^2 is a prefix of a power or an ω-power of y and $|x| \geq |y|$, a power or an ω-power of y should be a prefix of x. In the latter case there are swords y_1, y_2 and a prefix y_3 of y such that $y = y_1 y_2$ and $x = (y_1 y_2)^{\omega+r_1} y_1 = y_2 (y_1 y_2)^{\omega+r_2} y_3$ for some $r_1, r_2 \in \mathbb{Z}$ whence

$$x^2 = (y_1 y_2)^{\omega+r_1} y_1 y_2 (y_1 y_2)^{\omega+r_2} y_3 = y_1 (y_2 y_1)^{\omega+r_1} (y_2 y_1)^{\omega+r_2} y_1 y_3.$$

We see that x is not fully normal, a contradiction.

If a power of y but no ω-power of y is a prefix of x, then there exist swords y_1, y_2 and a prefix y_3 of y such that $y_1 y_2 = y$ and $x = (y_1 y_2)^{n_1} y_1 = y_2 (y_1 y_2)^{n_2} y_3$ for some $n_1, n_2 \geq 1$. Since both $y_1 y_2$ and $y_2 y_1$ are prefixes of x and have the same length, we conclude that $y_1 y_2 = y_2 y_1$. Since y is fully normal, by Lemma 3 we obtain that $y_1 = z^{k_1}$, $y_2 = z^{k_2}$ for some $k_1, k_2 \geq 1$ and some fully normal sword z. Hence x and y are powers of z.

The second statement of the lemma immediately follows from the fact that, because of the rule (6), the only power of z that can occur as a factor in a normal sword is z itself. Hence, $x = z$ and $y = z$.   □

3.3 Normalization

Our algorithm that constructs a normal form of an arbitrary sword will repeatedly invoke two procedures. Recall that every sword of height h can be represented as $\pi_0 \rho_1^{\omega+q_1} \pi_1 \cdots \rho_n^{\omega+q_n} \pi_n$, where each of the swords $\pi_0, \pi_1, \ldots, \pi_n, \rho_1, \ldots, \rho_n$ has height less than h. Therefore it suffices to exhibit a procedure that produces a normal form for a given sword being an ω-power of a normal swords and a procedure that produces a normal form for the product of two given normal swords.

We start with the latter procedure. First of all, observe that the product of two normal swords may indeed fail to be normal. For example, if $\sigma_1 = (xz^{\omega+2})^\omega$ and $\sigma_2 = z^{\omega-5}$, then the product $\sigma_1 \sigma_2 = (xz^{\omega+2})^\omega z^{\omega-5}$ is not normal because it is equal (as a sword) to $(xz^{\omega+2})^{\omega-1} xz^{\omega+2} z^{\omega-5}$. One can obtain a normal form of $(xz^{\omega+2})^{\omega-1} xz^{\omega+2} z^{\omega-5}$ by applying to it just one $\mathcal{R}/\mathcal{S}$-transition of the form (5), thus producing $(xz^{\omega+2})^{\omega-1} xz^{\omega-3}$.

Actually, the situation demonstrated by the above example is generic. By the definition of a normal sword, it is clear that the product of two normal swords is not normal if and only if it has a factor of the form $y^{\omega+r} y^{\omega+q}$. Thus, the fact that σ_1 and σ_2 are normal while $\sigma_1 \sigma_2$ is not is equivalent to the existence of a sword y such that σ_1 has a suffix and σ_2 has a prefix that are ω-powers of y. Obviously, if such a sword y exists, it should be fully normal and by Lemma 4 it is unique. We refer to y as to the *overlap* between σ_1 and σ_2.

Lemma 5 *Let σ_1, σ_2 be two normal swords of height no more than h. There exists an algorithm that decides whether the product $\sigma_1 \sigma_2$ is in normal form. If the product is not normal, the algorithm finds the overlap between σ_1 and σ_2 and constructs a normal form for the product.*

Proof: First, we describe an algorithm that, given two normal swords σ_1, σ_2 of height h, decides if they have an overlap of height $h - 1$, and in the case where the answer is positive, finds the overlap and constructs a normal form for $\sigma_1\sigma_2$. Since the algorithm will be repeatedly invoked in the rest of the proof, it is convenient to give it a name. So, let us call this algorithm TO (from "tall overlap").

We start with representing the given swords as

$$\sigma_1 = \sigma_1'\rho_1^{\omega+q_1}\pi_1 \text{ and } \sigma_2 = \pi_2\rho_2^{\omega+q_2}\sigma_2', \tag{8}$$

where $h(\rho_1) = h(\rho_2) = h - 1$ and $h(\pi_1), h(\pi_2) \leq h - 1$. If σ_1 has a suffix that is an ω-power of some sword of height $h - 1$, then the suffix is of height h, and hence, it has to involve some ω-power of ρ_1 as a factor. Clearly, this is only possible if $\rho_1 = \pi_1\rho_1'$ for some sword ρ_1', and we can decide whether or not the latter equality holds true by applying the algorithm of Proposition 2 to the swords π_1 and ρ_1 to find their longest common prefix and then deciding whether or not this prefix is equal to π_1. If the answer is positive, we can rewrite the sword σ_1 (by "rolling" $(\pi_1\rho_1')^{\omega+q_1}$ to the right) as

$$\sigma_1 = \sigma_1'\pi_1(\rho_1'\pi_1)^{\omega+q_1}.$$

Similarly, if σ_2 has a prefix that is an ω-power of some sword of height $h - 1$, then the prefix is of height h and has some ω-power of ρ_2 as a factor. This is only possible if $\rho_2 = \rho_2'\pi_2$ for some sword ρ_2', which can be verified by applying the "dual" of the algorithm of Proposition 2. If the answer is positive, we can rewrite the sword σ_2 (by "rolling" $(\rho_2'\pi_2)^{\omega+q_2}$ to the left) as

$$\sigma_2 = (\pi_2\rho_2')^{\omega+q_2}\pi_2\sigma_2'.$$

Now it remains to verify whether or not the swords $\rho_1'\pi_1$ and $\pi_2\rho_2'$ of height $h - 1$ are equal. If the answer is negative, σ_1 and σ_2 have no overlap of height $h - 1$. Otherwise, the sword $y = \rho_1'\pi_1 = \pi_2\rho_2'$ is the overlap of height $h - 1$ between σ_1 and σ_2 and $\sigma_1\sigma_2 = \sigma_1'\pi_1 y^{\omega+q_1}y^{\omega+q_2}\pi_2\sigma_2'$. Applying an $\mathcal{R}/\mathcal{S}$-transition of the form (5), we reduce it to the sword $\tau = \sigma_1'\pi_1 y^{\omega+q_1+q_2}\pi_2\sigma_2'$. We are going to prove that τ is normal, and thus, it is a normal form for the product $\sigma_1\sigma_2$. Arguing by contradiction, assume that τ is not normal. Then there should be the overlap z, say, between either $\sigma_1'\pi_1$ and $y^{\omega+q_1+q_2}\pi_2\sigma_2'$ or $\sigma_1'\pi_1 y^{\omega+q_1+q_2}$ and $\pi_2\sigma_2'$. Since the height of τ is h, the height of z is at most $h - 1$ whence z contains no ω-power of y as a prefix nor as a suffix. Then Lemma 4 easily implies that $z = y$, but this leads to a contradiction: if $\sigma_1'\pi_1$ has an ω-power of y as a suffix, the sword $\sigma_1 = \sigma_1'\pi_1 y^{\omega+q_1}$ could not be normal, and if $\pi_2\sigma_2'$ has an ω-power of y as a prefix, the same conclusion applies to the sword $\sigma_2 = y^{\omega+q_2}\pi_2\sigma_2'$.

Now assume that the algorithm TO has revealed that the swords σ_1 and σ_2 have no overlap of height $h - 1$. Then we have to check whether they have an overlap of lesser height. For this, we again represent the swords in the form (8) and apply the algorithm of Lemma 5 to the swords $\rho_1^2\pi_1$ and $\pi_2\rho_2^2$, which are both of height less than h. If there is no overlap between $\rho_1^2\pi_1$ and $\pi_2\rho_2^2$, then there also is no overlap of height less than $h - 1$ between σ_1 and σ_2 and the product $\sigma_1\sigma_2$ is in normal form. Otherwise, the algorithm finds the overlap between $\rho_1^2\pi_1$ and $\pi_2\rho_2^2$. Denoting the overlap by y, we can represent these swords as

$$\rho_1^2\pi_1 = \sigma_1''y^{\omega+r_1} \text{ and } \pi_2\rho_2^2 = y^{\omega+r_2}\sigma_2''$$

for some $r_1, r_2 \in \mathbb{Z}$. Consider the sword $\theta = \sigma_1'\rho_1^{\omega+q_1-2}\sigma_1''y^{\omega+r_1+r_2}\sigma_2''\rho_2^{\omega+q_2-2}\sigma_2'$ obtained from $\sigma_1\sigma_2$ by an $\mathcal{R}/\mathcal{S}$-transition of the form (5). Clearly, to check whether θ is normal amounts to examining overlaps between the swords $\sigma_1'\rho_1^{\omega+q_1-2}\sigma_1''$ and $y^{\omega+r_1+r_2}\sigma_2''\rho_2^{\omega+q_2-2}\sigma_2'$ or between the swords

$\sigma_1' \rho_1^{\omega+q_1-2} \sigma_1'' y^{\omega+r_1+r_2}$ and $\sigma_2'' \rho_2^{\omega+q_2-2} \sigma_2'$. In contrast to the situation in the previous paragraph, here the overlaps may exist, and it appears to make sense to illustrate this phenomenon by an example.

Thus, consider the normal swords $\tau_1 = (x^\omega y)^{\omega+1} x^\omega$ and $\tau_2 = (x^\omega y)^{\omega-2}$ of height 2. They have no overlap of height 1, but do have the overlap of height 0, namely, x: this becomes obvious if we rewrite τ_2 as $x^\omega y (x^\omega y)^{\omega-3}$. Applying an $\mathcal{R}/\mathcal{S}$-transition of the form (5) to the product $\tau_1\tau_2$, we obtain the sword $(x^\omega y)^{\omega+1} x^\omega y (x^\omega y)^{\omega-3}$, and we see that the swords $(x^\omega y)^{\omega+1}$ and $x^\omega y (x^\omega y)^{\omega-3} = (x^\omega y)^{\omega-2}$ have the overlap $x^\omega y$, this time of height 1. Resolving the overlap with yet another transition of the form (5), we finally obtain the normal sword $(x^\omega y)^{\omega-1}$ as a normal form for $\tau_1\tau_2$.

Observe that the above example illustrates not only the difficulty we encounter but also a way to overcome it: since the new overlap has height $h(\tau_1) - 1$, it can be found by the algorithm TO. Mutatis mutandis, this idea works also in the general case.

We return to the proof. Recall that we have to decide if there are overlaps between $\sigma_1' \rho_1^{\omega+q_1-2} \sigma_1''$ and $y^{\omega+r_1+r_2} \sigma_2'' \rho_2^{\omega+q_2-2} \sigma_2'$ or between $\sigma_1' \rho_1^{\omega+q_1-2} \sigma_1'' y^{\omega+r_1+r_2}$ and $\sigma_2'' \rho_2^{\omega+q_2-2} \sigma_2'$. First, we apply TO to decide if there are overlaps of height $h - 1$, and in the case where the answer is positive, to construct a normal form for the sword θ, which will be also a normal form for $\sigma_1\sigma_2$. Suppose that TO has found no overlaps of height $h-1$. Then we apply the algorithm of Lemma 5 to the swords $\rho_1^2 \sigma_1''$ and $y^{\omega+r_1+r_2} \sigma_2'' \rho_2^2$ or to the swords $\rho_1^2 \sigma_1'' y^{\omega+r_1+r_2}$ and $\sigma_2'' \rho_2^2$, which are all of height less than h. If no overlaps are found, then there are no overlaps of height less than $h - 1$ between $\sigma_1' \rho_1^{\omega+q_1-2} \sigma_1''$ and $y^{\omega+r_1+r_2} \sigma_2'' \rho_2^{\omega+q_2-2} \sigma_2'$ nor between $\sigma_1' \rho_1^{\omega+q_1-2} \sigma_1'' y^{\omega+r_1+r_2}$ and $\sigma_2'' \rho_2^{\omega+q_2-2} \sigma_2'$, and the sword θ is normal. Suppose that the algorithm has found the overlap z, say, between $\rho_1^2 \sigma_1''$ and $y^{\omega+r_1+r_2} \sigma_2'' \rho_2^2$ or between $\rho_1^2 \sigma_1'' y^{\omega+p_1+p_2}$ and $\sigma_2'' \rho_2^2$. If z has no ω-power of y as a prefix nor as a suffix, then Lemma 4 implies that $z = y$, and this leads to a contradiction: if $\rho_1^2 \sigma_1''$ has an ω-power of y as a suffix, the sword $\sigma_1 = \sigma_1' \rho_1^{\omega+q_1-4} \rho_1^2 \sigma_1'' y^{\omega+r_1}$ could not be normal, and if $\sigma_2'' \rho_2^2$ has an ω-power of y as a prefix, the same conclusion applies to the sword $\sigma_2 = y^{\omega+r_2} \sigma_2'' \rho_2^2 \rho_2^{\omega+q_2-4} \sigma_2'$. Thus, z has no ω-power of y as a prefix or as a suffix whence $h(y) < h(z) < h - 1$. Now we apply the same sequence of arguments to z, etc. Clearly, each step of the described process deals with some sword θ obtained from $\sigma_1\sigma_2$ by a sequence of $\mathcal{R}/\mathcal{S}$-transitions and leads to exactly one of the three following results:

1. TO finds the overlap of height $h - 1$, resolves it in θ, and returns a normal form for $\sigma_1\sigma_2$.

2. TO finds no overlap of height $h - 1$, and the algorithm of Lemma 5 applied to suitable words of height less than h finds no overlap of height less than $h - 1$, and therefore, θ constitutes a normal form for $\sigma_1\sigma_2$.

3. TO finds no overlap of height $h - 1$, but the algorithm of Lemma 5 applied to suitable words of height less than h finds the overlap whose height is less than $h - 1$ but greater than the height of the overlap found in the previous step. In this case we resolve the overlap in θ and pass to the next step.

It is clear that the number of steps of our process does not exceed h, and therefore, it will eventually return a normal form for $\sigma_1\sigma_2$.

It remains to analyze the situation where one of the swords σ_1 and σ_1 is of height less than h while the other has height h. (In the case where both $h(\sigma_1) < h$ and $h(\sigma_2) < h$, the induction hypothesis applies immediately.) The argument is similar to that described above but simpler because there is no need to invoke the algorithm TO—one of the swords is of height less than h, no overlap of height $h - 1$ is possible. By symmetry, we may suppose that $h(\sigma_1) < h$ and $h(\sigma_2) = h$. Then we can represent σ_2

as $\sigma_2 = \pi_2 \rho_2^{\omega+q_2} \sigma_2'$, where $h(\rho_2) = h - 1$, $h(\pi_2) \leq h - 1$. We apply the algorithm of Lemma 5 to the swords σ_1 and $\pi_2 \rho_2^2$, which are both of height less than h. If there is no overlap between σ_1 and $\pi_2 \rho_2^2$, then there also is no overlap between σ_1 and σ_2 and the product $\sigma_1 \sigma_2$ is in normal form. Otherwise, the algorithm finds the overlap between σ_1 and $\pi_2 \rho_2^2$. Denoting the overlap by y, we can represent these swords as

$$\sigma_1 = \sigma_1'' y^{\omega+r_1} \text{ and } \pi_2 \rho_2^2 = y^{\omega+r_2} \sigma_2''$$

for some $r_1, r_2 \in \mathbb{Z}$. Consider the sword $\theta = \sigma_1'' y^{\omega+r_1+r_2} \sigma_2'' \rho_2^{\omega+q_2-2} \sigma_2'$ obtained from $\sigma_1 \sigma_2$ by an $\mathcal{R}/\mathcal{S}$-transition of the form (5). Clearly, to check whether θ is normal amounts to examining the overlaps between the swords σ_1'' and $y^{\omega+r_1+r_2} \sigma_2'' \rho_2^{\omega+q_2-2} \sigma_2'$ and between the swords $\sigma_1'' y^{\omega+r_1+r_2}$ and $\sigma_2'' \rho_2^{\omega+q_2-2} \sigma_2'$. For this, we apply the algorithm of Lemma 5 to two pairs of swords: σ_1'' and $y^{\omega+r_1+r_2} \sigma_2'' \rho_2^2$ and respectively $\sigma_1'' y^{\omega+r_1+r_2}$ and $\sigma_2'' \rho_2^2$, which swords are all of height less than h. If no overlaps have been discovered, the sword θ is normal and thus constitutes a normal form for the product $\sigma_1 \sigma_2$. If the overlap z, say, has been found, then the same argument as above shows that $h(z) > h(y)$. We apply the same arguments to z, etc. The described process will eventually stop since the height of overlaps increases on each step but cannot reach $h - 1$. $\qquad\square$

Now we study how to construct a normal form for the ω-power of a normal sword.

Lemma 6 *Let ρ be a normal sword of height $h - 1$. There is an algorithm that reduces the sword $\rho^{\omega+q}$ either to a normal sword of height less than h or to a sword of the form $\alpha_1 \beta^{\omega+t} \alpha_2$ in which $h(\alpha_1), h(\alpha_2) \leq h - 1$, $h(\beta) = h - 1$, and the sword $\beta^{\omega+t}$ is normal.*

Proof: Assume that $\rho^{\omega+q}$ is not normal. This means that an $\mathcal{R}/\mathcal{S}$-transition can be applied to the sword. Depending on the form of the transition, one of the three following cases occurs:

1) $\rho = x^{\omega+m_1} x' x^{\omega+m_2}$ for some $m_1, m_2 \in \mathbb{Z}$ and some non-empty x' (the sword x' cannot be empty since ρ is normal);

2) $\rho = x^n$ for some integer $n \geq 2$;

3) $\rho = x^{\omega+m}$ for some integer m.

We apply the algorithm of Lemma 7 to the normal sword ρ of height $h - 1$ to check whether one of the cases 2) or 3) occurs, and if it does, to find a corresponding fully normal sword x. We may additionally assume that $x \neq y^p$ for any integer $p \geq 2$: in case 2) such an x is the sword of minimum length returned by the algorithm while in case 3) this holds automatically since ρ is normal. Then $\rho^{\omega+q}$ can be reduced to $x^{\omega+nq}$ in case 2) or to $x^{\omega+mq}$ in case 3) and either of these two ω-powers is easily seen to be normal.

In the remaining case 1), the sword ρ must have a proper overlap with itself. We can check if this indeed happens by invoking the algorithm of Lemma 5 since the height of ρ is less than h. Moreover, if the overlap exists, it is unique and fully normal, and the algorithm finds it. Thus, assume that $\rho = x_0^{\omega+m_1} x_0' x_0^{\omega+m_2}$ for some fully normal sword x_0 and some $m_1, m_2 \in \mathbb{Z}$. Then the sword $\rho^{\omega+q} = (x_0^{\omega+m_1} x_0' x_0^{\omega+m_2})^{\omega+q}$ can be reduced to the sword $x_0^{\omega+m_1} x_0' (x_0^{\omega+m_1+m_2} x_0')^{\omega+q-1} x_0^{\omega+m_2}$. Consider the sword $\rho_1 = x_0^{\omega+m_1+m_2} x_0'$. It is normal because any $\mathcal{R}/\mathcal{S}$-transition applicable to ρ_1 could have been applied also to ρ while ρ is normal. If $\rho_1^{\omega+q-1}$ is normal, we are done as we can put $\alpha_1 = x_0^{\omega+m_1} x_0'$, $\alpha_2 = x_0^{\omega+m_2}$, and $\beta = \rho_1$.

Suppose that $\rho_1^{\omega+q-1}$ is not normal. Then one of the above cases 1)–3) takes place for ρ_1. We already have seen how to handle case 2): we can reduce $\rho_1^{\omega+q-1}$ to its normal form being an ω-power

of a fully normal word of height less than h. Substituting this normal form for $\rho_1^{\omega+q-1}$ in the sword $x_0^{\omega+m_1}x_0'\rho_1^{\omega+q-1}x_0^{\omega+m_2}$ produces a sword of the desired form $\alpha_1\beta^{\omega+t}\alpha_2$.

In case 3) there is a fully normal sword x_1 of height less than $h-1$ such that $\rho_1 = x_1^{\omega+\ell}$ for some integer ℓ. Then $x_0^{\omega+m_1}x_0'\rho_1^{\omega+q-1}x_0^{\omega+m_2} = x_0^{\omega+m_1}x_0'(x_1^{\omega+\ell})^{\omega+q-1}x_0^{\omega+m_2}$, and we can apply an $\mathcal{R}/\mathcal{S}$-reduction of the form (7) to obtain the sword $x_0^{\omega+m_1}x_0'x_1^{\omega+\ell(q-1)}x_0^{\omega+m_2}$ of height less than h. We can construct a normal form using of the latter sword using Proposition 1.

Finally, consider the situation where ρ_1 falls in case 1). Assume that $\rho_1 = x_1^{\omega+\ell_1}x_1'x_1^{\omega+\ell_2}$ for some $\ell_1, \ell_2 \in \mathbb{Z}$ and some non-empty x_1'. If $h(x_0) = h(x_1)$, then Lemma 4 implies $x_0 = x_1$, and the sword x_0' has some ω-power of x_0 as a suffix. This would mean that the sword $\rho = x_0^{\omega+m_1}x_0'x_0^{\omega+m_2}$ is not normal, a contradiction. If $h(x_0) > h(x_1)$, then x_0 has a prefix of the form $x_1^{\omega+r_1}$ while x_0' has a suffix of the form $x_1^{\omega+r_2}$, and this again contradicts the assumption that ρ is normal. Thus, we conclude that $h(x_0) < h(x_1)$.

We proceed in the same way by reducing the sword $\rho_1^{\omega+q-1} = (x_1^{\omega+\ell_1}x_1'x_1^{\omega+\ell_2})^{\omega+q-1}$ to the sword $x_1^{\omega+\ell_1}x_1'(x_1^{\omega+\ell_1+\ell_2}x_1')^{\omega+q-2}x_1^{\omega+\ell_2}$ and letting $\rho_2 = x_1^{\omega+\ell_1+\ell_2}x_1'$. The only situation where we cannot immediately normalize the sword $\rho_2^{\omega+q-2}$ is that where $\rho_2 = x_2^{\omega+k_1}x_2'x_2^{\omega+k_2}$ for some $k_1, k_2 \in \mathbb{Z}$ and some non-empty x_2'. In this situation, as the argument from the preceding paragraph shows, we must have $h(x_1) < h(x_2)$. We then repeat the procedure, if necessary, until it eventually stops at some sword ρ_s such that the sword $\rho_s^{\omega+q-s}$ can be reduced to a normal sword of the form $\beta^{\omega+t}$ with $h(\beta) < h$. (Since the height of the overlaps $x_0, x_1, x_2, \ldots$ increases on each step, the number of steps is upper bounded by h.) Then the original ω-power $\rho^{\omega+q}$ is reduced to the sword $\alpha_1\beta^{\omega+t}\alpha_2$, where $\alpha_1 = x_0^{\omega+m_1}x_0'x_1^{\omega+\ell_1}x_1' \cdots x_s^{\omega+r_1}x_s'$ and $\alpha_2 = x_s^{\omega+r_2} \cdots x_1^{\omega+\ell_2}x_0^{\omega+m_2}$. $\qquad\square$

Now we are in a position to prove Proposition 1. Recall that is claims the existence of an algorithm that, given a sword σ of height h, returns a normal form of σ.

Proof of Proposition 1: Let $\sigma = \pi_0\rho_1^{\omega+q_1}\pi_1 \cdots \rho_n^{\omega+q_n}\pi_n$ be a height representation of σ. By the induction hypothesis, we assume that all the swords $\rho_1, \ldots, \rho_n$ and $\pi_0, \pi_1, \ldots, \pi_n$ are normal.

By Lemma 6, each sword $\rho_i^{\omega+q_i}$ can be effectively reduced to a sword of the form $\alpha_{i1}\beta_i^{\omega+r_i}\alpha_{i2}$ where the sword $\beta_i^{\omega+r_i}$ is normal of height h while the swords α_{i1}, α_{i2} have height at most $h-1$ and again may be assumed to be normal by the induction hypothesis. Then σ reduces to the following product of normal factors:

$$\pi_0\alpha_{11}\beta_1^{\omega+r_1}\alpha_{12}\pi_1 \ldots \alpha_{n1}\beta_i^{\omega+r_i}\alpha_{n2}\pi_n.$$

The algorithm of Lemma 5 allows us to construct a normal form for the product of two normal swords. Clearly, applying this algorithm several times, we can construct a normal form for the product of any finite number of normal swords, and hence, a normal form for σ. $\qquad\square$

3.4 Longest common prefix

Here we prove Proposition 2. Recall that it claims the existence of an algorithm that, given two normal swords σ and δ, say, both of height at most h, returns their longest common prefix, which we denote by $LCP(\sigma, \delta)$.

Proof of Proposition 2: We fix a height representation of the sword σ with the minimum number of factors of height h and an analogous height representation of the sword δ. We are going to induct on the total number t of factors of height h in these two representations. If $t = 0$, then $h(\sigma), h(\delta) < h$ and the hypothesis of external induction (on h) applies. Consider the situation where one of the swords σ

and δ has height less than h while the other has height h. For certainty, suppose that $h(\delta) < h(\sigma) = h$ and let $\pi_0 \rho_1^{\omega+q_1} \cdots \rho_n^{\omega+q_n} \pi_n$ be the chosen height representation of the sword σ. Then $LCP(\sigma, \delta) = LCP(\pi_0 \rho_1^k, \delta)$ where k is any integer large enough to ensure that $|\pi_0 \rho_1^k| > |\delta|$. Since $h(\pi_0 \rho_1^k) < h$, we can construct $LCP(\pi_0 \rho_1^k, \delta)$ using the external induction hypothesis. Therefore, we may assume that both σ and δ have height h.

First consider a special case where $\sigma = \pi \rho^{\omega+q}$ and $\delta = \alpha \beta^{\omega+r}$ for some $q, r \in \mathbb{Z}$, some swords ρ, β of height $h - 1$ and some swords π, α of height at most $h - 1$. By symmetry, we may assume that $|\alpha| \le |\pi|$.

We start with finding $\tau_1 = LCP(\alpha, \pi)$ using the external induction hypothesis. If $|\tau_1| < |\alpha|$, then clearly $LCP(\sigma, \delta) = \tau_1$. Otherwise, $\tau_1 = \alpha$ and $\pi = \tau_1 \pi'$ for some sword π' of height less than h. Now we should find the longest common prefix τ_2 of the swords $\beta^{\omega+r}$ and $\pi' \rho^{\omega+q}$. First, we verify whether τ_2 can be "long", that is, whether its length can exceed $\max\{|\beta^2|, |\pi'\rho^2|\}$. Since τ_2 is a prefix of $\beta^{\omega+r}$, we conclude that $\pi' = \beta^k \beta_1$ for some integer $k \ge 0$ and some prefix β_1 of β. Let β_2 be such that $\beta = \beta_1 \beta_2$. Then $\beta^{\omega+r} = \pi' \beta_2 \beta^{\omega+r-k-1} = \pi'(\beta_2 \beta_1)^{\omega+r-k-1}\beta_2$, and Lemma 4 implies that $\rho = \beta_2 \beta_1$, see Fig. 5. Hence, $\pi'\rho = \beta^k \beta_1 \beta_2 \beta_1 = \beta \beta^k \beta_1 = \beta \pi'$. Given the swords π', ρ, β, all of height less than
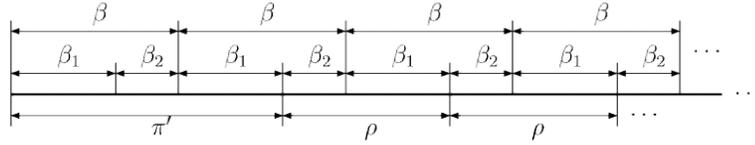

Fig. 5: Structure of τ_2 in case $|\tau_2| > \max\{|\beta^2|, |\pi'\rho^2|\}$

h, we can verify whether the equality $\pi'\rho = \beta\pi'$ holds in view of Corollary 1. If the equality holds true, then clearly $\pi'\rho^\omega = \beta^\omega \pi'$ whence τ_2 is the shortest of the swords $\pi'\rho^{\omega+q}$ and $\beta^{\omega+r}$. If the equality fails, we conclude that $|\tau_2| \le \max\{|\beta^2|, |\pi'\rho^2|\}$ and by the external induction assumption we can find τ_2 as $LCP(\beta^\ell, \pi'\rho^\ell)$ where ℓ is large enough to ensure that $\min\{|\beta^\ell|, |\pi'\rho^\ell|\} > \max(|\beta^2|, |\pi'\rho^2|)$. Finally, we obtain $LCP(\sigma, \delta) = \tau_1 \tau_2$.

Now consider the general case. Isolating the leftmost factors of height h in the height representations of the swords σ and δ chosen at the beginning of the proof, we can represent these swords as follows:

$$\sigma = \pi \rho^{\omega+q} \sigma', \quad \delta = \alpha \beta^{\omega+r} \delta',$$

where $q, r \in \mathbb{Z}$, $h(\rho) = h(\beta) = h - 1$, $h(\alpha), h(\pi) \le h - 1$. Using the algorithm for the special case that we described above, we can construct $\gamma_1 = LCP(\pi\rho^{\omega+q}, \alpha\beta^{\omega+r})$. If $h(\gamma_1) < h$, then clearly $LCP(\sigma, \delta) = \gamma_1$. Otherwise, the construction guarantees that γ_1 is the shortest of the swords $\pi\rho^{\omega+q}$ and $\alpha\beta^{\omega+r}$. For certainty, suppose that $\gamma_1 = \pi\rho^{\omega+q}$ and $\alpha\beta^{\omega+r} = \gamma_1 \delta''$. Since the total number of factors of height h in some height representations of the swords σ' and $\delta''\delta'$ is smaller than t, we can apply the internal induction assumption to find $\gamma_2 = LCP(\sigma', \delta''\delta')$. Then $LCP(\sigma, \delta) = \gamma_1 \gamma_2$. $\quad\square$

In order to close the cycle of simultaneous induction, it remains to prove the following result:

Lemma 7 *There exists an algorithm that, given a normal sword σ of height h, decides whether or not there exists a fully normal sword x such that either σ is an ω-power of x or there is an integer $m \ge 2$*

such that $\sigma = x^m$. If the answer is positive, the algorithm finds x in the first case and all possible pairs (x, m) in the second case.

Proof: If $\sigma = x^{\omega+q}$ for some sword x and integer q, then $|\sigma| = (\omega + q)|x|$ whence the number $-q$ must be a root of the polynomial $|\sigma|$. Thus, we can find all integer roots $q_1, \ldots, q_n$ of $|\sigma|$ and for each $i = 1, \ldots, n$, apply Lemma 1 to verify if σ has a prefix x_i of length $|\sigma|/(\omega + q_i)$. If this is the case, it remains to verify whether $x_i^{\omega+q_i} = \sigma$, and this can be done in view of Corollary 1.

Similarly, $\sigma = x^m$ for some sword x and integer $m \geq 2$, then the number m divides all coefficients of the polynomial $|\sigma|$. Thus, we can find all common divisors $m_1, \ldots, m_k$ of the coefficients of $|\sigma|$ such that $m_1, \ldots, m_k \geq 2$. Then for each $j = 1, \ldots, k$, we apply Lemma 1 to check if σ has a prefix x_j of length $|\sigma|/m_j$, and if this is the case, we use Corollary 1 to verify whether $x_j^{m_j} = \sigma$. $\qquad\square$

4   Proof of the theorem

4.1   *Normal swords and epigroup identities*

Recall that we consider epigroups as unary semigroups under the unary operation of pseudoinversion $x \mapsto \overline{x}$. It is known Shevrin (2005) that the following identities hold in the class $\mathfrak{E}$ of all epigroups:

$$\overline{(xy)}x \approx x\overline{(yx)}, \tag{9}$$

$$\overline{x}^2 x \approx \overline{x}, \tag{10}$$

$$x^2\overline{x} \approx \overline{\overline{x}}, \tag{11}$$

$$\overline{\overline{x}}x \approx \overline{x}x, \tag{12}$$

$$\overline{x^p} \approx \overline{x}^p \quad \text{for each prime } p. \tag{13}$$

We will often use also the identity $\overline{x}x \approx x\overline{x}$ that can be easily deduced from (9)–(13). Indeed,

$$\overline{x}x \overset{(10)}{\approx} \overline{x}^2 x \cdot x \overset{(13)}{\approx} \overline{x^2}x \cdot x \overset{(9)}{\approx} x\overline{x^2} \cdot x = x \cdot \overline{x^2}x \overset{(13)}{\approx} x \cdot \overline{x}^2 x \overset{(10)}{\approx} x\overline{x}.$$

Every unary semigroup term becomes a $\mathbb{Z}$-unary word if one replaces every expression of the form $\overline{x}$ by $x^{\omega-1}$. Conversely, every $\mathbb{Z}$-unary word will be treated as an epigroup term in which expressions of the form $x^{\omega+q}$, $q \in \mathbb{Z}$, are interpreted as follows:

$$x^{\omega+q} = \begin{cases} \overline{x}x^{q+1}, & \text{if } q \text{ is non-negative;} \\ \overline{x}^{(-q)}, & \text{otherwise.} \end{cases}$$

Proposition 3 *If $\mathbb{Z}$-unary words σ, σ' are $\mathcal{S}$-related, then the identity $\sigma \approx \sigma'$ holds in $\mathfrak{E}$.*

Proof: It suffices to verify that, for every integer q, each epigroup satisfies the identities

$$xx^{\omega+q} \approx x^{\omega+q+1}, \tag{14}$$

$$x^{\omega+q}x \approx x^{\omega+q+1}, \tag{15}$$

$$(xy)^{\omega+q}x \approx x(yx)^{\omega+q} \tag{16}$$

that correspond to the pairs (2)–(4) generating the relation $\mathcal{S}$ as a fully invariant congruence.

First, suppose that $q \geq 0$. Then $x^{\omega+q} = \overline{x}x^{q+1}$. Note that, since $\overline{x}x \approx x\overline{x}$, we have $\overline{x}x^{q+1} \approx x^{q+1}\overline{x}$. Therefore, the identities (14) and (15) clearly hold in $\mathfrak{E}$ since

$$xx^{\omega+q} \approx xx^{q+1}\overline{x} = x^{q+2}\overline{x} \approx x^{\omega+q+1} \text{ and } x^{\omega+q}x = \overline{x}x^{q+1}x = \overline{x}x^{q+2} = x^{\omega+q+1}.$$

Consider the identity (16). We have

$$(xy)^{\omega+q}x = \overline{xy}(xy)^{q+1}x = \overline{xy}x(yx)^{q+1} \stackrel{(9)}{\approx} x\overline{yx}(yx)^{q+1} = x(yx)^{\omega+q}.$$

Now suppose that $q < 0$. In this case $x^{\omega+q} = \overline{x}^{(-q)}$. If $q = -1$, then the identity (14) becomes $xx^{\omega-1} \approx x^{\omega}$, and it clearly holds in $\mathfrak{E}$ because $xx^{\omega-1} = x\overline{x}$ while $x^{\omega} = \overline{x}x$. For $q < -1$, we use (10) to obtain

$$xx^{\omega+q} = x\overline{x}^{(-q)} = x\overline{x}^2\overline{x}^{(-q-2)} \stackrel{(10)}{\approx} \overline{x}\,\overline{x}^{(-q-2)} = \overline{x}^{(-q-1)} = x^{\omega+q+1}.$$

The identity (15) is treated in the same way. Finally, we have

$$(xy)^{\omega+q}x = \overline{xy}^{(-q)}x = \overline{xy}^{(-q-1)}\overline{xy}x \stackrel{(9)}{\approx} \overline{xy}^{(-q-1)}x\overline{yx} \stackrel{(9)}{\approx} \dots$$

$$\stackrel{(9)}{\approx} x\overline{yx}\,\overline{yx}^{(-q-1)} = x\overline{yx}^{(-q)} = x(yx)^{\omega+q},$$

thus establishing (16). □

Proposition 3 allows us to treat expressions of the form $\sigma \approx \sigma'$, with σ, σ' being swords, as epigroup identities.

Proposition 4 *Let σ_1 and σ_2 be two swords and let α_1 and respectively α_2 be their normal forms. Then the identity $\sigma_1 \approx \sigma_2$ holds in $\mathfrak{E}$ if and only if so does the identity $\alpha_1 \approx \alpha_2$.*

Proof: It is enough to show that if α is a normal form of a sword σ, then the identity $\sigma \approx \alpha$ holds in $\mathfrak{E}$. For this, it clearly suffices to prove that $\mathfrak{E}$ satisfies the identities

$$x^{\omega+r}x^{\omega+q} \approx x^{\omega+r+q}, \tag{17}$$

$$(x^n)^{\omega+q} \approx x^{\omega+nq}, \tag{18}$$

$$(x^{\omega+r})^{\omega+q} \approx x^{\omega+rq} \tag{19}$$

for all $q, r \in \mathbb{Z}$ and all $n \geq 2$ as these identities correspond to the reduction rules (5)–(7) used in the normalization procedure.

The proof of (17) splits in 4 cases depending on the signs of q and r. If $q, r \geq 0$, we have

$$x^{\omega+r}x^{\omega+q} = \overline{x}x^{r+1}\overline{x}x^{q+1} \approx \overline{x}^2x^{r+q+2} \stackrel{(10)}{\approx} \overline{x}x^{p+q+1} = x^{\omega+p+q}$$

If $q, r < 0$, the proof is straightforward since

$$x^{\omega+r}x^{\omega+q} = \overline{x}^{(-r)}\,\overline{x}^{(-q)} = \overline{x}^{(-r-q)} = x^{\omega+r+q}.$$

Assume that $r \geq 0$ and $q < 0$. Then

$$x^{\omega+r}x^{\omega+q} = \overline{x}x^{r+1}\overline{x}^{(-q)} \approx \overline{x}^{(-q+1)}x^{r+1} \stackrel{(10)}{\approx} \begin{cases} \overline{x}x^{r+q+1} & \text{if } r \geq -q; \\ x^{-q-r} & \text{if } r < -q. \end{cases}$$

On the other hand, by the definition, we have

$$x^{\omega+r+q} = \begin{cases} \overline{x}x^{r+q+1} & \text{if } r \geq -q; \\ x^{-q-r} & \text{if } r < -q. \end{cases}$$

Thus, we conclude that $x^{\omega+r}x^{\omega+q} \approx x^{\omega+r+q}$. The case where $r < 0$ and $q \geq 0$ is completely analogous.

Before we proceed with proving (18), we notice that the identity $\overline{x^n} \approx \overline{x}^n$ holds in $\mathfrak{E}$ for every positive integer n. For this, we induct on n. The claim is trivial for $n = 1$. If $n > 1$, represent n as $n = kp$, with p being prime. Then we have $\overline{x^k} \approx \overline{x}^k$ by the induction assumption whence

$$\overline{x^n} = \overline{x^{kp}} = \overline{(x^k)^p} \stackrel{(13)}{\approx} \overline{x^k}^p \approx (\overline{x}^k)^p = \overline{x}^{kp} = \overline{x}^n.$$

Now, for each $q \geq 0$, we have

$$(x^n)^{\omega+q} = \overline{x^n}(x^n)^{q+1} \approx \overline{x}^n x^{nq+n} \stackrel{(10)}{\approx} \overline{x}^{n-1}x^{nq+n-1} \stackrel{(10)}{\approx} \ldots \stackrel{(10)}{\approx} \overline{x}x^{nq+1} = x^{\omega+nq}.$$

For $q < 0$, we have

$$(x^n)^{\omega+q} = \overline{x^n}^{(-q)} \approx (\overline{x}^n)^{-q} = \overline{x}^{(-nq)} = x^{\omega+nq}.$$

In order to verify (19), we first show that $\overline{\overline{\overline{x}}} \approx \overline{x}$. Indeed, substituting $\overline{x}$ for x in (11), we get

$$\overline{\overline{\overline{x}}} \approx \overline{x}^2\overline{\overline{x}} \stackrel{(11)}{\approx} \overline{x}^2 x^2 \overline{x} \approx \overline{x}^3 x^2 \stackrel{(10)}{\approx} \overline{x}^2 x \stackrel{(10)}{\approx} \overline{x}.$$

We use this to deduce yet another auxiliary identity, namely, $\overline{x^{\omega+r}} \approx x^{\omega-r}$ for every integer $r \in \mathbb{Z}$. If $r > 0$, we have

$$\overline{x^{\omega+r}} = \overline{\overline{x}x^{r+1}} \stackrel{(10)}{\approx} \overline{\overline{x}^2 x^{r+2}} \stackrel{(10)}{\approx} \ldots \stackrel{(10)}{\approx} \overline{\overline{x}^r x^{2r}} \approx \overline{(\overline{x}x^2)^r} \approx \left(\overline{\overline{x}x^2}\right)^r \approx$$

$$\left(\overline{x^2\overline{x}}\right)^r \stackrel{(11)}{\approx} \left(\overline{\overline{x}}\right)^r \approx \overline{x}^r = (x^{\omega-1})^r \approx x^{\omega-r}.$$

Here we have repeatedly employed (17) in the final step. If $r = 0$, we have

$$\overline{x^\omega} = \overline{\overline{x}x} \stackrel{(12)}{\approx} \overline{x}x = x^\omega.$$

If $r < 0$, we have

$$\overline{x^{\omega+r}} = \overline{\overline{x}^{(-r)}} \approx \overline{\overline{x}}^{(-r)} \stackrel{(11)}{\approx} (x^2\overline{x})^{-r} \approx (\overline{x}x^2)^{-r} = \overline{x}^{-r}x^{-2r} \stackrel{(10)}{\approx} \ldots \stackrel{(10)}{\approx} \overline{x}x^{-r+1} = x^{\omega-r}.$$

Now we are ready to deduce the identity (19). If $q \geq 0$, we have

$$(x^{\omega+r})^{\omega+q} = \overline{x^{\omega+r}}(x^{\omega+r})^{q+1} \approx x^{\omega-r}(x^{\omega+r})^{q+1} \approx x^{\omega+rq},$$

and if $q < 0$, we have

$$(x^{\omega+r})^{\omega+q} \approx \overline{x^{\omega+r}}^{(-q)} \approx (x^{\omega-r})^{(-q)} \approx x^{\omega+rq},$$

where the final steps in each of the two deductions follow from (17). $\square$

4.2 Connections to Burnside varieties

For any pair (m, k) of positive integers, the semigroup variety $\mathfrak{B}_{m,k}$ defined by the identity $x^m \approx x^{m+k}$ is called a *Burnside variety*. Let A be a finite set and denote by $B(A, m, k)$ the free A-generated semigroup in the variety $\mathfrak{B}_{m,k}$. We recall some results due to Victor Guba Guba (1993a,b).

Theorem 2 (Guba (1993b), Theorem A) *For $m \geq 3$, $k \geq 1$, the word problem for the semigroup $B(A, m, k)$ is decidable.*

Theorem 3 *For $m \geq 3$, $k \geq 1$, every element of the semigroup $B(A, m, k)$ has a finite number of factors.*

The next statement easily follows from Theorem 3. We supply a proof for the sake of completeness.

Proposition 5 *For $m \geq 3$, $k \geq 1$, the Burnside variety $\mathfrak{B}_{m,k}$ is generated by its finite members.*

Proof: Take any two different elements $a, b \in B(A, m, k)$ and let F_{ab} the set of all factors of their product ab. By Theorem 3, F_{ab} is finite, and it is easy to see that the set $I(ab) = B(A, m, k) \setminus F_{ab}$ forms an ideal of $B(A, m, k)$. Thus, the Rees quotient $B(A, m, k)/I(ab)$ is finite and the natural homomorphism $B(A, m, k) \to B(A, m, k)/I(ab)$ separates a and b since $a, b \notin I(ab)$. Therefore, the semigroup $B(A, m, k)$ is residually finite for any finite set A. Since each variety is generated by the collection of its finitely generated free objects, the variety $\mathfrak{B}_{m,k}$ is generated by its finite members. $\qquad\square$

In the sequel, it will be convenient to consider only the varieties $\mathfrak{B}_{m,k}$ with $k > m$. Observe that every such variety satisfies the identity $x^k \approx x^{2k}$. Indeed,

$$x^{2k} = x^{(m+k)+(k-m)} = x^{m+k}x^{k-m} \approx x^m x^{k-m} = x^{m+(k-m)} = x^k.$$

Semigroups in the Burnside varieties are periodic, and hence, we may (and will) treat them as epigroups. It is easy to see that in every epigroup from $\mathfrak{B}_{m,k}$ with $k > m$ one has $\overline{x} = x^{k-1}$ and $x^\omega = \overline{x}x = x^k$.

Let α be a $\mathbb{Z}$-unary word. We define the *depth* of α as follows:

$$d(\alpha) := \max\{0, -q \mid \text{ the expression } \omega + q \text{ occurs in } \alpha\}.$$

For instance, $d\big((x^{\omega-4}yx^{\omega+30})^{\omega-1}xy^\omega\big) = 4$. Given an integer $k > d(\alpha)$, we denote by $\alpha^{(k)}$ the expression obtained from α by substituting k for each occurrence of ω in α. The inequality $k > d(\alpha)$ ensures that after the substitution, all expressions $\omega + q$ involved in α become positive integers, and hence, $\alpha^{(k)}$ is in fact a well-formed ordinary word. Now take any $\ell > d(\alpha)$, any $k > \ell$ and let $m = k - \ell$. Then it is easy to see that the identity $\alpha \approx \alpha^{(k)}$ holds true in the variety $\mathfrak{B}_{m,k}$.

We want to extend "ordinarization" transforms of the form $\alpha \mapsto \alpha^{(k)}$ to swords. There is a subtlety here because the concept of depth is well defined only for $\mathbb{Z}$-unary words and not for swords: if two $\mathbb{Z}$-unary words α and α' are obtained from each other by "unwinding" or "winding up", they represent the same sword, but the equality $d(\alpha) = d(\alpha')$ need not be true. Therefore, given a sword σ, we should first fix a $\mathbb{Z}$-unary word α representing σ and choose an integer k strictly larger than $d(\alpha)$; we then denote by $\sigma^{(k)}$ the word $\alpha^{(k)}$. Observe that the conclusion that the identity $\sigma \approx \sigma^{(k)}$ holds in the variety $\mathfrak{B}_{m,k}$ remains valid for **every** choice of a $\mathbb{Z}$-unary word representing the sword σ provided that k is strictly larger than m and $\ell = k - m$ is is strictly larger than the depth of the chosen $\mathbb{Z}$-unary word.

We need also yet another auxiliary construction $\sigma \mapsto \widehat{\sigma}$ that associates ordinary words to swords. Again, it is first defined for $\mathbb{Z}$-unary words and then we extend it to swords by utilizing the same approach as

above, that is, by fixing a $\mathbb{Z}$-unary word representing a given sword. If α is a $\mathbb{Z}$-unary word, we define $\widehat{\alpha}$ using induction on height. If $h(\alpha) = 0$, i.e., if α is an ordinary word, then $\widehat{\alpha} := \alpha$. If $h(\alpha) > 0$, let $\pi_0 \rho_1^{\omega+q_1} \pi_1 \cdots \rho_n^{\omega+q_n} \pi_n$ be the height representation of α. Then for each $i = 1, \ldots, n$, we define $q_i' = 2$ if $q_i \leq 2$ and $q_i' = q_i$ otherwise, and let $\widehat{\alpha} := \widehat{\pi_0}\widehat{\rho_1}^{q_1'}\widehat{\pi_1} \cdots \widehat{\rho_n}^{q_n'}\widehat{\pi_n}$. For instance, if $\sigma = (x^{\omega-4}yx^{\omega+30})^{\omega-1}xy^{\omega}$, then $\widehat{\sigma} = (x^2yx^{30})^2yx^2$.

In the following statements and their proofs, whenever both constructions $\sigma^{(k)}$ and $\widehat{\sigma}$ are used, we assume that they are produced from the same $\mathbb{Z}$-unary word representing the sword σ.

Lemma 8 *Let σ_1, σ_2 be two normal swords. Suppose that $\sigma_1^{(k)} = \sigma_2^{(k)}$ for every choice of $\mathbb{Z}$-unary words representing σ_1 and σ_2, every $\ell > \max\{d(\sigma_1), d(\sigma_2)\}$ and every k such that $k - \ell - 2 > \max\{|\widehat{\sigma_1}|, |\widehat{\sigma_2}|\}$. Then $\sigma_1 = \sigma_2$.*

Proof: Suppose that $\sigma_1 \neq \sigma_2$. Let τ be the longest common prefix of σ_1 and σ_2 (it exists by Proposition 2). We write σ_1 and σ_2 as $\sigma_1 = \tau\rho_1$ and $\sigma_2 = \tau\rho_2$ for some swords ρ_1 and ρ_2 such that either one of them is empty while the other is not or they both are non-empty and start with different letters. Consider some $\mathbb{Z}$-unary words α, β_1, β_2 representing the swords τ, ρ_1, ρ_2 respectively. Then, clearly, the $\mathbb{Z}$-unary words $\alpha\beta_1$ and $\alpha\beta_2$ represent the swords σ_1 and respectively σ_2. If the parameters ℓ and k are calculated from these representations, then we have $\sigma_1^{(k)} = \tau^{(k)}\rho_1^{(k)}$ and $\sigma_2^{(k)} = \tau^{(k)}\rho_2^{(k)}$ whence $\rho_1^{(k)} = \rho_2^{(k)}$. Thus, the swords ρ_1 and ρ_2 that differ at their start should become equal when each ω in them is substituted with k. This is obviously not possible one of the swords is empty while the other is not since no ordinarization transform sends a non-empty sword to the empty word. Nor is it possible if ρ_1 and ρ_2 are non-empty and start with different letters because the starting letters of $\rho_1^{(k)}$ and $\rho_2^{(k)}$ remain the same as the ones of ρ_1 and respectively ρ_2. Thus, we arrive at a contradiction. $\square$

Recall that an ordinary word u is said to be *periodic* if $u = v^n$ for some word v and some $n \geq 2$.

Lemma 9 *Let σ be a normal sword. It is periodic if and only if the word $\sigma^{(k)}$ is periodic for every choice of a $\mathbb{Z}$-unary word representing σ, every $\ell > d(\sigma)$ and every k such that $k - \ell - 2 > |\widehat{\sigma}|$.*

Proof: If σ is a power then so is $\sigma^{(k)}$, and if σ is an ω-power, say, $\sigma = \tau^{\omega+q}$, then $\sigma^{(k)} = \left(\tau^{(k)}\right)^{k+q}$, and conditions imposed on k guarantee that $k + q \geq 2$. Conversely, suppose that an ordinarization of the sword σ is equal to v^n for some word v and some $n \geq 2$. Then a $\mathbb{Z}$-unary word representing σ should decompose as $\alpha_1 \cdots \alpha_n$, where the ordinarization sends each factor α_i, $i = 1, \ldots, n$, to the word v. If the parameters ℓ and k are calculated from this representation of the sword σ and τ_i is the normal sword represented by α_i, $i = 1, \ldots, n$, we have $\sigma = \tau_1 \cdots \tau_n$ and $\tau_i^{(k)} = v$ for each $i = 1, \ldots, n$. Since $|\widehat{\tau_i}| \leq |\widehat{\sigma}|$, we can apply Lemma 8 to the swords τ_i and obtain that they are all equal. Therefore σ is periodic. $\square$

A central concept in Guba's papers Guba (1993a,b) is the notion of the reduced form of a word relative to the Burnside variety $\mathfrak{B}_{m,k}$. We are not going to reproduce here the original definition of this notion because it is quite involved (it is given by simultaneous induction on five other notions) and because, as the reader will see, we can easily bypass the definition by working with a sufficient condition for a word to be in the reduced form (see Lemma 10 below). First we reproduce a result which is crucial for our considerations; it constitutes the main point of the proof of Theorem 4.1 in Guba (1993a).

Theorem 4 *Let $m \geq 3$, $k \geq 1$, and let u and v be words. The identity $u \approx v$ holds in the variety $\mathfrak{B}_{m,k}$ if and only if u and v have the same reduced forms relative to $\mathfrak{B}_{m,k}$.*

Now we again assume that $k > m$ and, as above, let $\ell = k - m$. For short, words that are in the reduced form relative to $\mathfrak{B}_{m,k}$ will be called $\mathfrak{B}_{m,k}$-*reduced* words. The following result that is a consequence of Lemma 2.2 in Guba (1993a) is sufficient for our purposes.

Lemma 10 *Let $k > m \geq 3$ and $\ell = k - m$. A word is $\mathfrak{B}_{m,k}$-reduced if it contains no factors of the form* $v^{2k-\ell-2}$.

We use Lemma 10 to prove that, for a normal sword σ and large enough k, the word $\sigma^{(k)}$ is $\mathfrak{B}_{m,k}$-reduced. We start with considering swords of height 1.

Lemma 11 *Let σ be a normal sword of height 1 and $\ell > d(\sigma)$, $k - \ell - 2 > |\widehat{\sigma}|$. Then the word $\sigma^{(k)}$ is $\mathfrak{B}_{m,k}$-reduced.*

Proof: Since $h(\sigma) = 1$, we have

$$\sigma = u_0 v_1^{\omega+q_1} u_1 \cdots v_n^{\omega+q_n} u_n,$$

for some ordinary words $u_0, u_1, \ldots u_n, v_1, \ldots, v_n$. Suppose that for some word v, the word $\sigma^{(k)}$ has a factor of the form $v^{2k-\ell-2}$. First assume that $v = v_i$ for some $i = 1, \ldots, n$. Since the sword σ is normal, Lemma 4 implies that the sword $v_{i-1}^2 u_{i-1} v_i^{\omega+q_i} u_i v_{i+1}^2$ is not a factor of any v_i-periodic sword. Therefore, $v_i^{2k-\ell-2}$ is a factor of the word $v_{i-1}^2 u_{i-1} v_i^{k+q_i} u_i v_{i+1}^2$. Consider the word $v_{i-1}^2 u_{i-1} v_i^{q_i'} u_i v_{i+1}^2$ where $q_i' = 2$ if $q_i \leq 2$ and $q_i' = q_i$ otherwise. Its length is not larger than $|\widehat{\sigma}|$. But $|v_i^{k-\ell-2}| > k - \ell - 2 > |\widehat{\sigma}|$. This implies that $v_i^{2k-\ell-2}$ cannot be a factor of $v_{i-1}^2 u_{i-1} v_i^{k+q_i} u_i v_{i+1}^2$.

Thus, the word $v^{2k-\ell-2}$ is a product of words of the form $t_1 v_i^{k+q_i} \ldots v_j^{k+q_j} t_2$ where t_1 is either a suffix of u_i or equals to $v_{i-1}^{s_1} u_i$, t_2 is either a prefix of u_{j+1} or equals to $u_{j+1} v_{j+1}^{s_2}$. Let $L = \max\{|v_i| \mid v_i \text{ is a factor of the word } v\}$. Then $|v|^{2k-\ell-2} \leq |\widehat{\sigma}| + Lk$. On the other hand, $|v|^{2k-\ell-2} \geq |v|k + k - \ell - 2 > |v|k + |\widehat{\sigma}|$. This implies $|v| < L$, a contradiction. $\square$

Now we consider the swords of larger height.

Lemma 12 *Let σ be a normal sword of height $h > 1$ then, for all integers k, p such that $p > p(\sigma)$ and $k - \ell - 2 > |\widehat{\sigma}|$, the word $\sigma^{(k)}$ is a $\mathfrak{B}_{m,k}$-reduced form.*

Proof: We are going to prove this lemma by induction on height of the sword σ using Lemma 11 as the basis of induction.

Let $\pi_0 \rho_1^{\omega+q_1} \pi_1 \ldots \rho_n^{\omega+q_n} \pi_n$ be a height representation of the sword σ. Consider the sword

$$\widetilde{\sigma} = \pi_0^{(k)} (\rho_1^{(k)})^{\omega+q_1} \pi_1^{(k)} \ldots (\rho_n^{(k)})^{\omega+q_n} \pi_n^{(k)}$$

of height 1. Note that $\sigma^{(k)} = \widetilde{\sigma}^{(k)}$.

By the induction hypothesis we have that all the words $\pi_i^{(k)}$ and $\rho_i^{(k)}$ are $\mathfrak{B}_{m,k}$-reduced forms. Let us prove now that $\widetilde{\sigma}$ is a normal sword. Indeed, the words ρ_i are not periodic by Lemma 9. Next, suppose that, for some index i, $(\rho_i^{(k)})^{\omega+q_i} \pi_i (\rho_{i+1}^{(k)})^{\omega+q_{i+1}} = (uv)^{\omega+q_i} u (vu)^{\omega+q_{i+1}}$. Let $\alpha_1, \alpha_2, \beta_1, \beta_2$ be swords such that $\alpha_1 \alpha_2 = \rho_i, \beta_1 \beta_2 = \rho_{i+1}$ and $\alpha_1^{(k)} = \beta_2^{(k)} = \pi_i^{(k)} = u, \alpha_2^{(k)} = \beta_1^{(k)} = v$. Again by Lemma 8 the following equalities hold $\alpha_1 = \beta_2 = \pi_i, \alpha_2 = \beta_1$. Thus, $(\alpha_1 \alpha_2)^{\omega+q_i} \alpha_1 (\alpha_2 \alpha_1)^{\omega+q_{i+1}}$ is a subsword of the normal sword σ. This implies that the sword $\widetilde{\sigma}$ is normal.

We proceed assuming that the word $\widetilde{\sigma}$ is not a $\mathfrak{B}_{m,k}$-reduced form and, for some word T, it contains $T^{2k-\ell-2}$ as a factor. Similarly to the proof of Lemma 11 suppose firstly that, for some index i, $T = \rho_i^{(k)}$. Again the word $\tau = (\rho_{i-1}^{(k)})^2\pi_{i-1}^{(k)}(\rho_{i-1}^{(k)})^{\omega+q_i}\pi_i^{(k)}(\rho_{i+1}^{(k)})^2$ can not be some factor of some T-periodic sword by Lemma 4. Thus, $|\tau| > |T^{2k-\ell-2}|$ and the length of $\tau^{(k)}$ does not exceed $|\widehat{\sigma}| + |\rho_i^{(k)}|k$. On the other hand, $|T^{2k-\ell-2}| = |\rho_i^{(k)}|(2k-\ell-2) > |\rho_i^{(k)}|k + |\rho_i^{(k)}||\widehat{\sigma}|$, a contradiction.

Suppose now that T has the form $t_1(\rho_i^{(k)})^{k+q_i}\ldots(\rho_j^{(k)})^{k+q_j}t_2$ where t_1 is a suffix of $\rho_{i-1}^{(k)}\pi_{i-1}^{(k)}$, t_2 is a prefix of $\pi_{j+1}\rho_{j+1}^{(k)}$. Let L be the maximum of $|\rho_i^{(k)}|$ where $\rho_i^{(k)}$ is a factor of T. Therefore,

$$|T| \leq Lk + |t_1(\rho_i^{(k)})^{q_i'}\ldots(\rho_j^{(k)})^{q_j'}t_2| \leq Lk + L|\widehat{\sigma}|.$$

But $|T|^{2k-\ell-2} = |T|k + |T|(k-\ell-2) > |T|(k+|\widehat{\sigma}|) > L(k+|\widehat{\sigma}|)$.

Hence, the word $\widetilde{\sigma}^{(k)}$ that equals to $\sigma^{(k)}$ is a $\mathfrak{B}_{m,k}$-reduced form. □

These lemmas lead us to the important

Proposition 6 *Let σ_1, σ_2 be two normal swords then the equality $\sigma_1 \approx \sigma_2$ holds in $\mathfrak{E}$ ($\mathfrak{E}_{fin}$) if and only if σ_1 and σ_2 are equal.*

Proof: Remind that every Burnside semigroup is an epigroup. Also, in view of Proposition 5 the free Burnside semigroup satisfies any identity that holds in $\mathfrak{E}_{fin}$. Thus, the identities $\sigma_1 \approx \sigma_2$ and, therefore, $\sigma_1^{(k)} \approx \sigma_2^{(k)}$ holds in the variety $var[x^{2k-\ell} \approx x^{k-\ell}]$ for large enough k, ℓ and $m = k - \ell$. By Lemmas 11 and 12 the words $\sigma_1^{(k)}$ and $\sigma_2^{(k)}$ are $\mathfrak{B}_{m,k}$-reduced forms. Then by Theorem 4 the words $\sigma_1^{(k)}$ and $\sigma_2^{(k)}$ are equal. Hence, by Lemma 8 the swords σ_1 and σ_2 coincide.

□

Proof of Theorem 1: Let $\sigma_1 \approx \sigma_2$ be any identity that holds in $\mathfrak{E}_{fin}$ or $\mathfrak{E}$. By Proposition 1 there is an algorithm that constructs normal forms α_1, α_2 of the swords σ_1, σ_2 respectively and the identity $\alpha_1 \approx \alpha_2$, by Proposition 4, also holds in $\mathfrak{E}_{fin}$ or $\mathfrak{E}$. By Proposition 6 this identity is equivalent to the equality of the swords α_1 and α_2 which we can check using algorithm from Proposition 2.

The following proof was given by M. Volkov in a verbal discussion. Let us prove that the identity basis of $\mathfrak{E}$ is infinite. For a prime number p, consider a non-trivial group G satisfying the identity $x^p \approx 1$. Let H be the semigroup G with adjoined 0. Define a unary operation on H by the following rule: for all $x \neq 1$ we set $\overline{x} = 0$, and $\overline{1} = 1$. It is clear that the unary semigroup H satisfies the first five identities.

Let q be a prime number distinct from p and let $x \in H$. Then $x^q \neq 1$ if and only if $x \neq 1$. Therefore, for $x \neq 1$, $\overline{x^q} = 0 = \overline{x}^q$. Thus, the identity $\overline{x^q} \approx \overline{x}^q$ holds in H. Meanwhile, taking $x \in G$ distinct from 1 we obtain $1 = \overline{x^p} \neq \overline{x}^p = 0$. Hence, the identity $\overline{x^p} \approx \overline{x}^p$ fails in H. □

Acknowledgements

References

J. Almeida. *Finite Semigroups and Universal Algebra*. World Scientific, 1995.

J. Almeida and B. Steinberg. On the decidability of iterated semidirect products and applications to complexity. *Proceedings of the London Mathematical Society*, 80:55–74, 2000.

J. C. Costa. Canonical forms for free κ-semigroups. Technical report, Universidade do Minho, 2013. URL http://arxiv.org/abs/1309.1450.

J. C. Costa. Canonical forms for free κ-semigroups. *Discrete Math. Theor. Comput. Sci*, 26:159–178, 2014.

V. Guba. The word problem for the relatively free semigroup satisfying $t^m = t^{m+n}$ with $m \geq 4$ or $m = 3, n = 1$. *International Journal of Algebra and Computation*, 3:125–140, 1993a.

V. Guba. The word problem for the relatively free semigroup satisfying $t^m = t^{m+n}$ with $m \geq 3$. *International Journal of Algebra and Computation*, 3:335–347, 1993b.

J. McCammond. Normal forms for free aperiodic semigroups. *International Journal of Algebra and Computation*, 11:581–625, 2001.

J. Reiterman. The Birkhoff theorem for finite algebras. *Algebra Universalis*, 14:1–10, 1982.

L. N. Shevrin. On the theory of epigroups. I. *Russian Acad. Sci. Sb. Math.*, 82:485–512, 1994a.

L. N. Shevrin. On the theory of epigroups. II. *Russian Acad. Sci. Sb. Math.*, 83:133–154, 1994b.

L. N. Shevrin. Epigroups. In V. B. Kudryavtsev and I. V. Rosenberg, editors, *Structural theory of automata, semigroups, and universal algebra*, Proc. NATO Advance Study Institute Workshop at the CRM, pages 331–380. Springer, 2005.

I. Y. Zhil'tsov. On ω-identities of finite semigroups. In C. L. Nehaniv and M. Ito, editors, *Algebraic Engineering*, Proc. Kyoto Workshop on Computer Systems and Formal Languages and First International Conference on Semigroups and Algebraic Engineering, pages 427–436. World Scientific, 1999.

I. Y. Zhil'tsov. On identities of epigroups. *Doklady Mathematics*, 375:10–13, 2000.