WORD PROBLEM FOR KNOTTED RESIDUATED LATTICES

ROSTISLAV HORČÍK

ABSTRACT. In this paper we prove that almost all varieties $\mathcal{RL}_m^n$ of residuated lattices satisfying $x^m \leq x^n$ have undecidable word problem. Namely, we show it for $1 \leq m < n$ and $2 \leq n < m$. Consequently, also the varieties $\mathcal{RL}_m^n \cap \mathcal{RL}_n^m$ for $2 \leq m, n$ have undecidable word problem. Finally, the same is proved also for varieties of distributive residuated lattices satisfying $x^m \leq x^n$ for $1 \leq m < n$.

1. INTRODUCTION

The identity $x^m = x^n$ received a lot of attention in semigroup theory. Having a variety $\mathcal{V}$ of semigroups defined by this identity, one can pose many questions concerning properties of $\mathcal{V}$. For example the question whether $\mathcal{V}$ is locally finite is just the bounded Burnside problem for semigroups. Another bunch of interesting questions arises from various decision problems for $\mathcal{V}$; for instance the word problem, decidability of its equational or universal theory. The literate on these topics is quite extensive. An overview of known results can be found in [5, 12, 4, 17].

In this paper we are interested in analogous questions replacing semigroups by residuated lattices which are lattice-ordered monoids whose monoid operation is residuated. Formally, a residuated lattice $\mathbf{A} = \langle A, \wedge, \vee, \cdot, \backslash, /, 1\rangle$ is an algebraic structure such that $\langle A, \wedge, \vee\rangle$ is a lattice, $\langle A, \cdot, 1\rangle$ is a monoid and for all $a, b, c \in A$ we have

$$a \cdot b \leq c \quad \text{iff} \quad b \leq a\backslash c \quad \text{iff} \quad a \leq c/b\,. \tag{1}$$

It is easy to see that the monoid operation has to be monotone in each argument by (1). It is well known that the class of all residuated lattices forms a variety $\mathcal{RL}$. For details on residuated lattices see [8].

We are interested in subvarieties of $\mathcal{RL}$ satisfying $x^m = x^n$. Since residuated lattices are ordered algebras, it makes sense to split the identity $x^m = x^n$ into two inequalities $x^m \leq x^n$ and $x^n \leq x^m$ and study particular inequalities separately. The class of residuated lattices satisfying $x^m \leq x^n$ still forms a variety (which we denote $\mathcal{RL}_m^n$) because $x^m \leq x^n$ is equivalent to $x^m \vee x^n = x^n$. The inequalities $x^m \leq x^n$ correspond to so-called knotted rules introduced in [10] dealing with proof theory of substructural logics for which residuated lattices are roughly speaking the same as Boolean algebras for classical logic.

Concerning decision problems for varieties $\mathcal{RL}_m^n$, it was proved in [18] that if we restrict to the variety $\mathcal{CRL}$ of commutative residuated lattices (i.e., residuated lattices with commutative monoid operation) then the universal theory is decidable. More precisely, the universal theory of $\mathcal{RL}_m^n \cap \mathcal{CRL}$ is decidable for $m \geq 1$, $n \geq 0$ and $m \neq n$ (the remaining cases for $m = 0$ are trivial). The proof is done by establishing the finite embeddability property (FEP); for the definition of FEP and its relation to decision problems see [6, 1, 2]. In this we paper we are

Key words and phrases. Residuated lattice, knotted rule, word problem, residuated frame, semi-Thue system.

going to show that in noncommutative case most of the varieties $\mathcal{RL}_m^n$ and $\mathcal{RL}_m^n \cap \mathcal{RL}_n^m$ have undecidable word problem (Theorem 5.2).

In order to prove this we construct a semi-Thue system $\langle \Sigma, R\rangle$ simulating a Minsky machine on square-free words (Section 4). This construction is inspired by the technique used in (see [12, Section 7.2.5]). Then in Section 5 we construct from $\langle \Sigma, R\rangle$ a residuated lattice via a residuated frame (for details on residuated frames see [7]). This construction is new partially resembling the construction on phase spaces due to Lafont [13].

Further we prove that some of the varieties of distributive residuated lattices satisfying $x^m \leq x^n$ have undecidable word problem as well (Theorem 5.5). Our proof can be also used in order to answer negatively the open question [2, Problem 4.5] asking whether the class of join-semilattice-ordered residuated semigroups satisfying $x^n = x^{n+1}$ possesses the FEP for $n \geq 2$. Since we can show that this class has undecidable word problem, it cannot have the FEP as the FEP would imply decidability of its universal theory.

Throughout the paper we are going to use the following notation and terminology. The set of natural numbers is denoted $\mathbb{N} = \{0, 1, 2, \ldots\}$. Let $n, m \in \mathbb{N}$ and $n < m$. Then $[n, m] = \{k \in \mathbb{N} \mid n \leq k \leq m\}$. Given a set X, $x \in X$ and an equivalence $\sim$ on X, the equivalence class of x with respect to $\sim$ is denoted $[x]_\sim$. A preorder on a set P is a reflexive and transitive relation $\preceq\, \subseteq P \times P$. If $\preceq$ is also antisymmetric then $\langle P, \preceq\rangle$ is called a poset. Let Σ be a finite set called alphabet. The set of all finite sequences (words) of elements from Σ is denoted Σ^*. In fact, Σ^* together with concatenation and the empty word ε forms the free monoid generated by Σ. Given a word $w \in \Sigma^*$, the reversely written w is denoted $\overline{w}$; e.g., $\overline{abcb} = bcba$. We say that a word $w \in \Sigma^*$ contains a square if $w = uxxv$ for some $u, x, v \in \Sigma^*$. A word $w \in \Sigma^*$ is called square-free if it does not contain a square.

2. Preliminaries

We start by recalling several notions which we will need at the sequel. First, we briefly review the word problem for a variety of algebras. Let $\mathcal{L}$ be an algebraic language, i.e., containing no relational symbol. Given a set X, one can build the set of terms $T(X)$ from X using the operations from $\mathcal{L}$. The set $T(X)$ forms the absolutely free algebra $\mathbf{T}(X)$ for the language $\mathcal{L}$ generated by X. A quasi-identity is a formula of the form

$$t_1 = s_1 \;\&\; \ldots \;\&\; t_n = s_n \implies t_0 = s_0\,, \tag{2}$$

where $t_0, s_0, \ldots, t_n, s_n \in T(X)$ are terms. Identities are special quasi-identities having empty premise. Let $\mathcal{K}$ be a class of algebras for the language $\mathcal{L}$. We say that (2) holds in $\mathcal{K}$ if for every algebra $\mathbf{A} \in \mathcal{K}$ and every homomorphism $\varphi\colon T(X) \to A$ we have $\varphi(t_0) = \varphi(s_0)$ provided that $\varphi(t_i) = \varphi(s_i)$ for all $i = 1, \ldots, n$.

A presentation for $\mathcal{L}$ is a pair $\langle X, E\rangle$ where X is a set of generators and E a set of identities over $T(X)$. If both X and E are finite, we call the presentation $\langle X, E\rangle$ finite. We denote the conjunction of identities in E by $\&E$. Consider a variety $\mathcal{V}$ of algebras for the language $\mathcal{L}$. Then $\mathcal{V}$ has undecidable word problem if there exists a finite presentation $\langle X, E\rangle$ such that there is no algorithm deciding whether the quasi-identity

$$\&E \implies t = s \tag{3}$$

holds in $\mathcal{V}$ having $t, s \in T(X)$ as input. More precisely, the set of pairs $\langle t, s\rangle \in T(X)^2$ such that (3) holds in $\mathcal{V}$ is undecidable. This definition is equivalent to the usual one saying that $\mathcal{V}$ has undecidable word problem if there is a finitely presented algebra $\mathbf{A} \in \mathcal{V}$ generated by a set X such that the following set is undecidable (see e.g. [8, Section 4.4]):

$$\{\langle t, s\rangle \in T(X)^2 \mid t = s \text{ holds in } \mathbf{A}\}\,.$$

Note that if $\mathcal{V}$ has undecidable word problem then it has undecidable quasi-equational hence also universal theory.

In order to show that the word problem for a variety of algebras is undecidable, one needs an undecidable problem to start with. We will use the halting problem for a Minsky machine. A Minsky machine $\mathcal{M}$ is a deterministic two-counter machine given by a finite number of states $[0, M] = \{0, 1, \ldots, M\}$, 0 is the final state, and a map

$$\tau\colon [1, M] \to \{+\} \times \{1, 2\} \times [0, M] \cup \{-\} \times \{1, 2\} \times [0, M] \times [0, M]\,,$$

describing the behavior of $\mathcal{M}$ by assigning to a non-final state an instruction for the machine. A triple $\langle i, n, m\rangle \in [0, M] \times \mathbb{N}^2$ is called a configuration of $\mathcal{M}$ where i is a state and n, m represent respectively the content of the first and the second counter. The set of all configurations of $\mathcal{M}$ is denoted $\mathrm{Conf}(\mathcal{M})$. Given a configuration $\langle i, n, m\rangle$ of $\mathcal{M}$, the map τ defines the next configuration in the computation of $\mathcal{M}$ as follows:

- $\langle j, n+1, m\rangle$ if $\tau(i) = \langle +, 1, j\rangle$ (increment the first counter),
- $\langle j, n-1, m\rangle$ if $\tau(i) = \langle -, 1, j, k\rangle$ and $n > 0$ (decrement the first counter),
- $\langle k, n, m\rangle$ if $\tau(i) = \langle -, 1, j, k\rangle$ and $n = 0$ (test if the first counter is zero),
- $\langle j, n, m+1\rangle$ if $\tau(i) = \langle +, 2, j\rangle$ (increment the second counter),
- $\langle j, n, m-1\rangle$ if $\tau(i) = \langle -, 2, j, k\rangle$ and $m > 0$ (decrement the second counter),
- $\langle k, n, m\rangle$ if $\tau(i) = \langle -, 2, j, k\rangle$ and $m = 0$ (test if the second counter is zero).

The machine $\mathcal{M}$ stops when $i = 0$ (note that τ is defined only for $i > 0$). A configuration $\langle i, n, m\rangle$ is said to be accepted by $\mathcal{M}$ if, starting from $\langle i, n, m\rangle$, $\mathcal{M}$ eventually stops its computation with empty counters (i.e., it stops at the configuration $\langle 0, 0, 0\rangle$). The set of configurations accepted by $\mathcal{M}$ is denoted $\mathrm{AConf}(\mathcal{M})$.

THEOREM 2.1 ([14, 16]). *There is a Minsky machine $\mathcal{M}$ whose set* $\mathrm{AConf}(\mathcal{M})$ *of accepted configurations is undecidable.*

Finally, we review the notion of residuated frame and show how it is related to residuated lattices. Recall that a residuated lattice is an algebra $\mathbf{A} = \langle A, \wedge, \vee, \cdot, \backslash, /, 1\rangle$ where $\langle A, \wedge, \vee\rangle$ is a lattice, $\langle A, \cdot, 1\rangle$ is a monoid and for all $a, b, c \in A$ we have

$$a \cdot b \leq c \qquad \text{iff} \qquad b \leq a\backslash c \qquad \text{iff} \qquad a \leq c/b\,.$$

An important example of a residuated lattice is the powerset monoid.

EXAMPLE 2.2 (see e.g. [11, 8]). *Let $\mathbf{M} = \langle M, \cdot, 1\rangle$ be a monoid. The powerset monoid is the residuated lattice $\mathcal{P}(\mathbf{M}) = \langle \mathcal{P}(M), \cap, \cup, \cdot, \backslash, /, \{1\}\rangle$ defined on the powerset of M, where for $A, B, C \subseteq M$ the operations are defined as follows:*

$$\begin{aligned} A \cdot B &= \{a \cdot b \in M \mid a \in A,\ b \in B\}\,, \\ A\backslash C &= \{b \in M \mid A \cdot \{b\} \subseteq C\}\,, \\ C/B &= \{a \in M \mid \{a\} \cdot B \subseteq C\}\,. \end{aligned}$$

Moreover, the monoid $\mathbf{M}$ embeds into $\mathcal{P}(\mathbf{M})$ via $x \mapsto \{x\}$.

Other examples of residuated lattices can be obtained from the powerset monoid $\mathcal{P}(\mathbf{M})$ by considering a suitable closure operator on the poset $\langle \mathcal{P}(M), \subseteq\rangle$. Recall that a closure operator on a poset $\mathbf{P} = \langle P, \leq\rangle$ is a map $\gamma\colon P \to P$ such that for all $x, y \in P$ we have

$x \leq \gamma(x)$, $\gamma(\gamma(x)) = \gamma(x)$ and $x \leq y$ implies $\gamma(x) \leq \gamma(y)$. The subposet $\langle \gamma[P], \leq \rangle$ is denoted $\mathbf{P}_\gamma = \langle P_\gamma, \leq \rangle$ and its elements are called γ-closed.

Let S be a set. Recall that every closure operator on the powerset $\langle \mathcal{P}(S), \subseteq \rangle$ is induced by a binary relation $N \subseteq S \times T$ for some set T (see e.g. [8]). Having such relation $N \subseteq S \times T$, one can introduce the following two maps which define a Galois connection between $\langle \mathcal{P}(S), \subseteq \rangle$ and $\langle \mathcal{P}(T), \subseteq \rangle$:

$$\begin{aligned} X^{\triangleright} &= \{b \in T \mid (\forall x \in X)(x\ N\ b)\}\,, \\ Y^{\triangleleft} &= \{a \in S \mid (\forall y \in Y)(a\ N\ y)\}\,. \end{aligned}$$

The maps ${}^{\triangleleft}$ and ${}^{\triangleright}$ are the polarities of this Galois connection having the following well-known properties.

LEMMA 2.3 (see e.g. [8]). *Let $N \subseteq S \times T$. Then we have*

1. *$X \subseteq Y$ implies $Y^{\triangleright} \subseteq X^{\triangleright}$ for $X, Y \subseteq S$.*
2. *$X \subseteq Y$ implies $Y^{\triangleleft} \subseteq X^{\triangleleft}$ for $X, Y \subseteq T$.*
3. *$\emptyset^{\triangleleft} = S$ and $\emptyset^{\triangleright} = T$.*
4. *${}^{\triangleright\triangleleft\triangleright} = {}^{\triangleright}$ and ${}^{\triangleleft\triangleright\triangleleft} = {}^{\triangleleft}$.*
5. *The map $\gamma_N \colon \mathcal{P}(S) \to \mathcal{P}(S)$ defined by $\gamma_N(X) = X^{\triangleright\triangleleft}$ is a closure operator on $\langle \mathcal{P}(S), \subseteq \rangle$.*

We will refer to the closure operator γ_N as the closure operator induced by the relation N. Let $x \in S$. To shorten the notation, we will write $\gamma_N\{x\}$ instead of $\gamma(\{x\})$.

Assume that we have a closure operator γ on a residuated lattice $\mathbf{A} = \langle A, \wedge, \vee, \cdot, \backslash, /, 1 \rangle$. If γ satisfies $\gamma(\gamma(x) \cdot \gamma(y)) = \gamma(x \cdot y)$ for all $x, y \in A$ then γ is called nucleus. In this case one can define a residuated lattice on γ-closed elements. The resulting algebra $\mathbf{A}_\gamma = \langle A_\gamma, \wedge, \vee_\gamma, \cdot_\gamma, \backslash, /, \gamma(1) \rangle$, where $x \vee_\gamma y = \gamma(x \vee y)$ and $x \cdot_\gamma y = \gamma(x \cdot y)$, is a residuated lattice (see e.g. [8]). Note that $\gamma \colon A \to A_\gamma$ is a monoid homomorphism since $\gamma(x \cdot y) = \gamma(\gamma(x) \cdot \gamma(y)) = \gamma(x) \cdot_\gamma \gamma(y)$.

Given a monoid $\mathbf{M}$, we can construct the powerset monoid $\mathcal{P}(\mathbf{M})$. Further, any binary $N \subseteq M \times T$ induces a closure operator γ_N on $\langle \mathcal{P}(M), \subseteq \rangle$. The following definition captures the cases when γ_N is nucleus.

DEFINITION 2.4 ([7]). *A residuated frame is a two-sorted structure $\mathbf{W} = \langle \mathbf{M}, T, N \rangle$ where $\mathbf{M} = \langle M, \cdot, 1 \rangle$ is a monoid, T is a set and $N \subseteq M \times T$ is a nuclear relation, i.e., there exist operations $\backslash\!\!\backslash \colon M \times T \to T$ and $/\!\!/ \colon T \times M \to T$ such that*

$$x \cdot y\ N\ z \qquad \text{iff} \qquad y\ N\ x \backslash\!\!\backslash z \qquad \text{iff} \qquad x\ N\ z /\!\!/ y\,.$$

Having a residuated frame $\mathbf{W} = \langle \mathbf{M}, T, N \rangle$, the induced closure operator γ_N is in fact a nucleus on the powerset monoid $\mathcal{P}(\mathbf{M})$ (see [7]). Thus one can define the complex algebra $\mathbf{W}^+$ of the residuated frame $\mathbf{W}$ by letting $\mathbf{W}^+$ to be the residuated lattice $\mathcal{P}(\mathbf{M})_{\gamma_N}$.

LEMMA 2.5. *The map $\varphi \colon M \to W^+$ defined by $\varphi(x) = \gamma_N\{x\}$ is a monoid homomorphism.*

Proof. Note that φ is a composition of the map $x \mapsto \{x\}$ and γ_N. Since both these maps are monoid homomorphisms, the claim follows. $\square$

3. Pomonoids and semi-Thue systems

In this section we review semi-Thue systems (also known as string rewriting systems) (see e.g. [3]) and their relation to partially ordered monoids. Semi-Thue systems will serve us as an intermediate structure for reducing the halting problem for Minsky machines into the word problem for residuated lattices.

A partially ordered monoid (pomonoid for short) is a structure $\mathbf{A} = \langle A, \cdot, 1, \leq\rangle$ such that $\langle A, \cdot, 1\rangle$ is a monoid and for all $a, b, u, v \in A$ we have $a \leq b$ implies $uav \leq ubv$. Note that any monoid can be viewed as a pomonoid ordered discretely. In particular the free finitely generated monoid Σ^* is also a pomonoid.

Let $\mathbf{A}$ be a monoid and $\preceq$ a preorder on A. We say that $\preceq$ is compatible if for all $a, b, u, v \in A$ we have $a \preceq b$ implies $uav \preceq ubv$. Having a compatible preorder $\preceq$, one can define a monoid congruence $\sim$ on $\mathbf{A}$ as follows:

$$x \sim y \quad \text{iff} \quad x \preceq y \text{ and } y \preceq x\,.$$

A congruence of a pomonoid $\mathbf{A} = \langle A, \cdot, 1, \leq\rangle$ is a compatible preorder $\preceq$ containing $\leq$. Then we can define the quotient pomonoid as $\mathbf{A}/{\preceq} = \langle \hat{\mathbf{A}}/{\sim}, {\preceq}/{\sim}\rangle$, where $\hat{\mathbf{A}} = \langle A, \cdot, 1\rangle$ is the monoid reduct of $\mathbf{A}$ and $[x]_\sim \preceq/{\sim}\, [y]_\sim$ iff $x \preceq y$.

Pomonoid homomorphisms are order-preserving monoid homomorphisms. Given pomonoids $\mathbf{A}$, $\mathbf{B}$, a pomonoid homomorphism $\varphi\colon A \to B$ induces the following pomonoid congruence $\leq_\varphi$ on $\mathbf{A}$:

$$x \leq_\varphi y \quad \text{iff} \quad \varphi(x) \leq \varphi(y)\,.$$

Let Σ be an alphabet and $u_0, \ldots, u_n, v_0, \ldots, v_n \in \Sigma^*$. A quasi-inequality is a formula of the following form:

$$u_1 \leq v_1 \;\&\; \ldots \;\&\; u_n \leq v_n \quad \Longrightarrow \quad u_0 \leq v_0\,. \tag{4}$$

The quasi-inequality (4) holds in a pomonoid $\mathbf{A}$ if for every pomonoid homomorphism $\varphi\colon \Sigma^* \to A$ we have $\varphi(u_0) \leq \varphi(v_0)$ whenever $\varphi(u_i) \leq \varphi(v_i)$ for all $i = 1, \ldots, n$.

Next we are going to define semi-Thue systems which one can view as finite pomonoid presentations. Given an alphabet Σ, a semi-Thue system is a tuple $\langle \Sigma, R\rangle$, where $R \subseteq \Sigma^* \times \Sigma^*$ is a finite binary relation on Σ^*. The elements $\langle x, y\rangle \in R$ are called rules and are usually denoted $x \to y$. A single-step reduction relation $\to_R \subseteq \Sigma^* \times \Sigma^*$ is defined as follows:

$$s \to_R t \text{ iff there are } u, v \in \Sigma^* \text{ and } x \to y \in R \text{ such that } s = uxv \text{ and } t = uyv.$$

If we want to stress that $r = x \to y$ is the element of R witnessing $s \to_R t$ then we also write $s \xrightarrow{r}_R t$. If $x \to y$ is a rule then $y \to x$ is called its inverse.

A reduction relation $\to_R^*$ is the reflexive transitive closure of $\to_R$. In fact $\to_R^*$ is the least compatible preorder on the free monoid Σ^* containing R. Thus $\Sigma^*/{\to_R^*}$ is a pomonoid.

LEMMA 3.1. *Let $\langle \Sigma, R\rangle$ be a semi-Thue system and $u, v \in \Sigma^*$. Assume that $R = \{u_1 \to v_1, \ldots, u_n \to v_n\}$ and consider the following quasi-inequality*

$$u_1 \leq v_1 \;\&\; \ldots \;\&\; u_n \leq v_n \quad \Longrightarrow \quad u \leq v\,. \tag{5}$$

Then (5) *holds in every pomonoid if, and only if, $u {\to_R^*} v$.*

Proof. Assume that $u {\to_R^*} v$. Let $\mathbf{A} = \langle A, \cdot, 1, \leq\rangle$ be a pomonoid and $\varphi\colon \Sigma^* \to A$ a pomonoid homomorphism such that $\varphi(u_i) \leq \varphi(v_i)$ for all $i = 1, \ldots, n$. This means that $u_i \leq_\varphi v_i$ for every rule from R, i.e., $R \subseteq {\leq_\varphi}$. Since $\to_R^*$ is the least compatible preorder containing R, we have ${\to_R^*} \subseteq {\leq_\varphi}$. Consequently, $u {\to_R^*} v$ implies $\varphi(u) \leq \varphi(v)$. Conversely, if (5) holds in every pomonoid then it holds in $\Sigma^*/{\to_R^*}$. Consequently, we have $u {\to_R^*} v$. $\square$

4. An undecidable Semi-Thue system

Let $\mathcal{M}$ be a Minsky machine such that the set $\mathrm{AConf}(\mathcal{M})$ of accepted configurations is undecidable (cf. Theorem 2.1). Now we are going to simulate $\mathcal{M}$ by a semi-Thue system $\langle \Sigma, R\rangle$ in such a way that the acceptance of a configuration is translated into the accessibility of a fixed word. In order to do this, we need to encode any configuration into a word over the alphabet Σ and the instruction map τ needs to be encoded into the set of rules R. Our coding is based on the idea from [12, Section 7.2.5]

One of the simplest ways how to encode a configuration $\langle i, n, m\rangle$ into a word is $Aa^n q_i a^m B \in \Sigma^*$ for $\Sigma = \{a, q_0, \dots, q_M, A, B\}$. Then the instructions are expressed by rules as follows:

- if $\tau(i) = \langle +, 1, j\rangle$ then we add $q_i \to aq_j$,
- if $\tau(i) = \langle -, 1, j, k\rangle$ then we add $aq_i \to q_j$ and $Aq_i \to Aq_k$.
- if $\tau(i) = \langle +, 2, j\rangle$ then we add $q_i \to q_j a$,
- if $\tau(i) = \langle -, 2, j, k\rangle$ then we add $q_i a \to q_j$ and $q_i B \to q_k B$.

However this encoding is not suitable if we want to deal with inequalities $x^r \leq x^s$, $r, s \in \mathbb{N}$, because the numbers stored in counters are encoded by powers a^n, a^m. In order to overcome this difficulty, we will encode numbers in counters by square-free words.

For this purpose we need a way how to construct square-free words. Let $h\colon \Sigma^* \to \Sigma^*$ be a monoid endomorphism. Then h is called square-free if $h(x)$ is square-free for all square-free words $x \in \Sigma^*$. Recall that every square-free endomorphism is injective.

EXAMPLE 4.1 ([15]). *Let $\Sigma = \{a, b, c\}$ and let $h\colon \Sigma^* \to \Sigma^*$ be the monoid endomorphism defined as follows:*

$$\begin{aligned} h(a) &= abc\,, \\ h(b) &= ac\,, \\ h(c) &= b\,. \end{aligned}$$

Then h is square-free.

Using the square-free monoid endomorphism h from Example 4.1, one can produce longer and longer square-free words by considering the words $h^k(a)$ for $k \in \mathbb{N}$ where $h^0(a) = a$ and $h^{k+1}(a) = h(h^k(a))$. This suggests that we can encode a number $n \in \mathbb{N}$ stored in a counter by the square-free word $h^n(a)$. Note that since the first letter of $h(a)$ is again a, it is easy to see that for every $n > 0$ we have $h^n(a) = h(a)w$ for some $w \in \Sigma^*$. This property is needed in order to recognize whether the counter is nonempty. We will also need a square-free endomorphism $g\colon \Sigma^* \to \Sigma^*$ with the dual property, namely $g^n(a) = ug(a)$ for $n > 0$ and some $u \in \Sigma^*$. One can define $g(x) = \overline{h(\overline{x})}$. Then g is again a square-free monoid endomorphism. Moreover, we have

$$g^n(a) = \overline{h^n(\overline{a})} = \overline{h^n(a)} = \overline{h(a)w} = \overline{w}\overline{h(\overline{a})} = \overline{w}g(a)\,.$$

Now we are ready to describe the complete encoding of $\mathcal{M}$ into a semi-Thue system $\langle \Sigma, R\rangle$. We have symbols $\Sigma_Q = \{q_0, \dots, q_m\}$ encoding the states of $\mathcal{M}$. Further, we have auxiliary symbols

$$\Sigma_{Aux} = \{A, B, B^+, B^-, C, C^+, C^-, D\}\,.$$

Finally, we have symbols $\Sigma_S = \{a, b, c\}$ for building square-free words. Thus our alphabet is $\Sigma = \Sigma_Q \cup \Sigma_{Aux} \cup \Sigma_S$.

The instructions τ are captured by the set R consisting of the following rules for every $i \in [1, M]$ depending on $\tau(i)$:

$$(r_i^{+1}) \qquad Bq_i \to B^+q_j \qquad \text{if } \tau(i) = \langle +, 1, j\rangle\,,$$

$$(r_i^{+2}) \qquad q_iC \to q_jC^+ \qquad \text{if } \tau(i) = \langle +, 2, j\rangle\,,$$

$$(r_i^{-1}) \qquad g(a)Bq_i \to g(a)B^-q_j,\ AaBq_i \to AaBq_k \qquad \text{if } \tau(i) = \langle -, 1, j, k\rangle\,,$$

$$(r_i^{-2}) \qquad q_iCh(a) \to q_jC^-h(a),\ q_iCaD \to q_kCaD \qquad \text{if } \tau(i) = \langle -, 2, j, k\rangle\,,$$

Further R contains the following auxiliary rules for every $d \in \Sigma_S$:

$$(r^1_{aux}) \qquad AB^+ \to AB,\ AB^- \to AB,\ dB^+ \to B^+g(d),\ Bd \to dB,\ g(d)B^- \to B^-d\,,$$

$$(r^2_{aux}) \qquad C^+D \to CD,\ C^-D \to CD,\ C^+d \to h(d)C^+,\ dC \to Cd,\ C^-h(d) \to dC^-\,.$$

A configuration $\langle i, n, m\rangle$ is going to be represented by the word $Ag^n(a)Bq_iCh^m(a)D$. Nevertheless, since one step of the computation of $\mathcal{M}$ is going to be simulated by several rewriting steps, there are several words which correspond to the configuration $\langle i, n, m\rangle$. For instance, the incrementation of the first counter is simulated as follows. Assume that we have a configuration $\langle i, n, m\rangle$ and $\tau(i) = \langle +, 1, j\rangle$. Let us denote $g^n(a) = d_1 \dots d_k$ and $g^{n+1}(a) = e_1 \dots e_l$ for some $d_1, \dots, d_k, e_1, \dots, e_l \in \Sigma_S$. Thus $g^{n+1}(a) = g(d_1 \dots d_k) = g(d_1) \dots g(d_k)$. Using consecutively the rules (r_i^{+1}), (r^1_{aux}), we have

$$\begin{aligned}
Ag^n(a)Bq_iCh^m(a)D &\to_R Ag^n(a)B^+q_jCh^m(a)D = Ad_1 \dots d_kB^+q_jCh^m(a)D\\
&\to_R Ad_1 \dots B^+g(d_k)q_jCh^m(a)D\\
&\to_R^* AB^+g(d_1 \dots d_k)q_jCh^m(a)D\\
&\to_R ABg(d_1 \dots d_k)q_jCh^m(a)D = ABe_1 \dots e_lq_jCh^m(a)D\\
&\to_R Ae_1B \dots e_lq_jCh^m(a)D\\
&\to_R^* Ae_1 \dots e_lBq_jCh^m(a)D = Ag^{n+1}(a)Bq_jCh^m(a)D\,.
\end{aligned}$$

In order to make the correspondence between configurations and words precise, we will define a map ϕ assigning to every configuration of $\mathcal{M}$ a set of words over Σ. The map $\phi\colon \mathrm{Conf}(\mathcal{M}) \to \mathcal{P}(\Sigma^*)$ will assign to every configuration $\langle i, n, m\rangle$ a set of words $\phi(i, n, m)$ in such a way that $\langle i, n, m\rangle \neq \langle j, n', m'\rangle$ implies $\phi(i, n, m) \cap \phi(j, n', m') = \emptyset$.

Let $n \in \mathbb{N}$. We start with a definition of the set $B_n \subseteq \Sigma^*$ containing words representing the fact that the number stored in the first counter is n.

$$\begin{aligned}
B_n^0 &= \{AuBv \in \Sigma^* \mid uv = g^n(a),\ u, v \in \Sigma_S^*\}\,,\\
B_n^+ &= \begin{cases}\{AuB^+g(v) \in \Sigma^* \mid uv = g^{n-1}(a),\ u, v \in \Sigma_S^*\} & \text{if } n > 0\,,\\ \emptyset & \text{if } n = 0\,,\end{cases}\\
B_n^- &= \{Ag(u)B^-v \in \Sigma^* \mid uv = g^n(a),\ u, v \in \Sigma_S^*\}\,,\\
B_n &= B_n^0 \cup B_n^+ \cup B_n^-\,.
\end{aligned}$$

Note that the sets B_n's are pair-wise disjoint. Indeed, suppose that $w \in B_n \cap B_m$. Due to the auxiliary symbols B, B^+, B^-, we have precisely one of the following cases: $w \in B_n^0 \cap B_m^0$, $w \in B_n^+ \cap B_m^+$, $w \in B_n^- \cap B_m^-$. Let us discuss the second case; the other cases are similar. Since $w \in B_n^+ \cap B_m^+$, we have $n, m > 0$ and $w = Au_1B^+g(v_1) = Au_2B^+g(v_2)$ for $u_1v_1 = g^{n-1}(a)$

and $u_2v_2 = g^{m-1}(a)$. Consequently, $u_1 = u_2$ and $g(v_1) = g(v_2)$. Since g is injective, we have $v_1 = v_2$. Thus $g^{n-1}(a) = g^{m-1}(a)$. Using injectivity of g again, we obtain $n = m$.

Further, it is obvious that B_n's contain only square-free words because uv and $g(uv) = g(u)g(v)$ are square-free and thus $u, v, g(u), g(v)$ are square-free as well since square-free words are closed under taking subwords.

We also have analogous definitions also for the second counter representing a value $n \in \mathbb{N}$:

$$\begin{aligned} C_n^0 &= \{uCvD \in \Sigma^* \mid uv = h^n(a),\ u, v \in \Sigma_S^*\}\,, \\ C_n^+ &= \begin{cases} \{h(u)C^+vD \in \Sigma^* \mid uv = h^{n-1}(a),\ u, v \in \Sigma_S^*\} & \text{if } n > 0\,, \\ \emptyset & \text{if } n = 0\,, \end{cases} \\ C_n^- &= \{uC^-h(v)D \in \Sigma^* \mid uv = h^n(a),\ u, v \in \Sigma_S^*\}\,, \\ C_n &= C_n^0 \cup C_n^+ \cup C_n^-\,. \end{aligned}$$

Similarly as for B_n's, the sets C_n's are pair-wise disjoint containing only square-free words.

Now we can define the map $\phi\colon \mathrm{Conf}(\mathcal{M}) \to \mathcal{P}(\Sigma^*)$ assigning to a configuration of $\mathcal{M}$ its corresponding set of words from Σ^* as follows:

$$\phi(i, n, m) = \{uq_iv \in \Sigma^* \mid u \in B_n,\ v \in C_m\}\,.$$

It is straightforward to check that sets $\phi(i, n, m)$ and $\phi(j, n', m')$ are disjoint if $\langle i, n, m\rangle \neq \langle j, n', m'\rangle$ using the fact that B_n's and C_m's are pair-wise disjoint.

Then we define the set of canonical words Can as words which correspond to a configuration, namely

$$Can = \bigcup_{\langle i,n,m\rangle \in \mathrm{Conf}(\mathcal{M})} \phi(i, n, m)\,.$$

Note that every canonical word w belongs to a unique $\phi(i, n, m)$, i.e., it corresponds precisely to one configuration. It is also easy to see that canonical words are square-free since B_n's and C_m's consist of square-free words.

LEMMA 4.2. *The set of canonical words Can contains only square-free words.*

The set of canonical words corresponding to the accepted configurations $\mathrm{AConf}(\mathcal{M})$ is denoted $ACan$, i.e.,

$$ACan = \bigcup_{\langle m,i,n\rangle \in \mathrm{AConf}(\mathcal{M})} \phi(m, i, n)\,.$$

In the rest of this section we are going to prove that the set $ACan$ is precisely the set of words which can be rewritten to $AaBq_0CaD$ (i.e., the word corresponding to the configuration $\langle 0, 0, 0\rangle$).

We first analyze some parts of the preordered set $\langle \Sigma^*, \to_R^*\rangle$. Let $n \in \mathbb{N}$, $i \in [0, M]$ and $q_i \in \Sigma_Q$. Then B_nq_i denotes the set $\{uq_i \in \Sigma^* \mid u \in B_n\}$. The set q_iC_m for $m \in \mathbb{N}$ is defined analogously. Observe that B_nq_i is closed under applications of the auxiliary rules (r^1_{aux}). Moreover, (r^1_{aux}) are the only rules in R which can be applied to B_nq_i in such a way the result is still in B_nq_i. The set q_iC_m and the auxiliary rules (r^2_{aux}) satisfies an analogous claim. In fact, by inspection of the rules in R, it is easy to realize how the preorder $\to_R^*$ behaves on B_nq_i and q_iC_m. Namely, the tuples $\langle B_nq_i, \to_R^*\rangle$ and $\langle q_iC_m, \to_R^*\rangle$ form posets whose Hasse diagrams are depicted respectively in Figure 1 and 2.

The posets B_nq_i's and q_iC_m's are further connected by $\to_R^*$ according to the instruction map τ. Depending on $\tau(i)$, we have four cases:

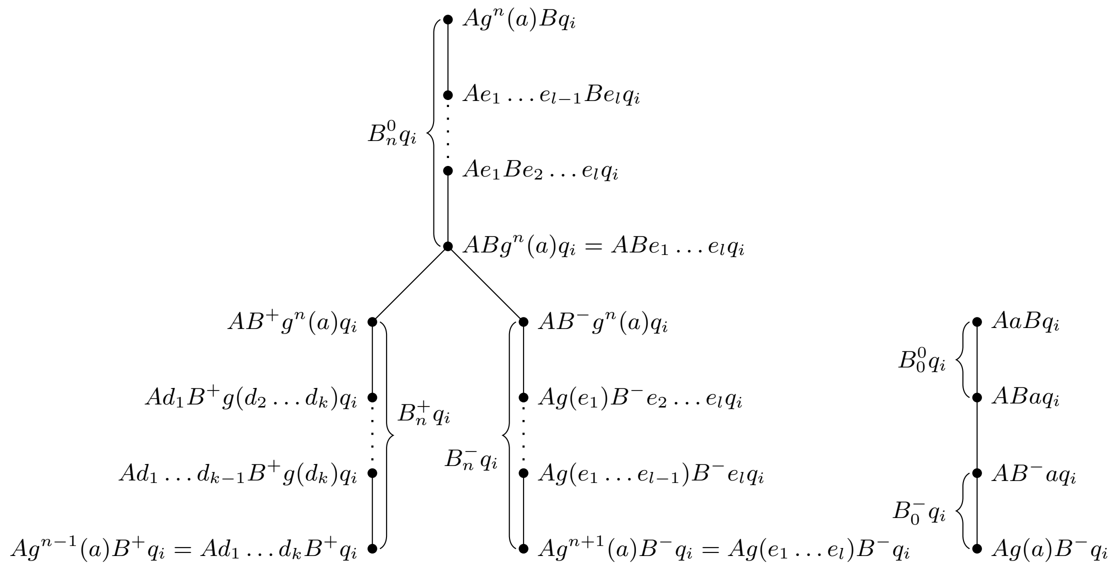

FIGURE 1. Hasse diagram of $\langle B_nq_i, \to_R^*\rangle$ for $n > 0$ left and for $n = 0$ right. We assume that $g^{n-1}(a) = d_1 \dots d_k$ and $g^n(a) = e_1 \dots e_l$ for some $d_1, \dots, d_k, e_1, \dots, e_l \in \Sigma_S$.

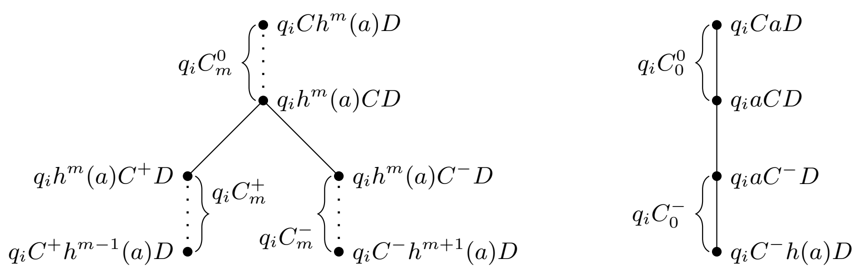

FIGURE 2. Hasse diagram of $\langle q_iC_m, \to_R^*\rangle$ for $m > 0$ left and for $m = 0$ right.

(1) if $\tau(i) = \langle +, 1, j\rangle$ then the maximum $Ag^n(a)Bq_i$ of B_nq_i is connected to $Ag^n(a)B^+q_j \in B_{n+1}q_j$ (see Figures 3 and 4).
(2) if $\tau(i) = \langle -, 1, j, k\rangle$ then $Ag^n(a)Bq_i \in B_nq_i$ is connected either to $Ag^n(a)B^-q_j \in B_{n-1}q_j$ if $n > 0$ (see Figure 3) or to $AaBq_k \in B_0q_k$ if $n = 0$ (see Figure 4).
(3) if $\tau(i) = \langle +, 2, j\rangle$ then $q_iCh^m(a)D \in q_iC_m$ is connected to $q_jC^+h^m(a)D \in q_jC_{m+1}$.
(4) if $\tau(i) = \langle -, 2, j, k\rangle$ then $q_iCh^m(a)D \in q_iC_m$ is connected either to $q_jC^-h^m(a)D \in q_jC_{m-1}$ if $m > 0$ or to $q_kCaD \in q_kC_0$ if $m = 0$.

Now we can prove that every canonical word corresponding to an accepted configuration can be rewritten to $AaBq_0CaD$.

LEMMA 4.3. *If $w \in ACan$ then $w \to_R^* AaBq_0CaD$.*

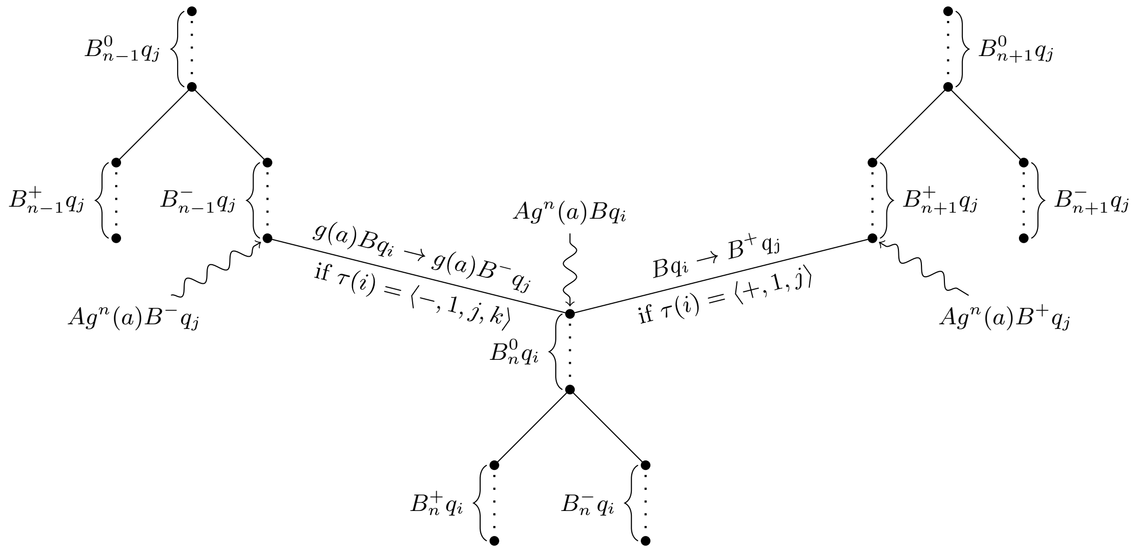

FIGURE 3. Connections between B_nq_i, $B_{n-1}q_j$ and $B_{n+1}q_j$ for $n > 0$. If $n = 1$ then $B_{n-1}q_j$ collapses into a four-element chain.

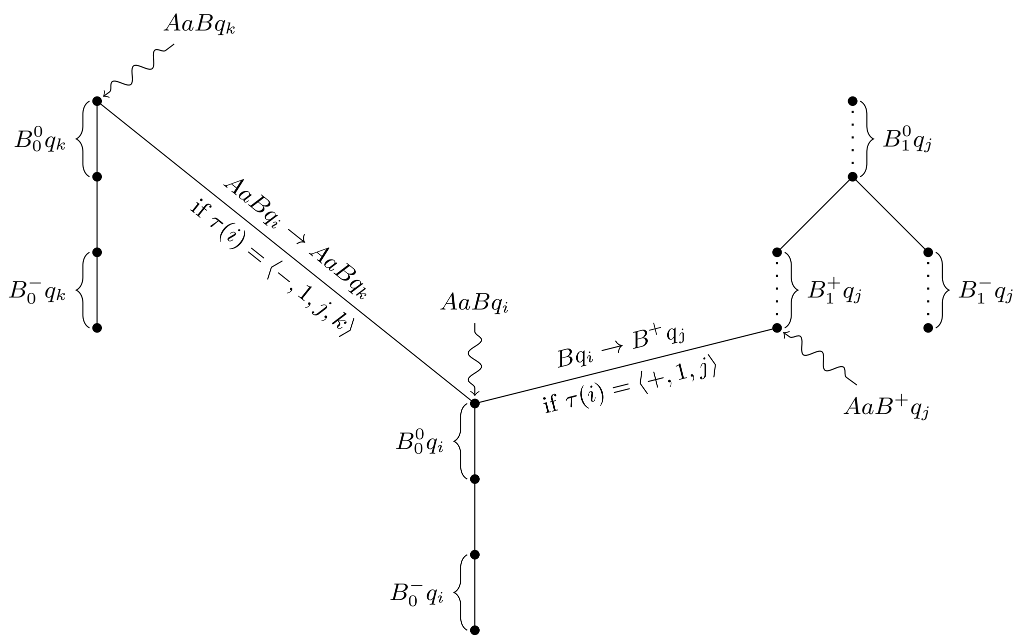

FIGURE 4. Connections between B_0q_i, B_0q_k and B_1q_j.

Proof. By definition of $ACan$, we have $w \in \phi(i, n, m)$ and $\langle i, n, m\rangle \in \mathrm{AConf}(\mathcal{M})$. Since $w \in \phi(i, n, m)$, we have $w = uq_iv$ for some $u \in B_n$ and $v \in C_m$. According to the structure of $\langle B_nq_i, \to^*_R\rangle$ and $\langle q_iC_m, \to^*_R\rangle$ (see Figures 1 and 2), we have $uq_i \to^*_R Ag^n(a)Bq_i$ and $q_iv \to^*_R q_iCh^m(a)D$. Thus $w \to^*_R Ag^n(a)Bq_iCh^m(a)D$.

We will prove the lemma by induction on the length l of the computation. If $l = 0$ then $\langle i, n, m\rangle$ has to be $\langle 0, 0, 0\rangle$. Thus the base case follows because $\to_R^*$ is reflexive, i.e., we have

$$AaBq_0CaD \to_R^* AaBq_0CaD\,.$$

Suppose that $l > 0$, i.e., after l many steps of the computation $\langle i, n, m\rangle$ is transformed to $\langle 0, 0, 0\rangle$. Then $i > 0$ and we have six possible cases depending on $\tau(i)$:

- If $\tau(i) = \langle +, 1, j\rangle$ then $\langle j, n+1, m\rangle$ is accepted by a computation of length $l-1$. Thus $Ag^{n+1}(a)Bq_jCh^m(a)D \in ACan$ and by the induction hypotheses

  $$Ag^{n+1}(a)Bq_jCh^m(a)D \to_R^* AaBq_0CaD\,.$$

  Since $\tau(i) = \langle +, 1, j\rangle$, the rule (r_i^{+1}) is in R. Then we can construct the following reduction (see Figures 1, 3 and 4):

  $$Ag^n(a)Bq_iCh^m(a)D \xrightarrow{r_i^{+1}}_R Ag^n(a)B^+q_jCh^m(a)D \to_R^* Ag^{n+1}(a)Bq_jCh^m(a)D\,.$$

- If $\tau(i) = \langle -, 1, j, k\rangle$ and $n > 0$ then $\langle j, n-1, m\rangle$ is accepted by a computation of length $l-1$. Thus $Ag^{n-1}(a)Bq_jCh^m(a)D \in ACan$ and by the induction hypotheses

  $$Ag^{n-1}(a)Bq_jCh^m(a)D \to_R^* AaBq_0CaD\,.$$

  Since $\tau(i) = \langle -, 1, j, k\rangle$, the rules (r_i^{-1}) are in R. Since $n > 0$, we have $g^n(a) = wg(a)$ for some $w \in \Sigma_S^*$ Thus the rule $g(a)Bq_i \to g(a)B^-q_j$ can be applied to $Ag^n(a)Bq_iCh^m(a)D$. Then we can construct the following reduction (see Figures 1 and 3):

  $$Ag^n(a)Bq_iCh^m(a)D \xrightarrow{r_i^{-1}}_R Ag^n(a)B^-q_jCh^m(a)D \to_R^* Ag^{n-1}(a)Bq_jCh^m(a)D\,.$$

- If $\tau(i) = \langle -, 1, j, k\rangle$ and $n = 0$ then $\langle k, n, m\rangle$ is accepted by a computation of length $l-1$. Thus $AaBq_kCh^m(a)D \in ACan$ and by the induction hypotheses

  $$AaBq_kCh^m(a)D \to_R^* AaBq_0CaD\,.$$

  Since $\tau(i) = \langle -, 1, j, k\rangle$, the rules (r_i^{-1}) are in R. Then we can construct the following reduction (see Figure 4):

  $$AaBq_iCh^m(a)D \xrightarrow{r_i^{-1}}_R AaBq_kCh^m(a)D\,.$$

The proof for the instructions dealing with the second counter is analogous. □

Next we are going to show that the converse of Lemma 4.3 holds as well. We will show that $ACan$ is downward closed with respect to $\to_R^*$, i.e., $w \in ACan$ and $u \to_R^* w$ implies $u \in ACan$. This is sufficient for if $u \to_R^* AaBq_0CaD$ then $u \in ACan$ because $AaBq_0CaD \in ACan$.

LEMMA 4.4. *Let $w \in ACan$ and $w' \xrightarrow{r}_R w$ by a rule $r \in R$. Then $w' \in ACan$.*

Proof. By definition of $ACan$ we have $w \in \phi(j, n, m)$ for some $\langle j, n, m\rangle \in \mathrm{AConf}(\mathcal{M})$, i.e., $w = uq_jv$ for some $u \in B_n$ and $v \in C_m$. Depending on the rule r, we have several cases.

If r is a rule from (r_{aux}^1) then its inverse can be applied only to uq_j producing again a word from B_nq_j (see Figure 1). Thus $w' \in \phi(j, n, m)$ as well and so $w' \in ACan$. Analogously, if r is from (r_{aux}^2) then its inverse is applicable only to q_jv producing again a word from q_jC_m. Thus $w' \in \phi(j, n, m)$ also in this case and so $w' \in ACan$.

If r is $Bq_i \to B^+q_j$ for some $i \in [1, M]$ then $n > 0$, $w = Ag^{n-1}(a)B^+q_jCh^m(a)D$ and $w' = Ag^{n-1}(a)Bq_iCh^m(a)D$ (see Figures 3 and 4). Thus $w' \in \phi(i, n-1, m)$. Since r is in R, we have $\tau(i) = \langle +, 1, j\rangle$. Consequently, $\langle i, n-1, m\rangle \in \mathrm{AConf}(\mathcal{M})$ and so $w' \in ACan$.

If r is $g(a)Bq_i \to g(a)B^-q_j$ for some $i \in [1, M]$ then $w = Ag^{n+1}(a)B^-q_jCh^m(a)D$ and $w' = Ag^{n+1}(a)Bq_iCh^m(a)D$ (see Figure 3). Thus $w' \in \phi(i, n+1, m)$. Since r is in R, we have $\tau(i) = \langle -, 1, j, k\rangle$ for some $k \in [0, M]$. Consequently, $\langle i, n+1, m\rangle \in \mathrm{AConf}(\mathcal{M})$ and so $w' \in ACan$.

If r is $AaBq_i \to AaBq_j$ for some $i \in [1, M]$ then $n = 0$ and $w = AaBq_jCh^m(a)D$ and $w' = AaBq_iCh^m(a)D$ (see Figure 4). Thus $w' \in \phi(i, 0, m)$. Since r is in R, we have $\tau(i) = \langle -, 1, k, j\rangle$ for some $k \in [0, M]$. Consequently, $\langle i, 0, m\rangle \in \mathrm{AConf}(\mathcal{M})$ and so $w' \in ACan$.

The proof for the rules (r_i^{+2}) and (r_i^{-2}) is analogous. $\square$

From Lemma 4.4 we obtain immediately the following lemma.

LEMMA 4.5. *Let $w \in \Sigma^*$. If $w \to_R^* AaBq_0CaD$ then $w \in ACan$.*

In what follows we will denote the word $AaBq_0CaD \in \Sigma^*$ shortly by w_0. Using Lemmas 4.3 and 4.5, it follows that

$$ACan = \{u \in \Sigma^* \mid u \to_R^* w_0\}\,.$$

Moreover, the set $ACan$ is undecidable. Indeed, if it would be decidable then we would have an algorithm how to decide whether $\langle i, n, m\rangle \in \mathrm{AConf}(\mathcal{M})$ just by deciding whether

$$Ag^n(a)Bq_iCh^m(a)D \to_R^* w_0$$

holds or not.

5. Main results

Consider the semi-Thue system $\langle \Sigma, R\rangle$ simulating the machine $\mathcal{M}$ with undecidable set $\mathrm{AConf}(\mathcal{M})$ constructed in the previous section. In this section we are going to use $\langle \Sigma, R\rangle$ in order to show that most of all varieties $\mathcal{RL}_m^n$ and $\mathcal{RL}_m^n \cap \mathcal{RL}_m^n$ have undecidable word problem. For this purpose consider the finite presentation $\langle \Sigma, E\rangle$ for the language of residuated lattices where

$$E = \{x \vee y = y \mid x \to y \in R\}\,.$$

Let $z \in ACan$. Then $z \to_R^* w_0$ and the quasi-inequality

$$\mathop{\&}_{x \to y \in R} x \leq y \implies z \leq w_0$$

holds in every pomonoid by Lemma 3.1. Since residuated lattices are special pomonoids, the following quasi-identity holds in every residuated lattice:

$$\&E \implies z \vee w_0 = w_0\,. \tag{6}$$

Conversely, given $z \in \Sigma^*$ such that $z \notin ACan$, we will construct a residuated lattice where (6) does not hold. Define the following binary relation $N \subseteq \Sigma^* \times (\Sigma^* \times \Sigma^*)$:

$$x\ N\ \langle u, v\rangle \quad \text{iff} \quad uxv \in ACan \text{ (i.e., } uxv \to_R^* w_0)\,.$$

Then N is nuclear since for all $x, y, u, v \in \Sigma^*$ we have

$$xy\ N\ \langle u, v\rangle \quad \text{iff} \quad y\ N\ \langle ux, v\rangle \quad \text{iff} \quad x\ N\ \langle u, yv\rangle \quad \text{iff} \quad uxyv \in ACan\,.$$

Consequently, $\mathbf{W} = \langle \Sigma^*, \Sigma^* \times \Sigma^*, N\rangle$ forms a residuated frame and the complex algebra

$$\mathbf{W}^+ = \langle W^+, \cap, \cup, \cdot_{\gamma_N}, \backslash, /, \gamma_N\{\varepsilon\}\rangle\,,$$

where $W^+ = \mathcal{P}(\Sigma^*)_{\gamma_N}$, is a residuated lattice. Consider the set of residuated-lattice terms $T(\Sigma)$ and the homomorphism $\varphi\colon T(\Sigma) \to W^+$ defined by $\varphi(a) = \gamma_N\{a\}$ for every $a \in \Sigma$. Note that we have $\varphi(x) = \gamma_N\{x\}$ for every word $x \in \Sigma^*$ by Lemma 2.5.

Assume that $x \to y \in R$. Then $\{y\}^\rhd \subseteq \{x\}^\rhd$. Indeed, let $\langle u, v\rangle \in \{y\}^\rhd$. Then $uyv \in ACan$, i.e., $uyv \to_R^* w_0$. Moreover $uxv \to_R uyv$ since $x \to y \in R$. Thus $uxv \to_R^* w_0$ which means that $\langle u, v\rangle \in \{x\}^\rhd$. Consequently, by Lemma 2.3 we have

$$\gamma_N\{x\} = \{x\}^{\rhd\lhd} \subseteq \{y\}^{\rhd\lhd} = \gamma_N\{y\}\,.$$

Thus every identity in E is satisfied by φ. On the other hand, $\gamma_N\{z\} \not\subseteq \gamma_N\{w_0\}$. Indeed, first we have $z \in \gamma_N\{z\}$ since γ_N is a closure operator. Further, note that $\langle \varepsilon, \varepsilon\rangle \in \{w_0\}^\rhd$ because $w_0 \to_R^* w_0$. By Lemma 2.3 we have $\gamma_N\{w_0\} \subseteq \{\langle\varepsilon,\varepsilon\rangle\}^\lhd$. Since

$$\{\langle\varepsilon,\varepsilon\rangle\}^\lhd = \{w \in \Sigma^* \mid \varepsilon w \varepsilon \in ACan\} = ACan\,,$$

we obtain $z \notin \gamma_N\{w_0\}$.

Since the set $ACan$ is undecidable, we obtain the following theorem.

THEOREM 5.1. *Any variety $\mathcal{V}$ of residuated lattices containing $\mathbf{W}^+$ has undecidable word problem.*

Proof. If the word problem for $\mathcal{V}$ would be decidable, we would have an algorithm deciding whether (6) holds in $\mathcal{V}$ or not. Then we could decide whether $z \in ACan$. Indeed, if (6) holds in $\mathcal{V}$ then $z \in ACan$ otherwise (6) would not hold in $\mathbf{W}^+ \in \mathcal{V}$. Conversely, if (6) does not hold in $\mathcal{V}$ then $z \notin ACan$ otherwise (6) would hold in $\mathcal{RL} \supseteq \mathcal{V}$. Thus we have reached a contradiction. □

Now it suffices to realize for which $m, n \in \mathbb{N}$ we have $\mathbf{W}^+ \in \mathcal{RL}^n_m$. Let $k \in \mathbb{N}$ and $X \in W^+$, hence $X = \gamma_N(X)$. Then X^k denotes the k-fold multiplication in the powerset monoid $\mathcal{P}(\Sigma^*)$, i.e.,

$$X^k = \{x_1 \dots x_k \in \Sigma^* \mid x_1, \dots, x_k \in X\}\,.$$

For the k-fold multiplication in $\mathbf{W}^+$ we have the following

$$\underbrace{X \cdot_{\gamma_N} \dots \cdot_{\gamma_N} X}_{k-\text{times}} = \underbrace{\gamma_N(X) \cdot_{\gamma_N} \dots \cdot_{\gamma_N} \gamma_N(X)}_{k-\text{times}} = \gamma_N(X^k)\,,$$

because γ_N is a monoid homomorphism. Thus we are interested in natural numbers $m, n \in \mathbb{N}$, $m \neq n$, such that $\gamma_N(X^m) \subseteq \gamma_N(X^n)$.

THEOREM 5.2. *The word problem is undecidable for the following varieties of residuated lattices:*

(1) $\mathcal{RL}^n_m$ *for* $1 \le m < n$,
(2) $\mathcal{RL}^n_m$ *for* $2 \le n < m$,
(3) $\mathcal{RL}^n_m \cap \mathcal{RL}^m_n$ *for* $m \neq n$ *and* $2 \le m, n$.

Proof. Let $X \in W^+$. If $X = \emptyset$ then $\emptyset$ is γ_N-closed, i.e., $\gamma_N(\emptyset) = \emptyset$. Then $\gamma_N(X^k) = \gamma_N(\emptyset) = \emptyset$ for all $k \in \mathbb{N}$. If $X \neq \emptyset$ then there is $x \in X$ and $xx \in X^2$. Consequently, $(X^2)^\rhd = \emptyset$ because there is no $\langle u, v\rangle \in \Sigma^* \times \Sigma^*$ such that $uxxv \in ACan$ as $ACan$ contains only square-free words (see Lemma 4.2). Thus $\gamma_N(X^2) = \Sigma^*$ by Lemma 2.3. Therefore $\gamma_N(X) \subseteq \gamma_N(X^2)$ and $\gamma_N(X^3) \subseteq \gamma_N(X^2)$, i.e., $\mathbf{W}^+ \in \mathcal{RL}^2_1 \cap \mathcal{RL}^2_3$. Since $\mathcal{RL}^2_1 \subseteq \mathcal{RL}^n_m$ for $1 \le m < n$, the first claim follows. Similarly, the second claim holds as $\mathcal{RL}^2_3 \subseteq \mathcal{RL}^n_m$ for $2 \le n < m$. Consequently, the last claim also holds. □

Observe that the quasi-identity (6) does not use the full language of residuated lattices but uses only $\cdot$ and $\vee$. Thus we can reformulate Theorem 5.1 as follows. Recall that an idempotent semiring $\mathbf{A} = \langle A, \vee, \cdot, 1\rangle$ is an algebra such that $\langle A, \vee\rangle$ is a semilattice, $\langle A, \cdot, 1\rangle$ is a monoid and for all $a, b, c \in A$ we have $c(a \vee b) = ca \vee cb$ and $(a \vee b)c = ac \vee bc$. Note that any idempotent semiring forms a pomonoid with respect to the semilattice order.

THEOREM 5.3. *Any variety $\mathcal{V}$ of idempotent semirings containing the $\{\vee, \cdot, 1\}$-reduct of $\mathbf{W}^+$ has undecidable word problem.*

A residuated idempotent semiring is an algebra $\mathbf{A} = \langle A, \vee, \cdot, \backslash, /, 1\rangle$ such that $\langle A, \vee, \cdot, 1\rangle$ is an idempotent semiring and (1) holds for all $a, b, c \in A$. A particular application of Theorems 5.3 and 5.2 is the following corollary.

COROLLARY 5.4. *The variety $\mathcal{V}_n$ of residuated idempotent semirings satisfying $x^n = x^{n+1}$ for $n \geq 2$ has undecidable word problem.*

This result is closely related to the question posed in [2, Problem 4.5] asking whether the variety of residuated join-semilattice-ordered semigroups (i.e., residuated idempotent semirings without multiplicative unit) satisfying $x^n = x^{n+1}$ for $n \geq 2$ has the finite embeddability property (FEP). Here we prove that $\mathcal{V}_n$ for $n \geq 2$ cannot have the FEP. Indeed, if $\mathcal{V}_n$ would have the FEP then its universal theory would be decidable (see [2]) which is in contradiction with Corollary 5.4. Although we do not answer precisely [2, Problem 4.5], our method used in this paper can be easily modified so that it would give a negative answer to [2, Problem 4.5]. This is possible because we use the monoid unit 1 solely in virtue of $\mathbf{W}^+$ being a residuated lattice and not only a residuated lattice-ordered semigroup.

Finally, we restrict our attention to distributive residuated lattices. Let $\mathcal{DRL}$ be the variety of distributive residuated lattices, i.e., residuated lattices whose lattice reduct is distributive. Recall that a subset S of a poset $\mathbf{P} = \langle P, \leq\rangle$ is called downset if $x \leq y$ and $y \in S$ implies $x \in S$. The collection of all downsets is denoted $\mathcal{O}(\mathbf{P})$. Let $x \in P$. The downset generated by $\{x\}$ is denoted $\downarrow\{x\}$.

THEOREM 5.5. *The word problem is undecidable in $\mathcal{DRL} \cap \mathcal{RL}_m^n$ for $1 \leq m < n$.*

Proof. First, observe that one can use meets instead of joins in (6) obtaining an equivalent quasi-identity, namely

$$\& E' \implies z = z \wedge w_0\,, \tag{7}$$

where $E' = \{x = x \wedge y \mid x \to y \in R\}$.

Having the residuated lattice $\mathbf{W}^+$ belonging to $\mathcal{RL}_1^2$ by Theorem 5.2, consider the collection of all downsets $\mathcal{O}(\mathbf{W}^+)$ which forms a distributive residuated lattice belonging to $\mathcal{RL}_1^2$ as well (see [9, Section 3.8]). Moreover, the map $x \mapsto \downarrow\{x\}$ is a one-to-one map preserving all operations except of $\vee$ (see [9, Section 3.8]). Thus if (7) does not hold in $\mathbf{W}^+$ then it does not hold also in $\mathcal{O}(\mathbf{W}^+) \in \mathcal{DRL} \cap \mathcal{RL}_1^2$. □

6. Conclusion

We proved that the varieties $\mathcal{RL}_m^n$ have undecidable word problem for almost all $m, n \in \mathbb{N}$ such that $m \neq n$. Now we will discuss the remaining cases which are not covered by Theorem 5.2.

(1) If $m = 0$ then all varieties $\mathcal{RL}_m^n$ are trivial since $1 \leq x^n$ holds only in the trivial residuated lattice.

(2) If $n = 0$ then all varieties $\mathcal{RL}_m^n$ have decidable universal theory since $x^m \leq 1$ implies $x \leq 1$. Consequently, $\mathcal{RL}_m^0 = \mathcal{RL}_1^0$ which is the variety of integral residuated lattices whose universal theory is known to be decidable (see [2, 7]).

(3) The only remaining cases are the varieties $\mathcal{RL}_m^1$ for $m > 1$. It turns out that the decidability of the word problem for these varieties is closely related to the bounded Burnside problem for groups and we will deal with these cases in a subsequent paper.

Acknowledgment

The work of the author was partly supported by the grant P202/11/1632 of the Czech Science Foundation and partly by the long-term strategic development financing of the Institute of Computer Science (RVO:67985807).

References

[1] Willem J. Blok and Clint J. van Alten. The finite embeddability property for residuated lattices, pocrims and BCK-algebras. *Algebra Universalis*, 48(3):253–271, 2002.

[2] Willem J. Blok and Clint J. van Alten. On the finite embeddability property for residuated ordered groupoids. *Transactions of the American Mathematical Society*, 357(10):4141–4157, 2005.

[3] Ronald V. Book and Friedrich Otto. *String-rewriting Systems*. Springer-Verlag, New York, 1993.

[4] Aldo de Luca and Stefano Varricchio. *Finiteness and Regularity in Semigroups and Formal Languages*. Springer-Verlag, 1999.

[5] Nachum Dershowitz. Semigroups satisfying $x^{m+n} = x^n$. In Michaël Rusinowitch and Jean-Luc Rémy, editors, *Conditional Term Rewriting Systems*, volume 656 of *Lecture Notes in Computer Science*, pages 307–314. Springer Berlin Heidelberg, 1993.

[6] Trevor Evans. Some connections between residual finiteness, finite embeddability and the word problem. *J. London Math. Soc. 1*, 1:399–403, 1969.

[7] Nikolaos Galatos and Peter Jipsen. Residuated frames with applications to decidability. *Transactions of the American Mathematical Society*, 365(3):1219–1249, 2013.

[8] Nikolaos Galatos, Peter Jipsen, Tomasz Kowalski, and Hiroakira Ono. *Residuated Lattices: An Algebraic Glimpse at Substructural Logics*, volume 151 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, Amsterdam, 2007.

[9] Rostislav Horčík. Algebraic semantics: Semilinear FL-algebras. In Petr Cintula, Petr Hájek, and Carles Noguera, editors, *Handbook of Mathematical Fuzzy Logic - Volume 1*, volume 37 of *Studies in Logic, Mathematical Logic and Foundations*. 283–353, London, 2011.

[10] Ryuichi Hori, Hiroakira Ono, and Harold Schellinx. Extending intuitionistic linear logic with knotted structural rules. *Notre Dame Journal of Formal Logic*, 35(2):219–242, 1994.

[11] Peter Jipsen and Constantine Tsinakis. A survey of residuated lattices. In J. Martinez, editor, *Ordered Algebraic Structures*, pages 19–56. Kluwer Academic Publishers, Dordrecht, 2002.

[12] O. Kharlampovich and M. Sapir. Algorithmic problems in varieties, a survey. *International Journal of Algebra and Computation*, 12:379–602, 1995.

[13] Yves Lafont. The undecidability of second order linear logic without exponentials. *Journal of Symbolic Logic*, 61(2):541–548, 1996.

[14] Joachim Lambek. How to program an infinite abacus. *Canadian Math. Bulletin*, 4:295–302, 1961.

[15] M. Lothaire. *Algebraic Combinatorics on Words*. Cambridge University Press, Cambridge, 2002.

[16] M. Minsky. Recursive unsolvability of post's problem of 'tag' and other topics in the theory of turing machines. *Annals of Mathematics*, 74:437–455, 1961.

[17] Antonio Restivo and Christophe Reutenauer. Rational languages and the burnside problem. *Theoretical Computer Science*, 40:13–30, 1985.

[18] Clint J. van Alten. The finite model property for knotted extensions of propositional linear logic. *Journal of Symbolic Logic*, 70(1):84–98, 2005.

Institute of Computer Science, Czech Academy of Sciences of the Czech Republic, Pod Vodárenskou věží 2, 182 07 Prague 8, Czech Republic. Email: horcik@cs.cas.cz