



Decision problems for semi-Thue systems with a few rules[☆]

Yuri Matiyasevich^a, Géraud Sénizergues^{b,*}

^a*Steklov Institute of Mathematics at St. Petersburg, 27 Fontanka, 191023 St. Petersburg, Russia*

^b*LaBRI and Université de Bordeaux I 351, Cours de la Libération 33405 Talence, France*

Abstract

We show that the accessibility problem, the common descendant problem, the termination problem and the uniform termination problem are undecidable for 3-rules semi-Thue systems. As a corollary we obtain the undecidability of the Post correspondence problem for 7 rules.

© 2004 Elsevier B.V. All rights reserved.

Keywords: Decidability; Bounds; Semi-Thue system; Accessibility; Post correspondence problem; Termination

1. Introduction

The very first undecidable problem found in mathematics proper (i.e., not in logic or computability theory) was the so-called *word problem for finitely presented semi-groups*. This problem is also known as *Thue problem* after Axel Thue who posed it in [36] in 1914, i.e. long before the development of a general notion of algorithm and Church Thesis.

[☆] This work began while both authors were at LaBRI (Bordeaux), with financial support of the CNRS; it ended while both authors were at FMI (Stuttgart), both of them being supported by the Humboldt-foundation.

* Corresponding author. Institut für Formale Methoden der Informatik, Universitätsstraße 38, D-70569, Stuttgart, Germany. Tel.: +49 711 7816 257; fax: +49 711 7816 310.

E-mail addresses: yumat@pdm.ras.ru (Y. Matiyasevich), ges@labri.fr, ges@labri.u-bordeaux.fr (G. Sénizergues)

URLs: <http://logic.pdm.ras.ru/~yumat>, <http://dept-info.labri.u-bordeaux.fr/~ges>.

Informally, this problem can be described as follows. We are given a finite alphabet A and a finite set T of *defining relations*

$$\begin{array}{c} u_1 \longleftrightarrow v_1, \\ \vdots \\ u_n \longleftrightarrow v_n, \end{array} \quad (1)$$

where the u 's and v 's are words from A^* . Two words, f and g , from A^* are considered to be equivalent modulo T if one of these words can be obtained from the other word via finitely many replacements of u_i by v_i or vice versa. Thue asked for a method to decide, given T , f and g , whether the two latter words are equivalent modulo T .

In 1947 Andrei Markov [23,24] and Emil Post [32] proved (independently) that no such method is possible. Moreover, we can fix T and f , and still have undecidability. A lot of efforts was spent by many researchers in attempts to construct a “simple” T with undecidable word problem (for surveys of such results see, for example, [27,28]).

One of the measures of “simplicity” is n , the number of defining relations. In 1970 the first author ([25], for detailed proofs see [7,28]) constructed a particular system with only 3 defining relations for which the word problem is undecidable. This result remains the best (in the number of relations) till now. On the other hand, it is rather striking that no algorithm was found for the case of a single defining relation (for partial progress in this direction see, for example, [1,22]).

In the present paper we shall deal with similar problems but with more flavor of computer science than that of algebra. Namely, instead of defining relations (1) we shall deal with a system S of *rewriting rules*

$$\begin{array}{c} u_1 \longrightarrow v_1, \\ \vdots \\ u_n \longrightarrow v_n. \end{array} \quad (2)$$

Such collections of rules are called *semi-Thue systems* in contrast to Thue-systems which are collections of bi-directional rules (1). A word g is called a *descendant* of a word f modulo S as soon as the word g can be obtained from the word f via finitely many replacements of u_i by v_i .

A straightforward counterpart of Thue problem for semi-Thue systems is the *accessibility problem*: given S , f and g , to decide whether g is a descendant of f modulo S .

Another problem, named *common descendant problem*, can be also viewed as a counterpart of Thue problem for semi-Thue systems: given S , f and g , to decide whether there exists a word h which is a descendant of both f and g .

If we put more attention to the process of transformation of words rather than to its result (which is typical to computer science but has no counterpart in, say, algebra), then we can consider infinite *derivations* modulo a given semi-Thue system. Thus we come to the classical *termination problem*: given S and f , to decide whether there is an infinite derivation from f modulo S . If we do not specify a word f , we get the *uniform termination problem*.

The accessibility problem for semi-Thue systems is undecidable. This follows from the above-mentioned result of Markov–Post because the word problem for a Thue system T is equivalent to the accessibility problem for the semi-Thue system T_{sym} resulting from the system T by replacing each defining relation $u \longleftrightarrow v$ by two rewriting rules $u \longrightarrow v$ and $v \longrightarrow u$; in fact the direct proof of the undecidability of the accessibility problem for semi-Thue systems is much simpler than the proof of undecidability of the original Thue problem, the main obstacle which Markov and Post had to overcome was the bi-directional character of the rules in Thue systems.

For a “symmetric” semi-Thue system T_{sym} , the common descendant problem is equivalent to the accessibility problem (and to the word problem for Thue system T) and hence the common descendant problem is also undecidable.

The undecidability of the termination problem can be deduced easily from the undecidability of the “*halting-problem*” for some fixed Turing machine [9, p. 70, Theorem 2.2] via a general translation of Turing machines into semi-Thue systems [9, p. 88–93, Section 2]. The undecidability of the uniform termination problem for finite semi-Thue systems is a somewhat more subtle result; it is closely linked with the problem to determine whether a given Turing machine is terminating on *every* starting configuration; this last problem has been proved undecidable in [17] and the corollary that the Uniform Terminating Problem is undecidable is derived in [17, p. 227, point (8)].

The main results of the present paper are constructions of particular semi-Thue systems, each with 3 rules only, for which the accessibility problem, common descendant problem, and termination problem are undecidable; for the uniform termination problem we show that it remains undecidable even if we restrict ourselves to semi-Thue systems with 3 rules only.

The first of the above-mentioned 3-rules semi-Thue system can be transformed, by the technique from [6], into an undecidable Post Correspondence Problem (PCP) with only 7 pairs of words.

The construction of undecidable 3-rules semi-Thue systems exploits the main idea from the first author construction of an undecidable Thue-system with 3 defining relations cited above. However, this was not enough, and the present paper is not a mere translation of the technique known for Thue systems to the case of semi-Thue systems. Quite a new idea of a hierarchy of letters and their transformations is introduced here in order to keep the number of rules as small as in the case of Thue systems, and this new technique might find applications in other cases.

The results of this paper were announced in [29] but detailed proofs are published here for the first time. The new bound on undecidability of PCP was used by [2,4,5].

2. Preliminaries

2.1. Vocabulary, notation

2.1.1. Words

By ε we denote, as usual, the *empty word*. If a word g is a *suffix* of a word f , i.e. $f = hg$ for some word h , then we shall use the notation fg^{-1} for this word h .

2.1.2. Semi-Thue systems

Formally, a *semi-Thue* system over an alphabet A is a subset of $A^* \times A^*$; usually a system $S = \{\langle u_1, v_1 \rangle, \dots, \langle u_n, v_n \rangle\}$ will be exhibited as (2). By \longrightarrow_S we denote the binary relation among words from A^* such that

$$f \longrightarrow_S g \iff \exists u, v, p, q \in A^*, (\langle u, v \rangle \in S \text{ \& } f = puq \text{ \& } g = pvq). \quad (3)$$

The relation \longrightarrow_S is called the *one-step* rewriting relation generated by S .

A *derivation* modulo S is a sequence $D = (w_i, p_i, u_i, v_i)_{i \in I}$, where I is a non-empty beginning section of \mathbb{N} (i.e. $I = [0, k]$ for some $k \in \mathbb{N}$ or $I = \mathbb{N}$), w_i is a word from A^* , $\langle u_i, v_i \rangle$ is a rule from S , provided that for every positive i from I there exist a word q_{i-1} such that $w_i = p_{i-1}v_{i-1}q_{i-1}$ and $w_{i-1} = p_{i-1}u_{i-1}q_{i-1}$. In order to abbreviate the notation we often (incorrectly) drop the data p_i, u_i, v_i in the definition of a derivation D .

The *length* of D is k (if $I = [0, k]$) or ∞ (if $I = \mathbb{N}$).

By $f \xrightarrow{*}_S g$, $f \xrightarrow{+}_S g$, $f \xrightarrow{k}_S g$ (where $k \in \mathbb{N}$) we denote, respectively, the mere existence of a derivation of the form $f = w_0, \dots, w_k = g$, the existence of such a derivation of some positive length or of length exactly k (see [18]); by $f \xrightarrow{\infty}_S$ we denote the existence of an infinite derivation starting from f .

The set of descendants of f modulo S , denoted by $\Delta_S^*(f)$, is defined by:

$$\Delta_S^*(f) = \{g \in A^*, f \xrightarrow{*}_S g\}.$$

A derivation D is said to be an *rl-derivation* (rl stands for right-to-left) iff, $\forall i \in I - \{0\}$, $|p_i| < |p_{i-1}v_{i-1}|$.

We remind the reader that a semi-Thue system $S \subseteq A^* \times A^*$ is said *confluent* iff

$$\forall u, v, w \in A^*, (u \xrightarrow{*}_S v \& u \xrightarrow{*}_S w) \Rightarrow (\exists u' \in A^*, v \xrightarrow{*}_S u' \& w \xrightarrow{*}_S u').$$

It is easy to see that when S is confluent and there is no infinite derivation modulo S , then every word w has a unique *normal form*, denoted by $\rho_S(w)$, such that $w \xrightarrow{*}_S \rho_S(w)$ and no rule from S is applicable to $\rho_S(w)$. We shall use this property for defining different maps.

2.1.3. Algorithmic problems

The following algorithmic problems on semi-Thue systems are classical:

The individual accessibility problem (IAP) for the alphabet A , the semi-Thue system $S \subseteq A^* \times A^*$ and the word $w_0 \in A^*$:

instance : one word $w \in A^*$

question : $w \xrightarrow{*}_S w_0$?

The accessibility problem (ACP) for the alphabet A and the semi-Thue system $S \subseteq A^* \times A^*$:

instance : two words $w_1, w_2 \in A^*$

question : $w_1 \xrightarrow{*}_S w_2$?

The common descendant problem (CDP) for the alphabet A and the semi-Thue system $S \subseteq A^* \times A^*$:

instance : two words $w_1, w_2 \in A^*$

question : is there a word $w \in A^*$ such that $w_1 \xrightarrow{*}_S w$ and $w_2 \xrightarrow{*}_S w$?

The *termination problem (TP)* for the alphabet A and the semi-Thue system $S \subseteq A^* \times A^*$:

instance : $w \in A^*$

question : does every derivation modulo S starting on w have finite length?

(when the answer is “yes”, we say that S *terminates* on w).

The *uniform termination problem (UTP)* for a class \mathcal{S} of semi-Thue systems:

instance : an alphabet A and a finite semi-Thue system $S \subseteq A^* \times A^*$ which belongs to \mathcal{S}

question : does every derivation modulo S starting from a word in A^* have finite length?

(when the answer is “yes” we say that S is *uniformly-terminating*, sometimes abbreviated as u-terminating).

For more information the reader can refer to [3,19] (about semi-Thue systems) or [10,11] (about termination problems).

2.2. Some useful results

The following reduction of the IAP to the PCP will be useful.

Theorem 2.1 (Claus [6]). *The individual accessibility problem for a semi-Thue system with n rules reduces to a Post correspondence problem for $n + 4$ pairs of words.*

The following lemma will ease the extraction of a “regular” infinite derivation from a general infinite derivation, in Section 3.2.4.

Lemma 2.1 (Sénizergues [33]). *Let S be a finite subset of $A^+ \times A^*$ and let $D = (w_i, p_i, u_i, v_i)_{i \in \mathbb{N}}$ be a derivation modulo S . Then, there exists some injection $\sigma : \mathbb{N} \rightarrow \mathbb{N}$ and some sequence $(w'_i, p'_i)_{i \in \mathbb{N}}$ such that, $w'_0 = w_0$ and $(w'_i, p'_i, u_{\sigma(i)}, v_{\sigma(i)})_{i \in \mathbb{N}}$ is a rl-derivation modulo S .*

3. Constructions

All constructions of 3-rule semi-Thue systems in this paper are done according to the following scheme. We start with some semi-Thue system S_0 over a finite alphabet A_0 and then construct

- a sequence of alphabets A_i and semi-Thue systems S_i over A_i (for $1 \leq i \leq 5$),
 - maps $\tau_i : A_i^* \rightarrow A_{i+1}^*$, (for $0 \leq i \leq 4$),
 - partial maps $\phi_i : A_{i+1}^* \rightarrow A_i^*$ (for $0 \leq i \leq 4$) and $\phi_5 : A_5^* \rightarrow A_5^*$,
- such that for $i = 0, \dots, 4$ the map ϕ_i is a left-inverse of τ_i in the sense that

$$\forall w \in A_i^*, \phi_i(\tau_i(w)) = w.$$

Every τ_i is then an *encoding* (i.e. an injective map) while ϕ_i will be called a *decoding*.

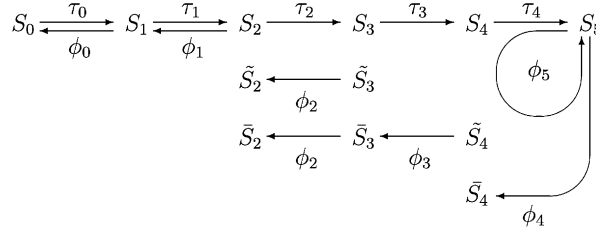


Fig. 1. Systems, codings and decodings.

In proofs of Theorems 4.1–4.3 we just start from different semi-Thue systems S_0 . The required relationship between S_0 and S_5 is established in subsection 3.2. In an ideal world it should take only the two following general forms:

- for every words w, w' in A_i^* ,

$$w \rightarrow_{S_i} w' \Rightarrow \tau_i(w) \xrightarrow{*}_{S_{i+1}} \tau_i(w')$$

- for every words w, w' in A_{i+1}^* (and fulfilling some suitable condition)

$$w \rightarrow_{S_{i+1}} w' \Rightarrow \phi_i(w) \xrightarrow{*}_{S_i} \phi_i(w'). \quad (4)$$

For technical reasons we are to introduce auxiliary systems \tilde{S}_i and \bar{S}_i ($i = 2, 3, 4$) which slightly extend the main systems S_i , and replace the latter systems by the former in (4) as summarized in Fig. 1.

3.1. Definitions

In this section we describe the construction of systems S_1 – S_5 .

3.1.1. System S_0

We start with an arbitrary semi-Thue system S_0 over some finite alphabet $A_0 = \{a_1, \dots, a_k\}$ and denote the rules of this system as follows:

$$\begin{aligned} \overline{u_1} &\longrightarrow \overline{v_1}, \\ &\vdots \\ \overline{u_{n_0}} &\longrightarrow \overline{v_{n_0}}. \end{aligned}$$

Let λ_0 (resp. μ_0) be the maximum length of the left-hand (resp. right-hand) sides of the rules of S_0 .

3.1.2. System S_1

We extend the alphabet A_0 by a new letter a_0 and define an auxiliary system T over the extended alphabet $B_0 = A_0 \cup \{a_0\}$ consisting of the rules

$$\begin{aligned} a_0^{\lambda_0} &\longrightarrow \varepsilon, \\ \overline{u_1}q &\longrightarrow \overline{v_1}q \quad \left(\text{for all } q \in B_0^{\lambda_0 - |\overline{u_1}|}\right), \\ &\vdots \\ \overline{u_{n_0}}q &\longrightarrow \overline{v_{n_0}}q \quad \left(\text{for all } q \in B_0^{\lambda_0 - |\overline{u_{n_0}}|}\right). \end{aligned} \quad (5)$$

Note that all rules have the same length of their left-hand sides equal to λ_0 .

Now let $A_1 = \{x, y\}$ and $\eta : B_0^* \rightarrow A_1^*$ be the monoid homomorphism defined by

$$\forall i \in [0, \kappa], \eta(a_i) = xxy^{i+1}xy^{\kappa+1-i}.$$

The map $\tau_0 : A_0^* \rightarrow A_1^*$ is then defined by

$$\forall w \in A_0^*, \tau_0(w) = \eta(wa_0^{\lambda_0}).$$

The system S_1 consists of the rules

$$\begin{aligned} \eta(a_0^{\lambda_0}) &\longrightarrow \varepsilon, \\ \eta(\overline{u_1}q) &\longrightarrow \eta(\overline{v_1}q) \quad \left(\text{for all } q \in B_0^{\lambda_0 - |\overline{u_1}|}\right), \\ &\vdots \\ \eta(\overline{u_{n_0}}q) &\longrightarrow \eta(\overline{v_{n_0}}q) \quad \left(\text{for all } q \in B_0^{\lambda_0 - |\overline{u_{n_0}}|}\right). \end{aligned} \quad (6)$$

The map $\phi_0 : A_1^* \rightarrow A_0^*$ is defined by means of the following two semi-Thue systems over $B_0 \cup A_1$:

$$\begin{aligned} T_0 : xxy^{i+1}xy^{\kappa+1-i} &\longrightarrow a_i \quad (\text{for } 0 \leq i \leq \kappa), \\ T'_0 : x &\longrightarrow \varepsilon, \\ y &\longrightarrow \varepsilon, \\ a_0 &\longrightarrow \varepsilon. \end{aligned} \quad (7)$$

One can easily check that both semi-Thue systems T_0 and T'_0 are u-terminating and confluent. For every w in A_1^* we set:

$$\phi_0(w) = \rho_{T'_0}(\rho_{T_0}(w)).$$

Finally, we introduce homogeneous notation—let rules (6) be written as

$$\begin{aligned} u_0 &\longrightarrow v_0, \\ &\vdots \\ u_n &\longrightarrow v_n \end{aligned}$$

with $n \geq 0$, $|u_0| = \dots = |u_n| = \lambda_1 = \lambda_0(\kappa + 5)$, and $|v_0| \leq \mu_1, \dots, |v_n| \leq \mu_1 = (\lambda_0 + \mu_0)(\kappa + 5)$.

3.1.3. System S_2

Let $A_2 = \{a, b\}$ and let $\delta : A_1^* \rightarrow A_2^*$ be the monoid homomorphism defined by

$$\delta(x) = b^2abaa; \quad \delta(y) = b^2aaba.$$

The map $\tau_1 : A_1^* \rightarrow A_2^*$ is then defined by

$$\forall w \in A_1^*, \tau_1(w) = \delta(w)b^2.$$

The system S_2 consists of the rules

$$\begin{aligned} \tau_1(u_0) &\longrightarrow \tau_1(v_0), \\ &\vdots \\ \tau_1(u_n) &\longrightarrow \tau_1(v_n). \end{aligned} \tag{8}$$

The system \tilde{S}_2 is the extension of S_2 by the additional rule

$$b \longrightarrow a \tag{9}$$

and the system \bar{S}_2 is further extension of \tilde{S}_2 by the rule

$$\varepsilon \longrightarrow a. \tag{10}$$

We denote by $S_a^{\varepsilon, b}$ the semi-Thue system consisting of the above two rules (9) and (10).

The map $\phi_1 : A_2^* \rightarrow A_1^*$ is defined by means of the following two semi-Thue systems T_1 and T_1' :

$$\begin{aligned} T_1 : \quad &b^2abaa \longrightarrow x, \\ &b^2aaba \longrightarrow y, \\ T_1' : \quad &a \longrightarrow \varepsilon, \\ &b \longrightarrow \varepsilon. \end{aligned} \tag{11}$$

One can easily check that both semi-Thue systems T_1 and T_1' are u-terminating and confluent. For every w in A_2^* we set

$$\phi_1(w) = \rho_{T_1'}(\rho_{T_1}(w)).$$

3.1.4. System S_3

Let $A_3 = \{a, b, c, d\}$. The map $\tau_2 : A_2^* \rightarrow A_3^*$ is then defined by $\tau_2(w) = w$, i.e., τ_2 is simply the natural embedding of A_2^* into A_3^* .

Let $\gamma : (A_2 \cup \{c\})^* \rightarrow A_3^*$ be the monoid homomorphism defined by

$$\forall x \in A_2 \cup \{c\}, \gamma(x) = cx.$$

The system S_3 consists of the rules

$$\begin{aligned} \tau_1(u_0) &\longrightarrow \gamma(\tau_1(v_0)c^{6(\mu_1 - |v_0|)}), \\ &\vdots \\ \tau_1(u_n) &\longrightarrow \gamma(\tau_1(v_n)c^{6(\mu_1 - |v_n|)}), \\ c &\longrightarrow \varepsilon. \end{aligned} \tag{12}$$

The system \tilde{S}_3 is the extension of S_3 by the additional rules:

$$a \longrightarrow d, \quad b \longrightarrow a \quad (13)$$

and the system \bar{S}_3 is further extension of \tilde{S}_3 by the additional rule

$$c \longrightarrow d. \quad (14)$$

Let us denote by $L_i \longrightarrow M_i$, $i = 0, \dots, n$, the “long” rules of the system S_3 . All the left-hand sides of these rules have the lengths equal to $\lambda = 6\lambda_1 + 2$, and all the right-hand sides have the lengths equal to $\mu = 12\mu_1 + 5$, and we introduce notation for the letters of the M ’s and L ’s. Namely, let $l_{i,j}$ denote the $(j + 1)$ th letter of L_i and $m_{i,k}$ denote the $(k + 1)$ th letter of M_i , i.e. for $i = 0, \dots, n$

$$L_i = l_{i,0} \dots l_{i,\lambda}, \quad (15)$$

$$M_i = m_{i,0} \dots m_{i,\mu}. \quad (16)$$

The map $\phi_2 : A_3^* \rightarrow A_2^*$ is the homomorphism from A_3^* onto A_2^* such that

$$\phi_2(a) = a, \quad \phi_2(b) = b, \quad \phi_2(c) = \varepsilon, \quad \phi_2(d) = a.$$

3.1.5. System S_4

Let $A_4 = \{a, b, c, d, \hat{a}, \hat{b}, \hat{c}, \check{c}\}$. Let us call *main* letters the elements of $\{\hat{a}, \hat{b}, \hat{c}\}$ and *nominal* letters the elements of $\{a, b, c, \check{c}\}$.

Let $\varphi : A_3^* \rightarrow A_4^*$ be the unique monoid homomorphism such that

$$\varphi(a) = \hat{a}b^n, \quad \varphi(b) = \hat{b}b^n, \quad \varphi(c) = \check{c}b^n, \quad \varphi(d) = db^n.$$

The map $\tau_3 : A_3^* \rightarrow A_4^*$ is then defined by

$$\forall w \in A_3^*, \tau_3(w) = \varphi(aw)c.$$

The system S_4 is defined as follows. Let

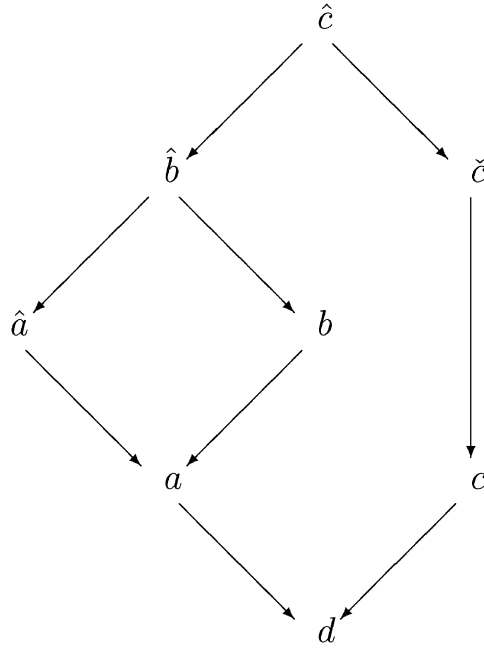
$$L = l_{0,0}l_{1,0} \dots l_{n,0} \dots l_{0,\lambda}l_{1,\lambda} \dots l_{n,\lambda}, \quad (17)$$

$$M = m_{0,0}m_{1,0} \dots m_{n,0} \dots m_{0,\mu}m_{1,\mu} \dots m_{n,\mu}. \quad (18)$$

The system S_4 consists of the rules

$$\begin{array}{lll} L \longrightarrow M, & & \\ \hat{b} \longrightarrow b, & \hat{a} \longrightarrow a, & \check{c} \longrightarrow c, \\ \hat{b} \longrightarrow \hat{a}, & a \longrightarrow d, & c \longrightarrow d, \\ b \longrightarrow a, & & \\ \hat{a}d^n cd^n a \longrightarrow \hat{a}b^n \hat{a}, & \hat{a}d^n cd^n b \longrightarrow \hat{a}b^n \hat{b}, & \hat{a}d^n cd^n c \longrightarrow \hat{a}b^n \check{c}, \\ \hat{b}d^n cd^n a \longrightarrow \hat{b}b^n \hat{a}, & \hat{b}d^n cd^n b \longrightarrow \hat{b}b^n \hat{b}, & \hat{b}d^n cd^n c \longrightarrow \hat{b}b^n \check{c}. \end{array} \quad (19)$$

Note that when the number n is fixed, all information about the original system S_0 is coded in the two words, L and M , and the other rules of the system S_4 do not depend on S_0 . This way of coding a (semi-)Thue system by two words was the main idea of the first author’s construction of an undecidable Thue-system with 3 rules.

Fig. 2. Lattice A_4 .

The system \tilde{S}_4 is the extension of S_4 by the additional rules:

$$\begin{aligned} \hat{c} &\longrightarrow \check{c}, \\ \hat{c}d^n cd^n a &\longrightarrow \hat{c}b^n \hat{a}, \quad \hat{c}d^n cd^n b \longrightarrow \hat{c}b^n \hat{b}, \quad \hat{c}d^n cd^n c \longrightarrow \hat{c}b^n \check{c} \end{aligned} \quad (20)$$

and the system \bar{S}_4 is further extension of \tilde{S}_4 by the rule

$$\hat{c} \longrightarrow \hat{b}. \quad (21)$$

Let us notice that the ordered set $(A_4, \xrightarrow{*}_{\bar{S}_4})$ is a lattice (see its Hasse diagram in Fig. 2, where the ordering $\xrightarrow{*}_{\bar{S}_4}$ goes from top to bottom). This hierarchy of letters is the second main idea which finally resulted in 3-rule semi-Thue systems.

Let $\pi : A_4^* \rightarrow A_3^*$ be the homomorphism defined by

$$\pi(a) = a, \pi(\hat{a}) = a, \pi(b) = b, \pi(\hat{b}) = b, \pi(c) = c, \pi(\check{c}) = c, \pi(\hat{c}) = c, \pi(d) = d.$$

We introduce two subsets $Q_n, R_n \subseteq A_4^*$ by

$$Q_n = \{w \in A_4^* \mid \forall i \in [1, |w|], w[i] \in \{\hat{a}, \hat{b}, \check{c}, \hat{c}\} \Rightarrow i \equiv 1 \pmod{n+1}\},$$

$$R_n = Q_n \cap \{w \in A_4^* \mid |w| \equiv 1 \pmod{n+1}\}.$$

The partial map $\phi_3 : A_4^* \rightarrow A_3^*$ is defined by

$$\text{Dom}(\phi_3) = R_n$$

and for every $w = z_1 z_2 \dots z_k$, where $z_i \in A_4$,

$$\phi_3(w) = \pi(z_{n+2})\pi(z_{2n+3}) \dots \pi(z_{j(n+1)+1})$$

for j such that $j(n+1) + 1 < k \leq (j+1)(n+1) + 1$.

3.1.6. System S_5

Let $A_5 = \{x, \bar{x}, y\}$. We shall use the abbreviation $u_1 = x\bar{x}$, $u_2 = x^2\bar{x}^2$.

Let $\psi : A_4^* \rightarrow A_5^*$ be the unique monoid homomorphism such that

$$\begin{aligned} \psi(\hat{b}) &= yu_2u_2u_2u_2, & \psi(b) &= yu_1u_1u_2u_2, \\ \psi(\hat{a}) &= yu_2u_2u_2, & \psi(a) &= yu_1u_1u_2, \\ \psi(\hat{c}) &= yu_2u_2u_2u_2u_1, & \psi(\check{c}) &= yu_2u_2u_1u_1u_1, & \psi(c) &= yu_1u_1u_1u_1u_1, \\ \psi(d) &= y. \end{aligned} \quad (22)$$

The map $\tau_4 : A_4^* \rightarrow A_5^*$ is then defined by

$$\forall w \in A_4^*, \tau_4(w) = \psi(w)y.$$

The system S_5 consists of the rules

$$\begin{aligned} \psi(L)y &\longrightarrow \psi(M)y, \\ u_2u_2u_2\psi(d^n c d^n)yu_1u_1 &\longrightarrow u_2u_2u_2\psi(b^n)yu_2u_2, \\ x\bar{x} &\longrightarrow \varepsilon. \end{aligned} \quad (23)$$

We denote by \mathcal{D} the semi-Thue system consisting of the single rule

$$x\bar{x} \longrightarrow \varepsilon.$$

The set of words $\{w \in \{x, \bar{x}\}^* \mid w \xrightarrow{*}_{\mathcal{D}} \varepsilon\}$ is denoted by D_1^* , it is known as the *Dyck-language*.

Let us denote by P_4 the set $\psi(A_4)$. One can check that $(P_4, \xrightarrow{*}_{\mathcal{D}})$ is a lattice too and that $\psi : A_4 \rightarrow P_4$ is a lattice-isomorphism. We define a map $\bar{\psi} : yD_1^* \rightarrow A_4^*$ by

$$\forall w \in yD_1^*, \bar{\psi}(w) = \psi^{-1} \left(\bigwedge_{P_4} (\mathcal{A}_{\mathcal{D}}^*(w) \cap P_4) \right) \quad (24)$$

(where the symbol \bigwedge_{P_4} denotes the g.l.b. in $(P_4, \xrightarrow{*}_{\mathcal{D}})$).

As yD_1^* is a suffix code which is the base of $(yD_1^*)^*$, $\bar{\psi}$ admits a unique extension as a morphism $(yD_1^*)^* \rightarrow A_4^*$ which is still denoted by $\bar{\psi}$. The partial map $\phi_4 : A_5^* \rightarrow A_4^*$ is then defined by

$$\begin{aligned} \text{Dom}(\phi_4) &= (yD_1^*)^*y, \\ \forall w \in (yD_1^*)^*y, \phi_4(w) &= \bar{\psi}(wy^{-1}). \end{aligned}$$

3.2. General properties

3.2.1. Encodings

Proposition 3.1. *For every $w, w' \in A_0^*$, if $w \xrightarrow{s_0} w'$ then $\tau_0(w) \xrightarrow{s_1} \tau_0(w')$.*

Proof. Straightforward. \square

Proposition 3.2. For every $w, w' \in A_1^*$, if $w \rightarrow_{S_1} w'$ then $\tau_1(w) \rightarrow_{S_2} \tau_1(w')$.

Proof. Straightforward. \square

Proposition 3.3. For every $w, w' \in A_2^*$, if $w \rightarrow_{S_2} w'$ then $\tau_3 \circ \tau_2(w) \xrightarrow{+}_{S_4} \tau_3 \circ \tau_2(w')$.

Proof. Let $w = puq$, $w' = pvq$ and $\langle u, v \rangle \in S_2$.

Then

$$\tau_3 \circ \tau_2(w) = \varphi(ap)\varphi(u)\varphi(q)c, \quad \tau_3 \circ \tau_2(w') = \varphi(ap)\varphi(v)\varphi(q)c.$$

The rule $\langle u, v \rangle$ must have the form: $u = \tau_1(u_i) = L_i$, $v = \tau_1(v_i) = M_i$ (where $0 \leq i \leq n$).

There should exist $z \in \{a, b\}$, $L'_i \in \{a, b\}^*$, $t \in \{\hat{a}, \hat{b}, c\}$, $r', r'' \in A_4^*$ such that

$$\varphi(ap) = r' \hat{z} b^n, L_i = L'_i b, \varphi(q)c = tr''. \quad (25)$$

Then

$$\tau_3 \circ \tau_2(w) = r' \hat{z} b^n \varphi(L'_i) \hat{b} b^{n-i} tr'' = r' \hat{z} b^{n-i} (b^i \varphi(L'_i) \hat{b} b^{n-i}) b^i tr''. \quad (26)$$

One can check that

$$b^i \varphi(L'_i) \hat{b} b^{n-i} \xrightarrow{*}_{S_4} L \quad (27)$$

because

- $|b^i \varphi(L'_i) \hat{b} b^{n-i}| = (\lambda + 1)(n + 1) = |L|$,
- the image by π of the letters at positions $\equiv i + 1 \pmod{n + 1}$ in $b^i \varphi(L'_i) \hat{b} b^{n-i}$ (resp. in L) is L_i ,
- every letter at position $j \not\equiv i + 1 \pmod{n + 1}$ in $b^i \varphi(L'_i) \hat{b} b^{n-i}$ (resp. in L) is equal to b (resp. belongs to $\{a, b\}$).

Hence

$$\begin{aligned} r' \hat{z} b^{n-i} (b^i \varphi(L'_i) \hat{b} b^{n-i}) b^i tr'' &\xrightarrow{*}_{S_4} r' \hat{z} b^{n-i} (L) b^i tr'' \\ &\xrightarrow{*}_{S_4} r' \hat{z} b^{n-i} (M) b^i tr'' \end{aligned}$$

(here we use the rule $b \rightarrow a$ as many times as necessary).

Let $M'_i = M_i c^{-1}$. Let us define a homomorphism $\theta : A_3^* \rightarrow A_4^*$ (which is analogous to φ) by

$$\theta(a) = ad^n, \quad \theta(b) = bd^n, \quad \theta(c) = cd^n, \quad \theta(d) = d^n.$$

One can notice that, by arguments similar to those used for derivation (27),

$$M \xrightarrow{*}_{S_4} d^i \theta(M'_i) cd^{n-i}. \quad (28)$$

Hence

$$\begin{aligned} r' \hat{z} b^{n-i} (M) b^i tr'' &\xrightarrow{*}_{S_4} r' \hat{z} b^{n-i} (d^i \theta(M'_i) cd^{n-i}) b^i tr'' \\ &\xrightarrow{*}_{S_4} r' \hat{z} d^n \theta(M'_i) cd^n tr''. \end{aligned} \quad (29)$$

Owing to the equality $M_i = \gamma(\tau_1(v_i)c^{6(\mu_1-|v_i|)})c$ and using the last block of six rules of (19), we get

$$\hat{z}d^n\theta(M'_i)cd^n t \xrightarrow{*}_{S_4} \varphi(z\tau_1(v_i))t. \quad (30)$$

By all the above derivations we have:

$$\begin{aligned} \tau_3 \circ \tau_2(w) &\xrightarrow{S_4} r'\hat{z}b^n\varphi(\tau_1(v_i))tr'' \\ &= \varphi(ap)\varphi(\tau_1(v_i))\varphi(q)c \\ &= \tau_3 \circ \tau_2(w'). \quad \square \end{aligned} \quad (31)$$

Proposition 3.4. For every $w, w' \in A_4^*$, if $w \xrightarrow{S_4} w'$ then $\tau_4(w) \xrightarrow{+}_{S_5} \tau_4(w')$.

Proof. Not difficult. \square

3.2.2. Decodings

Proposition 3.5. Let $w \in (yD_1^*)^*y$, $w' \in A_5^*$ be such words that

$$w \xrightarrow{S_5} w'. \quad (32)$$

Then

- (1) $w' \in (yD_1^*)^*y$,
- (2) $\phi_4(w) \xrightarrow{*}_{\bar{S}_4} \phi_4(w')$,
- (3) If the rule used in derivation (32) is $\psi(L)y \rightarrow \psi(M)y$ then $\phi_4(w) \xrightarrow{S_4} \phi_4(w')$.

Proof. Let us notice first that, for every $w \in P_4$, equality (24) implies that $\bar{\psi}(w) = \psi^{-1}(w)$. Hence

$$\bar{\psi} \circ \psi = \text{Id}_{A_4^*}. \quad (33)$$

Let w and w' be such words from A_5^* that $w \in (yD_1^*)^*y$ and $w \xrightarrow{S_5} w'$.

Case 1: The rule used is $\psi(L)y \rightarrow \psi(M)y$.

The occurrence of $\psi(L)y$ in w must be of the form

$$w = p\psi(L)yq \text{ with } p \in (yD_1^*)^* \text{ and } q \in (D_1^*y)^*.$$

Hence

$$w' = p\psi(M)yq$$

which shows that $w' \in (yD_1^*)^*y$ (point (1) of the proposition), and

$$\phi_4(w) = \bar{\psi}(p)\bar{\psi}(\psi(L))\phi_4(yq), \quad \phi_4(w') = \bar{\psi}(p)\bar{\psi}(\psi(M))\phi_4(yq).$$

By identity (33)

$$\phi_4(w) = \bar{\psi}(p)L\phi_4(yq), \quad \phi_4(w') = \bar{\psi}(p)M\phi_4(yq).$$

Hence $\phi_4(w) \xrightarrow{S_4} \phi_4(w')$ (proving points (2) and (3) of the proposition).

Case 2: The rule used is $u_2u_2u_2\psi(d^ncd^n)yu_1u_1 \longrightarrow u_2u_2u_2\psi(b^n)yu_2u_2$.
Then

$$w = pyw_1u_2u_2u_2\psi(d^ncd^n)yu_1u_1w_2qy,$$

$$w' = pyw_1u_2u_2u_2\psi(b^n)yu_2u_2w_2qy$$

with $p, q \in (yD_1^*)^*$, $w_1, w_2 \in D_1^*$.

As $\psi(\hat{a}) \in \Delta_{\mathcal{D}}^*(yw_1u_2u_2u_2)$

$$\bar{\psi}(yw_1u_2u_2u_2) \xrightarrow{*}_{\mathcal{D}} \hat{a}.$$

Hence $\bar{\psi}(yw_1u_2u_2u_2) \in \{\hat{a}, \hat{b}, \hat{c}\}$.

Let us examine all the possible values of the pair $(\bar{\psi}(yu_1u_1w_2), \bar{\psi}(yu_2u_2w_2))$.

One can check that for every $v \in yD_1^*$, only the following cases are possible:

$$\Delta_{\mathcal{D}}^*(v) \cap \{\psi(a), \psi(b), \psi(c)\} = \emptyset, \quad \bar{\psi}(v) = d, \quad (\mathbf{C1})$$

$$\Delta_{\mathcal{D}}^*(v) \cap \{\psi(a), \psi(b), \psi(c)\} = \{\psi(a)\}, \quad \bar{\psi}(v) \in \{a, \hat{a}\}, \quad (\mathbf{C2})$$

$$\Delta_{\mathcal{D}}^*(v) \cap \{\psi(a), \psi(b), \psi(c)\} = \{\psi(a), \psi(b)\}, \quad \bar{\psi}(v) \in \{b, \hat{b}\}, \quad (\mathbf{C3})$$

$$\Delta_{\mathcal{D}}^*(v) \cap \{\psi(a), \psi(b), \psi(c)\} \supseteq \{\psi(c)\}, \quad \bar{\psi}(v) \in \{c, \check{c}, \hat{c}\}. \quad (\mathbf{C4})$$

But the fact that every word in $\{\psi(a), \psi(b), \psi(c)\}$ begins with yu_1u_1 implies that

$$\Delta_{\mathcal{D}}^*(yu_1u_1w_2) \cap \{\psi(a), \psi(b), \psi(c)\} = \Delta_{\mathcal{D}}^*(yu_2u_2w_2) \cap \{\psi(a), \psi(b), \psi(c)\}.$$

Hence both words $yu_1u_1w_2, yu_2u_2w_2$ fulfill the same case \mathbf{Ci} ($1 \leq i \leq 4$).

It follows that

$$\begin{aligned} &(\bar{\psi}(yu_1u_1w_2), \bar{\psi}(yu_2u_2w_2)) \\ &\in \{(x, x) | x \in A_4\} \cup \{(a, \hat{a}), (b, \hat{b}), (c, \check{c}), (c, \hat{c}), (\check{c}, \hat{c})\}. \end{aligned} \quad (34)$$

Let us prove that the two last values $(c, \hat{c}), (\check{c}, \hat{c})$ are impossible.

If $\bar{\psi}(yu_2u_2w_2) = \hat{c}$ then either $\{\psi(a), \psi(c)\} \subseteq \Delta_{\mathcal{D}}^*(yu_2u_2w_2)$ or $\{\psi(\hat{c})\} \subseteq \Delta_{\mathcal{D}}^*(yu_2u_2w_2)$.

In the former case, $\{\psi(a), \psi(c)\} \subseteq \Delta_{\mathcal{D}}^*(yu_1u_1w_2)$ too, so that

$$\bar{\psi}(yu_1u_1w_2) = \hat{c}. \quad (35)$$

In the latter case, $yu_1u_1u_2u_2u_1 \in \Delta_{\mathcal{D}}^*(yu_1u_1w_2)$, hence $\{\psi(a), \psi(c)\} \subseteq \Delta_{\mathcal{D}}^*(yu_1u_1w_2)$ and again (35) holds.

Thus we refined (34) to

$$(\bar{\psi}(yu_1u_1w_2), \bar{\psi}(yu_2u_2w_2)) \in \{(x, x) | x \in A_4\} \cup \{(a, \hat{a}), (b, \hat{b}), (c, \check{c})\}.$$

Hence $\phi_4(w) \xrightarrow{*}_{\bar{s}_4} \phi_4(w')$ using either no rule at all or one of the six last rules of (19) or the three last rules of (20).

Case 3: The rule used is $x\bar{x} \longrightarrow \varepsilon$.

Let $w_1, w'_1 \in A_5^*$ be such words that $w = w_1 y, w' = w'_1 y$. We have $w_1 \xrightarrow{*}_{\mathcal{D}} w'_1$ hence $\Delta_{\mathcal{D}}^*(w_1) \supseteq \Delta_{\mathcal{D}}^*(w'_1)$, so that

$$\bigwedge_{P_4} (\Delta_{\mathcal{D}}^*(w_1) \cap P_4) \xrightarrow{*}_{\mathcal{D}} \bigwedge_{P_4} (\Delta_{\mathcal{D}}^*(w'_1) \cap P_4).$$

As ψ is a lattice isomorphism from A_4 to P_4 we have

$$\psi^{-1} \left(\bigwedge_{P_4} (\Delta_{\mathcal{D}}^*(w_1) \cap P_4) \right) \xrightarrow{*}_{\tilde{s}_4} \psi^{-1} \left(\bigwedge_{P_4} (\Delta_{\mathcal{D}}^*(w'_1) \cap P_4) \right). \quad \square$$

Proposition 3.6. *Let $w, w' \in R_n$ be such words that $w \xrightarrow{*}_{\tilde{s}_4} w'$.*

Then $\phi_3(w) \xrightarrow{}_{\tilde{s}_3} \phi_3(w')$.*

Proof. Easy. \square

Proposition 3.7. *Let w, w' be words from A_3^* .*

(1) *If $w \xrightarrow{*}_{\tilde{s}_3} w'$ then $\phi_2(w) \xrightarrow{*}_{\tilde{s}_2} \phi_2(w')$.*

(2) *If $w \xrightarrow{*}_{\tilde{s}_3} w'$ then $\phi_2(w) \xrightarrow{*}_{\tilde{s}_2} \phi_2(w')$.*

Proof. Easy. \square

Proposition 3.8. *Let $w, w' \in A_2^*$ and $\bar{w} \in \text{Im } \tau_1$ be such words that $\bar{w} \xrightarrow{*}_{S_a^{e,b}} w \xrightarrow{*}_{S_2} w'$. Then $\exists \bar{w}' \in \text{Im } \tau_1$ such that $\bar{w} \xrightarrow{*}_{S_2} \bar{w}' \xrightarrow{*}_{S_a^{e,b}} w'$.*

Proof. Suppose that $w, w' \in A_2^*$ and $\bar{w} \in \text{Im } \tau_1$ are fulfilling

$$\bar{w} \xrightarrow{*}_{S_a^{e,b}} w \xrightarrow{*}_{S_2} w'. \quad (36)$$

Let us distinguish two cases, according to the rule used in the first step of (36).

Case 1: The rule used is $\varepsilon \rightarrow a$.

There exist $p, q, p', q' \in A_2^*, i \in [0, n]$ such that

$$\bar{w} = pq, \quad w = paq = p'\tau_1(u_i)q', \quad w' = p'\tau_1(v_i)q'.$$

If the word p (resp. q) had no factor bb , then no rule of S_2 can use this position of letter a . Hence the given occurrence of $\tau_1(u_i)$ must take place inside p or q . Therefore, there exists $\bar{w}' \in \text{Im } \tau_1$ such that

$$\bar{w} \xrightarrow{*}_{S_2} \bar{w}' \xrightarrow{*}_{S_a^{e,b}} w'. \quad (37)$$

Otherwise, let $p = p_0 b b p_1, q = q_1 b b q_0$ be the decompositions corresponding to the rightmost (resp. leftmost) occurrence of bb in p (resp. q). As $|p_1 q_1| = 4$, we must have $|p_1 a q_1| = 5$, hence no rule of S_2 can use the given occurrence of a . We can thus again conclude that derivation (37) holds.

Case 2: The rule used is $b \rightarrow a$.

There exist $p, q, p', q' \in A_2^*, i \in [0, n]$ such that

$$\bar{w} = pbq, \quad w = paq = p'\tau_1(u_i)q', \quad w' = p'\tau_1(v_i)q'.$$

If p (resp. q) has no factor bb , then $p \in \{\varepsilon, b\}$ (resp. $q \in \{\varepsilon, b\}$). It follows that the given position of a in w cannot be used in a rule of S_2 . We thus reach conclusion (37) again.

Otherwise, let $p = p_0bbp_1, q = q_1bbq_0$ be the decompositions corresponding to the rightmost (resp. leftmost) occurrence of bb in p (resp. q). We must have either $p_1aq_1 = aaaa$ or $|p_1aq_1| = 10$ (if the l.h.s. of $b \rightarrow a$ was taken in a factor bb). In both situations, no rule of S_2 can use this occurrence of a , so that (37) follows again. \square

Proposition 3.9. *Let $w, w' \in A_2^*$ be such words that $w \rightarrow_{S_2} w'$. Then $\phi_1(w) \rightarrow_{S_1} \phi_1(w')$.*

Proof. Not difficult. \square

Proposition 3.10. *Let $w, w' \in A_1^*$ be such words that $w \rightarrow_{S_1} w'$. Then*

- (1) *if the rule used is $\eta(a_0^{\lambda_0}) \rightarrow \varepsilon$, then $\phi_0(w) = \phi_0(w')$,*
- (2) *otherwise, $\phi_0(w) \rightarrow_{S_0} \phi_0(w')$.*

Proof. Not difficult. \square

3.2.3. Stability

Proposition 3.11. *Let $w, w' \in A_5^*$ be such words that $w \in \Delta_{\mathcal{D}}^*(\text{Im } \tau_4)$ and $w \rightarrow_{S_5} w'$. Then $w' \in \Delta_{\mathcal{D}}^*(\text{Im } \tau_4)$.*

Proof. Straightforward. \square

Proposition 3.12. *Let $w, w' \in A_4^*$ be such words that $w \in R_n$ and $w \rightarrow_{\bar{S}_4} w'$. Then $w' \in R_n$.*

Proof. Easy. \square

3.2.4. Extractions

Proposition 3.13. *Let $w \in A_5^*$ be such a word that $w \xrightarrow{\infty}_{S_5}$. Then, $\exists w' \in (yD_1^*)^*y$, $w' \xrightarrow{\infty}_{S_5}$.*

Proof. We define a map $\phi'_5 : (y\{x, \bar{x}\}^*)^* \rightarrow (yD_1^*)^*$ in the following way. Let w be some word in $y\{x, \bar{x}\}^*$. It has a unique decomposition as

$$w = yw_0z_1w_1 \dots z_iw_i \dots z_kw_k,$$

where $w_i \in D_1^*, z_i \in \{x, \bar{x}\}$ and $z_1 \dots z_i \dots z_k = \rho_{\mathcal{D}}(w)$. Then we define

$$\phi'_5(w) = yw_0w_1 \dots w_i \dots w_k.$$

As $y\{x, \bar{x}\}^*$ is a suffix code which is the base of the monoid $(y\{x, \bar{x}\}^*)^*$, ϕ'_5 admits a unique extension as a homomorphism $(y\{x, \bar{x}\}^*)^* \rightarrow (yD_1^*)^*$ which is still denoted by ϕ'_5 .

Now we define a map $\phi_5 : A_5^* \rightarrow (yD_1^*)^*y$ by

$$\forall w \in A_5^*, \quad \phi_5(w) = \phi'_5(ywy).$$

One can check that for all $w, w' \in A_5^*$,

$$w \rightarrow_{S_5} w' \implies \phi_5(w) \rightarrow_{S_5} \phi_5(w').$$

It follows that

$$w \xrightarrow{\infty}_{S_5} \implies \phi_5(w) \xrightarrow{\infty}_{S_5}. \quad \square$$

Proposition 3.14. *Let $w \in A_4^*$ be such a word that $w \xrightarrow{\infty}_{\bar{S}_4}$. Then, $\exists w' \in R_n, w' \xrightarrow{\infty}_{\bar{S}_4}$.*

Proof. Let $D = (w_i)_{i \in \mathbb{N}}$ be an infinite derivation modulo \bar{S}_4 starting from $w = w_0$. For every $v \in A_4^*$ we call *alternation* any factor f of v of the form

$$f = z_1 g z_2$$

such that z_1, z_2 are main letters, $g \in A_4^*$ contains only nominal letters, and $|g| \not\equiv n \pmod{n+1}$. We denote by $\|v\|$ the *number of alternations* of v . We observe first that the rules from $\rightarrow_{\bar{S}_4}$ do not increase the number of alternations. Without loss of generality we can then suppose that all w_i have the same number of alternations, say J . By left-product by a fixed main letter, we can also suppose that all w_i are beginning with the main letter \hat{a} . Let us consider the decompositions

$$w_i = z_{i,0} w_{i,0} z_{i,1} w_{i,1} \dots z_{i,j} w_{i,j} \dots z_{i,J} w_{i,J},$$

where $z_{i,j}$ is nominal, $z_{i,j} w_{i,j}$ has no alternation but $z_{i,j} w_{i,j} z_{i,j+1}$ has one alternation.

The word $z_{i,j} w_{i,j}$ will be called the $(j+1)$ th *block* of w_i . By Lemma 2.1, we can suppose that D is an rl-derivation. We show now that if $J > 0$ then there exists another infinite derivation with at most $J-1$ alternations.

- If some step of derivation applies one of the rules $\hat{b} \rightarrow b, \hat{a} \rightarrow a, \hat{c} \rightarrow \check{c}$ on $z_{i,J}$, then no rule applied later can involve any position of the $(J+1)$ th block. Hence, $(w_{i+1+k}(z_{i+1,J} w_{i+1,J})^{-1})_{k \in \mathbb{N}}$ is an infinite derivation with $(J-1)$ alternations.
- If some step of derivation applies one rule in some j th block ($1 \leq j \leq J$), then no rule applied later can involve any position of the $(J+1)$ th block. Hence we obtain again some infinite derivation with $J-1$ alternations.
- if none of the two above cases occurs, then every rule applies on the $(J+1)$ th block, and the prefix $z_{i,0} w_{i,0} z_{i,1} w_{i,1} \dots z_{i,J-1} w_{i,J-1}$ is fixed. Hence $(z_{i,J} w_{i,J})_{i \in \mathbb{N}}$ is an infinite derivation with 0 alternation.

We have proved by induction that, under the hypothesis of the proposition, there exists some infinite derivation $D' = (w'_i)_{i \in \mathbb{N}}$ with 0 alternation and, in fact, in Q_n . Let $v \in [1, n+1]$ be such an integer that $|w'_i| \equiv v \pmod{n+1}$. Then $(\hat{a} b^n w'_i b^{n+1-v} \check{c})_{i \in \mathbb{N}}$ is an infinite derivation starting in R_n . \square

Proposition 3.15. *Let $w \in A_3^*$ be such a word that $w \xrightarrow{\infty}_{\tilde{S}_3}$. Then, $w \xrightarrow{\infty}_{\tilde{S}_3}$.*

Sketch of proof. Suppose that $D = (w_i)_{i \geq 0}$ is an infinite derivation modulo \tilde{S}_3 , such that $w = w_0$.

Let us remark that no left-hand side of rule of \tilde{S}_3 uses letter d . Hence, after replacing every application of rule $c \rightarrow d$ by an application of the trivial rule $c \rightarrow c$ in D , we obtain another sequence $D' = (w'_i)_{i \geq 0}$ such that

$$w = w'_0 \text{ \& \; } \forall i \in \mathbb{N}, \exists k_i \in \{0, 1\}, w'_i \xrightarrow{k_i}_{\tilde{S}_3} w'_{i+1}.$$

As the system $\{c \rightarrow d\}$ is u-terminating, it is not possible that almost all the steps of derivation D use this rule $c \rightarrow d$. Hence

$$k_i = 1 \text{ for infinitely many } i \in \mathbb{N}.$$

Hence $w \xrightarrow{\infty}_{\tilde{S}_3}$. \square

Proposition 3.16. *Let $w \in A_2^*$ be such a word that $w \xrightarrow{\infty}_{\tilde{S}_2}$. Then*

- (1) $\exists w' \in A_2^*, w' \xrightarrow{\infty}_{S_2}$,
- (2) if $w \in \text{Im } \tau_1$, then $w \xrightarrow{\infty}_{S_2}$.

Proof. Let us suppose that $w \in A_2^*$ is such a word that $w \xrightarrow{\infty}_{\tilde{S}_2}$. Let us prove point (1). We observe that the number of factors b^3 can only decrease in a derivation modulo \tilde{S}_2 . Hence there exists $w_1 \in A_2^*$ such that $w_1 \xrightarrow{\infty}_{\tilde{S}_2}$ and the number of factors b^3 is fixed (throughout the derivation). Now, in such a derivation, the number of consecutive blocks b^2 at distance < 4 (i.e. factors of the form b^2ub^2 with no occurrence of b^2 in bub and $|u| < 4$) can only decrease. Hence there exists $w_2 \in A_2^*$ such that $w_2 \xrightarrow{\infty}_{\tilde{S}_2}$, and the number of factors b^3 is fixed, and the number of consecutive blocks b^2 at distance < 4 is fixed too. In such a derivation the rule $b \rightarrow a$ can be applied only

- between two consecutive b^2 at distance ≥ 5 ,
- or before the first block b^2 or after the last block b^2 ,
- or inside a block b^2 ,
- or can transform a block b^2abaab^2 or b^2aabab^2 into b^2aaaab^2 .

In either case the position of the new letter a introduced by the rule will never be usable later on in the derivation. Hence we can discard all the applications of the rule $b \rightarrow a$ in the derivation, and obtain another infinite derivation modulo S_2 starting on w_2 . Point (1) is proved.

If $w \in \text{Im } \tau_1$, then w has neither factor b^3 nor consecutive b^2 at distance < 4 . Hence, by the above arguments, $w \xrightarrow{\infty}_{S_2}$. Point (2) is proved. \square

4. Reductions and bounds

Let us use the notation

$$\tau = \tau_4 \circ \tau_3 \circ \tau_2 \circ \tau_1 \circ \tau_0, \quad \phi = \phi_0 \circ \phi_1 \circ \phi_2 \circ \phi_3 \circ \phi_4.$$

An easy verification from the definitions shows that for $i = 0, \dots, 4$

$$\phi_i \circ \tau_i = \text{Id}_{A_i^*}, \quad (38)$$

which also implies that

$$\phi \circ \tau = \text{Id}_{A_0^*}. \quad (39)$$

4.1. Finitary problems

4.1.1. Accessibility and common descendant problems

Theorem 4.1. *There exists some semi-Thue system S with 3 rules which has undecidable individual accessibility problem (for some word w_0) and also undecidable common descendant problem.*

Proof. Let S be some finite semi-Thue system over a finite alphabet A , which has undecidable IAP on a given word $w_0 \in A^*$. Let us define a new semi-Thue system by

$$A_0 = A \cup \{\bar{a}\}, \quad S_0 = S \cup \{\bar{a}w_0\bar{a} \rightarrow \varepsilon\},$$

where \bar{a} is a letter not from the alphabet A . It is undecidable, for words $u \in A_0^*$, whether $u \xrightarrow{*}_{S_0} \varepsilon$ or not. Let us choose this system S_0 as a starting-point for our constructions: we consider the sequence of systems $(S_i)_{0 \leq i \leq 5}$ defined in Section 3.1 and starting by the above S_0 . We shall show that, for every $u \in A_0^*$, the three following statements are equivalent:

- (1) $u \xrightarrow{*}_{S_0} \varepsilon$,
- (2) $\tau(u) \xrightarrow{*}_{S_5} y^{3(n+1)+2}$,
- (3) $\tau(u), y^{3(n+1)+2}$ have some common descendant modulo S_5 .

Part (1) \implies (2):

Let us suppose $u \xrightarrow{*}_{S_0} \varepsilon$. Using Proposition 3.1 and the first rule of S_1 we obtain

$$\tau_0(u) \xrightarrow{*}_{S_1} \eta \left(a_0^{\lambda_0} \right) \rightarrow_{S_1} \varepsilon.$$

By Propositions 3.2–3.4

$$\tau(u) \xrightarrow{*}_{S_5} \tau_4(\tau_3(\tau_2(\tau_1(\varepsilon)))), \quad (40)$$

where

$$\tau_4(\tau_3(\tau_2(\tau_1(\varepsilon)))) = \tau_4(\hat{a}b^n\hat{b}b^n\hat{b}b^n c) = \psi(\hat{a}b^n\hat{b}b^n\hat{b}b^n c)y.$$

As for every $z \in A_4$, $\psi(z) \xrightarrow{*}_{\mathcal{D}} y$ we get

$$\tau_4(\tau_3(\tau_2(\tau_1(\varepsilon)))) \xrightarrow{*}_{S_5} y^{3(n+1)+2}. \quad (41)$$

By derivations (40), (41), $\tau(u) \xrightarrow{*}_{S_5} y^{3(n+1)+2}$.

Part (2) \implies (3) is obvious.

Part (3) \implies (1):

Let us suppose that $\tau(u)$ and $y^{3(n+1)+2}$ have some common descendant modulo S_5 . As $y^{3(n+1)+2}$ is irreducible modulo S_5 , we can conclude that

$$\tau(u) \xrightarrow{*}_{S_5} y^{3(n+1)+2}.$$

By Proposition 3.5 we obtain

$$\phi_4(\tau(u)) \xrightarrow{*}_{\bar{S}_4} d^{3(n+1)+1}.$$

As $\phi_4(\tau(u)) \in \text{Im } \tau_3$, $\phi_4(\tau(u)) \in R_n$ and has no occurrence of \hat{c} . Hence by Proposition 3.6

$$\phi_3(\phi_4(\tau(u))) \xrightarrow{*}_{\bar{S}_3} dd$$

which, by Proposition 3.7 leads to

$$\phi_2(\phi_3(\phi_4(\tau(u)))) \xrightarrow{*}_{\bar{S}_2} aa.$$

Applying Proposition 3.8 inductively, we obtain

$$\exists \bar{w}' \in \text{Im } \tau_1, \phi_2(\phi_3(\phi_4(\tau(u)))) \xrightarrow{*}_{S_2} \bar{w}' \xrightarrow{*}_{S_a^{b,b}} aa.$$

The only possible value of \bar{w}' is bb , hence

$$\phi_2(\phi_3(\phi_4(\tau(u)))) \xrightarrow{*}_{S_2} bb$$

and Propositions 3.9, 3.10 then show that

$$\phi(\tau(u)) \xrightarrow{*}_{S_0} \varepsilon, \quad \text{i.e.} \quad u \xrightarrow{*}_{S_0} \varepsilon.$$

The equivalence between points (1), (2) and (3) is then established.

The fact that (1) \iff (2) proves that S_5 has undecidable individual accessibility problem for $w_0 = y^{3(n+1)+2}$.

The fact that (1) \iff (3) proves that S_5 has undecidable common descendant problem. \square

Corollary 1. *The Post correspondence problem is undecidable for 7 pairs of words.*

Proof. Follows from Theorems 4.1 and 2.1. \square

4.2. Infinitary problems

4.2.1. Termination problem

Theorem 4.2. *There exists some semi-Thue system S with 3 rules and with undecidable termination problem.*

Proof. Let S_0 be some finite semi-Thue system over some finite alphabet A_0 having undecidable termination problem. Let us consider the sequence of systems $(S_i)_{0 \leq i \leq 5}$ defined in Section 3.1 and starting by the above S_0 . We reduce now the termination problem for S_0 to the termination problem for S_5 by showing that, for every $u \in A_0^*$

$$u \xrightarrow{\infty}_{S_0} \text{ if and only if } \tau(u) \xrightarrow{\infty}_{S_5}. \quad (42)$$

This implies that the system $S = S_5$ has the required property.

Part “only if”: Let us suppose that $u \xrightarrow{\infty}_{S_0}$. By Propositions 3.1–3.4, we obtain

$$\tau(u) \xrightarrow{\infty}_{S_5}.$$

Part “if”: Let us suppose that

$$\tau(u) \xrightarrow{\infty}_{S_5}. \quad (43)$$

By Proposition 3.5 and owing to the fact that $S_5 - \{\psi(L)y \rightarrow \psi(M)y\}$ is u-terminating, we have

$$\phi_4(\tau(u)) \xrightarrow{\infty}_{\tilde{S}_4}.$$

By Proposition 3.11 the whole derivation (43) lies inside $\Delta_{\mathcal{D}}^*(\text{Im } \tau_4)$, hence

$$\phi_4(\tau(u)) \xrightarrow{\infty}_{\tilde{S}_4}.$$

By Proposition 3.6 and owing to the fact that $\tilde{S}_4 - \{L \rightarrow M\}$ is u-terminating,

$$\phi_3(\phi_4(\tau(u))) \xrightarrow{\infty}_{\tilde{S}_3}.$$

By Proposition 3.15, it is also true that

$$\phi_3(\phi_4(\tau(u))) \xrightarrow{\infty}_{\tilde{S}_3}.$$

By Proposition 3.7, point (2), and owing to the fact that $\{c \rightarrow \varepsilon, a \rightarrow d\}$ is u-terminating

$$\phi_2(\phi_3(\phi_4(\tau(u)))) \xrightarrow{\infty}_{\tilde{S}_2}.$$

Using identities (38) we observe that

$$\phi_2(\phi_3(\phi_4(\tau(u)))) = \tau_1(u) \in \text{Im } \tau_1.$$

Hence by Proposition 3.16, point (2)

$$\phi_2(\phi_3(\phi_4(\tau(u)))) \xrightarrow{\infty}_{S_2}$$

and by Propositions 3.9, 3.10

$$\phi_0(\phi_1(\phi_2(\phi_3(\phi_4(\tau(u))))) \xrightarrow{\infty}_{S_0}$$

i.e., by identity (39)

$$u \xrightarrow{\infty}_{S_0}. \quad \square$$

4.2.2. Uniform termination problem

Theorem 4.3. *The uniform termination problem is undecidable for 3 rules semi-Thue systems.*

Proof. We reduce below the uniform termination problem for finite semi-Thue systems to the uniform termination problem for 3-rules semi-Thue systems. As the former is undecidable (as recalled in Section 1), the second problem is undecidable too.

Let S_0 be some finite semi-Thue system over some finite alphabet A_0 . Here again we consider the sequence of systems $(S_i)_{0 \leq i \leq 5}$ defined in Section 3.1 and starting by the above S_0 . We show now that the uniform termination property for S_0 is equivalent to the uniform termination property for S_5

$$\exists u \in A_0^*, u \xrightarrow{\infty}_{S_0} \text{ if and only if } \exists w \in A_5^*, w \xrightarrow{\infty}_{S_5}. \quad (44)$$

Part “only if”: Let us suppose $u \xrightarrow{\infty}_{S_0}$.

By the same arguments as in part “only if” of the proof of Proposition 4.2, we have

$$\tau(u) \xrightarrow{\infty}_{S_5}.$$

Part “if”: Let us suppose that there exists some $w \in A_5^*$ such that

$$w \xrightarrow{\infty}_{S_5}.$$

By Proposition 3.13

$$\exists w' \in (yD_1^*)^*y, w' \xrightarrow{\infty}_{S_5}.$$

By Proposition 3.5, and owing to the fact that $S_5 - \{\Psi(L)y \rightarrow \Psi(M)y\}$ is u-terminating,

$$\phi_4(w') \xrightarrow{\infty}_{\tilde{S}_4}.$$

By Proposition 3.14

$$\exists w'' \in R_n, w'' \xrightarrow{\infty}_{\tilde{S}_4}.$$

Owing to the fact that $\xrightarrow{\infty}_{\tilde{S}_4}$ does not increase the number of \hat{c} ,

$$\exists w''' \in A_4^*, w'' \xrightarrow{*}_{\tilde{S}_4} w''' \xrightarrow{\infty}_{\tilde{S}_4}$$

and by Proposition 3.12, the whole derivation $w''' \xrightarrow{\infty}_{\tilde{S}_4}$ is inside R_n . Using now Proposition 3.6 and the fact that $\tilde{S}_4 - \{L \rightarrow M\}$ is u-terminating, we obtain

$$\phi_3(w''') \xrightarrow{\infty}_{\tilde{S}_3}.$$

Thus, by proposition 3.15,

$$\phi_3(w''') \xrightarrow{\infty}_{\tilde{S}_3}.$$

Using Proposition 3.7, point (2), and the fact that $\{a \rightarrow d, c \rightarrow e\}$ is u-terminating, we obtain

$$\phi_2(\phi_3(w''')) \xrightarrow{\infty} \tilde{s}_2.$$

By point (1) of Proposition 3.16,

$$\exists w''' \in A_2^*, \quad w''' \xrightarrow{\infty} s_2$$

which, by Propositions 3.9, 3.10 implies

$$\phi_0(\phi_1(w''')) \xrightarrow{\infty} s_0.$$

We have then exhibited some $u \in A_0^*$ such that $u \xrightarrow{\infty} s_0$ as was required. Equivalence (44) is thus proved. \square

5. Related work and perspectives

5.1. Other types of rewriting systems

Beside semi-Thue systems, other kinds of “rewriting systems” among combinatorial objects have been investigated in the literature.

The notion of *Term Rewriting Systems* (TRS) is nowadays considered, on its own, as a domain of theoretical computer science (see [11]). These systems are in some sense brothers of Thue-systems since they were also considered by Thue (as asserted in [35], commenting on [37]). Concerning the termination problem for TRS, it was proved in [8] that this problem is undecidable even when restricted to the one rule case. A systematic classification of termination problems for TRS, from the decidability point of view, is exposed in [14].

A very general notion of *Word Rewriting Systems* was introduced by Post in [31]. These systems consist of rules which are no more linear (as it is the case for TRS) but still apply on words (as it is the case for semi-Thue systems). Concerning these systems, the first author has shown [26] that the accessibility is undecidable, even when restricted to the one rule case.

5.2. Positive side of the same decision problems

As explained in Section 1, much work has been devoted to the search for a solution of the word-problem for one rule Thue systems, which can be seen as the accessibility problem for symmetric two-rules semi-Thue systems (see [1,22]).

The Post Correspondence Problem has been shown decidable for 2 pairs of words [12]. A generalization of this positive result is given in [16], but it remains unknown whether the PCP is solvable for 3 pairs of words.

More recently, a good deal of work has been devoted to the termination and the u-termination problem for one rule semi-Thue systems: [13,15,20,21,30,34,38]. It seems generally hoped that this problem will turn out to be decidable, though no general solution has been found yet.

Acknowledgements

We gratefully thank Vesa Halava for carefully reading a first version of the manuscript and pointing to some mistakes in it. We are also indebted to V. Diekert for inviting both authors in FMI under the support of the Humboldt foundation.

References

- [1] S.I. Adjan, G.S. Makanin, Investigations on algorithmic problems in algebra (in Russian), *Trudy Mat. Inst. Steklov.* 168 (1984) 197–217, English translation in *Proceedings of the Steklov Institute of Mathematics*, Vol. 168, 1986, pp. 207–226.
- [2] V.D. Blondel, V. Canterini, Undecidable problems for probabilistic automata of fixed dimension, *Theory Comput. Syst.* 36 (3) (2003) 231–245.
- [3] R. Book, F. Otto, *String Rewriting Systems*, Texts and Monographs in Computer Science, Springer, Berlin, 1993.
- [4] J. Cassaigne, T. Harju, J. Karhumäki, On the undecidability of freeness of matrix semigroups, *Internat. J. Algebra Comput.* 9 (3–4) (1999) 295–305.
- [5] J. Cassaigne, J. Karhumäki, Examples of undecidable problems for 2-generator matrix semi-groups, *Theoret. Comput. Sci.* 204 (1998) 29–34.
- [6] V. Claus, Some remarks on PCP(k) and related problems, *Bull. EATCS* 12 (1980) 54–61.
- [7] D.J. Collins, Word and conjugacy problems in groups with only a few defining relations, *Z. Math. Logik Grundlag. Math.* 15 (4) (1969) 305–323.
- [8] M. Dauchet, Simulation of Turing machines by a left-linear rewrite rule, in: *Proceedings RTA 89*, Lecture Notes in Computer Science, Vol. 355, Springer, Berlin, 1989, pp. 109–120.
- [9] M. Davis, *Computability and Unsolvability*, McGraw-Hill, New York, 1958 reprinted by Dover Publications, New York, 1982.
- [10] N. Dershowitz, Termination of rewriting, *J. Symbolic Comput.* 3 (1987) 69–116.
- [11] N. Dershowitz, J.P. Jouannaud, *Rewrite Systems*, Handbook of Theoretical Computer Science, Vol. B, Elsevier, Amsterdam, 1991, pp. 243–320 (Chapter 2).
- [12] A. Ehrenfeucht, J. Karhumäki, G. Rozenberg, The (generalized) Post correspondence problem with lists consisting of two words is decidable, *Theoret. Comput. Sci.* 21 (2) (1982) 119–144.
- [13] A. Geser, Decidability of termination of grid string rewriting rules, *SIAM J. Comput.* 31 (4) (2002) 1156–1168 (electronic).
- [14] A. Geser, A. Middeldorp, E. Ohlebusch, H. Zantema, Relative undecidability in term rewriting. I. The termination hierarchy, *Inform. and Comput.* 178 (1) (2002) 101–131.
- [15] A. Geser, H. Zantema, Non-looping string rewriting, *Theor. Inform. Appl.* 33 (3) (1999) 279–301.
- [16] V. Halava, T. Harju, M. Hirvensalo, Generalized Post correspondence problem for marked morphisms, *Internat. J. Algebra Comput.* 10 (6) (2000) 757–772.
- [17] P. Hooper, The undecidability of the Turing machine immortality problem, *J. Symbolic Logic* 31 (2) (1966) 219–234.
- [18] G. Huet, Confluent reductions: abstract properties and applications to term rewriting systems, *J. Assoc. Comput. Mach.* 27 (4) (1980) 797–821.
- [19] M. Jantzen, *Confluent String Rewriting*, EATCS Monograph, Vol. 14, Springer, Berlin, 1988.
- [20] Y. Kobayashi, M. Katsura, K. Shikishima-Tsuji, Termination and derivational complexity of confluent one-rule string-rewriting systems, *Theoret. Comput. Sci.* 262 (1–2) (2001) 583–632.
- [21] W. Kurth, One-rule semi-Thue systems with loops of length one two or three, *RAIRO Inform. Theor. Appl.* 30 (5) (1996) 415–429.
- [22] G. Lallement, The word problem for Thue rewriting systems, *Term Rewriting (Font Romeux, 1993)*, Lecture Notes in Computer Science, Vol. 909, Springer, Berlin, 1995, pp. 27–38.
- [23] A.A. Markov, Impossibility of certain algorithms in the theory of associative systems, *Dokl. Akad. Nauk. SSSR* 55 (7) (1947) 587–590 (in Russian), reprinted in his *Selected Papers*, Vol. 2, MTsNMO Publisher, Moscow, 2003, pp. 3–7 (in Russian).

- [24] A.A. Markov, Impossibility of certain algorithms in the theory of associative systems, Dokl. Akad. Nauk. SSSR 58 (1947) 353–356 (in Russian), reprinted in his Selected Papers, Vol. 2, MTsNMO Publisher, Moscow, 2003, pp. 13–17 (in Russian).
- [25] Yu.V. Matiyasevich, Simple examples of undecidable associative calculi, Dokl. AN SSSR 173 (16) (in Russian), English translation in Soviet Math. Dokl. 8 (1967) 555–557.
- [26] Yu.V. Matiyasevich, Simple examples of unsolvable canonical calculi, Trudy Mat. Inst. Steklov 93 (1967) 50–88 (in Russian), English translation in Proc. Steklov Inst. Math. 93 (1967) 61–110.
- [27] Yu.V. Matiyasevich, On investigations on some algorithmic problems in algebra and number theory, Trudy Matematicheskogo instituta im. V. A. Steklova 168 (1984) 218–235 (in Russian), English translation in Proc. Steklov Inst. Math. 168(3) (1986) 227–252.
- [28] Yu. Matiyasevich, Word problem for Thue systems with a few relations, in: Term Rewriting (Font Romeux, 1993), Lecture Notes in Computer Science, Vol. 909, Springer, Berlin, 1995, pp. 39–53.
- [29] Yu. Matiyasevich, G. Sénizergues, Decision problems for semi-Thue systems with a few rules, Lecture Notes in Computer Science, Vol. 96, IEEE Computer Society Press, Silver Spring, MD, 1996, pp. 523–531.
- [30] R. McNaughton, Semi-Thue systems with an inhibitor, J. Automat. Reason. 26 (4) (2001) 409–431.
- [31] E.L. Post, Formal reductions of the general combinatorial decision problem, Amer. J. Math. 65 (1943) 197–215.
- [32] E.L. Post, Recursive unsolvability of a problem of Thue, J. Symbolic Logic 12 (1) (1947) 1–11 reprinted in: M. Davis (Ed.), Solvability, Provability, Definability: The Collected Works of Emil L. Post, Birkhäuser, Boston a.o., 1994, pp. 503–513.
- [33] G. Sénizergues, Some undecidable termination problems for semi-Thue systems, Theoret. Comput. Sci. 142 (1995) 257–276.
- [34] G. Sénizergues, On the termination-problem for one-rule semi-Thue systems, in: RTA 96, Lecture Notes in Computer Science 1103 (1996) 302–316.
- [35] M. Steinby, W. Thomas, Trees and term rewriting in 1910: on a paper by Axel Thue, Bull. Eur. Assoc. Theoret. Comput. Sci. EATCS (72) (2000) 256–269.
- [36] A. Thue. Probleme über veränderungen von zeichenreihen nach gegebenen regeln, Skr. Vid. Kristiania, I Mat. Naturv. Klasse 10 (1914) 34. Reprinted in his Selected Mathematical Papers, Universitetsforlaget, Oslo, 1977, pp. 493–524.
- [37] A. Thue, Die lösung eines spezialfalles eines generellen logischen problems, Kra. Videnskabs-Selskabets Skrifter. I. Mat. Nat. Kl.nr 8. Reprinted in his Selected Mathematical Papers, Universitetsforlaget, Oslo, 1977, pp. 273–310.
- [38] H. Zantema, A. Geser, A complete characterization of termination of $0^p 1^q \rightarrow 1^r 0^s$, Appl. Algebra Eng. Comm. Comput. 11 (1) (2000) 1–25.