ON SYSTEMS OF WORD EQUATIONS WITH SIMPLE LOOP SETS

ŠTĚPÁN HOLUB AND JUHA KORTELAINEN

Abstract. Consider the infinite system S of word equations

$$\{\mathbf{x}_0\mathbf{u}_1^i\mathbf{x}_1\mathbf{u}_2^i\mathbf{x}_2\cdots\mathbf{u}_m^i\mathbf{x}_m = \mathbf{y}_0\mathbf{v}_1^i\mathbf{y}_1\mathbf{v}_2^i\mathbf{y}_2\cdots\mathbf{v}_n^i\mathbf{y}_n \mid i \in \mathbb{N}\}$$

For each $k \in \mathbb{N}_+$, let T_k be the subsystem of S given by $i \in \{k, k+1, k+2\}$. We prove two properties of the above system.

1) Let $k \geq 1$. If φ is a solution of T_k such that primitive roots of $\varphi(\mathbf{u}_1), \varphi(\mathbf{u}_2), \ldots, \varphi(\mathbf{u}_m)$ are conjugated, as well as primitive roots of $\varphi(\mathbf{v}_1), \varphi(\mathbf{v}_2), \ldots, \varphi(\mathbf{v}_n)$, then φ is a solution of the whole S.
2) If $n = 1$ then, for any $k \geq 2$, a solution φ of T_k is also a solution of S.

1. Introduction

Classical examples of language families whose elements possess some kind of a pumping property are regular, context-free, bounded, and commutative languages. When considering, for instance, the decidability of morphism (or some other mapping) equivalence or effective existence of a test set for those languages, we are led to systems of word equations where pumping in one or several points in an equation can appear.

Throughout the paper we will study the infinite system S of word equations:

$$\{\mathbf{x}_0\mathbf{u}_1^i\mathbf{x}_1\mathbf{u}_2^i\mathbf{x}_2\cdots\mathbf{u}_m^i\mathbf{x}_m = \mathbf{y}_0\mathbf{v}_1^i\mathbf{y}_1\mathbf{v}_2^i\mathbf{y}_2\cdots\mathbf{v}_n^i\mathbf{y}_n \mid i \in \mathbb{N}\}$$

Its subsystem of cardinality three, given by $i \in \{k, k+1, k+2\}$, with $k \in \mathbb{N}$, will be denoted T_k.

By the validity of Ehrenfeucht Conjecture [2], [4], [11], the system S has a finite subsystem that is equivalent to S. Let us briefly survey what is known about our system up to now.

In [1] it is shown that the single equation

$$\mathbf{u}_1^n = \mathbf{v}_1^n\mathbf{v}_2^n\cdots\mathbf{v}_n^n$$

is equivalent to

$$\{\mathbf{u}_1^i = \mathbf{v}_1^i\mathbf{v}_2^i\cdots\mathbf{v}_n^i \mid i \in \mathbb{N}\}.$$

This fact was generalized in [6]. The results of [7] imply that if all the midwords x_i and y_i are empty, the system S is equivalent to its

The first author was supported by the research project MSM 0021620839 financed by MSMT and the Grant Agency of Czech Republic, Grant 201/03/D117.

subsystem T_k, whenever $k \geq 2$. The paper [5] considers S when $\max\{m, n\} = 3$. It is proved that in such a case it is equivalent to the subsystem induced by $i = 0, 1, 2, 3, 4, 5$. Finally, in [9] it is shown that S is equivalent to its subsystem induced by $i = 0, 1, 2, \ldots m+n+2$.

It is not known (see *Open Problem 1*), whether S has an equivalent subsystem of a constant size, i.e., a size independent of m and n. In this paper we give small equivalent subsystems in two special cases. It is organized as follows.

In the second section some preliminaries, definitions and well-known results in the theory of combinatorics on words are given.

In the third section, the first of our cases is studied. We impose an additional condition on the structure of loops, and prove that if for some $k \geq 1$ there is a solution φ of T_k such that the primitive roots of $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_m)$ are conjugated, and also the primitive roots of $\varphi(v_1), \varphi(v_2), \ldots, \varphi(v_n)$ are conjugated, then φ is a solution of whole S.

Section four explains in some generality a method, which in section five is used to prove that if $n = 1$ then S is equivalent to T_k for any $k \geq 2$. That is our second special case, in which the system contains just one loop on one side. Note that the number of loops on the other side is arbitrary.

In the sixth section some open problems and topics of further investigation are presented.

2. Preliminaries

We suppose that the reader is familiar with basic concepts of combinatorics on words as it can be found in [10], where also a proof is given for the following two results belonging to the folklore of combinatorics on words.

Lemma 1. *Let x and y be nonempty words. The following three conditions are equivalent.*

1. *The words x and y are conjugate ;*
2. *The words x and y are of equal length and there exist unique words t_1, and t_2, with t_2 nonempty, such that $t = t_1t_2$ is primitive and $x \in (t_1t_2)^+$ and $y \in (t_2t_1)^+$;*
3. *There exists a word z such that $xz = zy$.*

Furthermore, assume that any of the three conditions above holds and that t_1 and t_2 are as in condition (2). Then, for each word w, we have $xw = wy$ if and only if $w \in (t_1t_2)^*t_1$.

In the setting of the previous lemma we say that x and y are conjugated by z.

Lemma 2. *Two nonempty words commute if and only if they are powers of the same (primitive) word, i.e., they have the same primitive root.*

Recall that the primitive root of a word u is the shortest word r such that $u = r^i$ for some integer $i \geq 1$.

One of the strongest results in the elementary theory of combinatorics on words is the Periodicity Lemma. A slight modification of it can be stated as follows (for the proofs, see for instance [3], [8] and [10]).

Lemma 3. *If two powers u^m and v^n of nonempty words u and v have a common subword of length at least $|u| + |v| - d$ (d being the greatest common divisor of $|u|$ and $|v|$), then the primitive roots of u and v are conjugated.*

Note that if in the previous lemma u^m and v^n have a common prefix of length at least $|u| + |v| - d$, then u and v have the same primitive root, so they are powers of the same (primitive) word.

For each word w, the infinite word $w\,w \cdots$ is denoted by w^ω. In our considerations we will also need the following lemma.

Lemma 4. *Let u and v be words such that $|u| \leq |v|$ and each factor of v of length $|u|$ is conjugated with u. Then v is a factor of u^ω.*

Proof. Let arb be a factor of v of length $|u| + 1$, where a and b are letters. Since both ar and rb are conjugated with u, we deduce $a = b$ from $|ar|_a = |rb|_a = |u|_a$. The claim follows. □

3. Conjugated primitive roots

In this section we prove the result announced in the introduction. To simplify notation, we like to formulate it in the following way.

Theorem 1. *Let m, n be positive integers, and $x_0, \ldots, x_m$, $y_0, \ldots, y_n$, $u_1, \ldots, u_m$, $v_1, \ldots, v_n$ words such that for each $i, j \in \{1, 2, \ldots, m\}$ the primitive roots of u_i and u_j are conjugated, and similarly for each $i, j \in \{1, 2, \ldots, n\}$ the primitive roots of v_i and v_j are conjugated. Let $k \geq 1$ be a positive integer. If*

$$(1) \quad x_0 u_1^i x_1 u_2^i x_2 \cdots u_m^i x_m = y_0 v_1^i y_1 v_2^i y_2 \cdots v_n^i y_n \quad (i = k, k+1, k+2)$$

then also

$$(2) \quad x_0 u_1^i x_1 u_2^i x_2 \cdots u_m^i x_m = y_0 v_1^i y_1 v_2^i y_2 \cdots v_n^i y_n \quad (i = 0, 1, 2, 3, \ldots)\ .$$

Proof. We first introduce several additional assumptions which do not harm generality.

Clearly, we may suppose that the words u_i, $i \in \{1, \ldots, m\}$, and v_i, $i \in \{1, 2, \ldots, n\}$, are non-empty. Assume also that $y_0 = \epsilon$ and that either $x_m = \epsilon$ or $y_n = \epsilon$.

Let $i \in \{1, \ldots, m-1\}$ be such that x_i is empty. We then may suppose that u_i and u_{i+1} do not commute, since otherwise we merge them by writing $(u_i u_{i+1})^j$ instead of $u_i^j u_{i+1}^j$.

We say that two nonempty words u and v are *marked* if they do not begin with the same symbol.

Let $i \in \{1, 2, \ldots, m\}$ be such that x_i is nonempty. The reasoning below verifies that we may consider, without loss of generality, only cases in which u_i and x_i, are marked.

Suppose that z is the longest nonempty prefix of x_i, which is also a prefix of $u_i x_i$. Let $x'_{i-1} = x_{i-1}z$, $u'_i = z^{-1}u_i z$, and $x'_i = z^{-1}x_i$. It is not difficult to see that x'_{i-1}, x'_i and u'_i are well defined, and for any j the word

$$x_0 u_1^j x_1 u_2^j x_2 \cdots u_m^j x_m$$

does not change if we substitute x_{i-1}, x_i, and u_i by x'_{i-1}, x'_i, and u'_i. Repeating the procedure finitely many times we shall obtain the markedness.

Analogously we assume that for each $i \in \{1, 2, \ldots, n-1\}$ such that $y_i = \epsilon$, the words v_i and v_{i+1} do not commute and that for each $j \in \{1, 2, \ldots, n\}$ such that $y_j \neq \epsilon$, the words v_j and y_j are marked.

The proof of the theorem will now proceed by induction with respect to the number $m + n$.

Suppose that $m + n \leq 2$. An obvious length argument yields that $m = n = 1$, $x_1 = \epsilon$, $|x_0| = |y_1|$, and $|u_1| = |v_1|$. From equalities

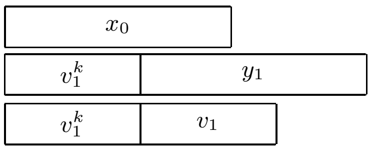
$$x_0 u_1^i = v_1^i y_1 \quad (i = k, k+1) \tag{3}$$

one obtains that v_1 and u_1 are conjugated by $x_0 u_1^k = v_1^k y_1$. Lemma 1 now easily implies that (2) holds.

Suppose that $m + n > 2$. We distinguish two main cases:

1° $|x_0| > |v_1^k|$;
2° $|x_0| \leq |v_1^k|$.

Consider the first case. If $|y_1| > 0$ then the words x_0, v_1 and y_1 begin with the same symbol, and v_1, y_1 are not marked, which is against our assumptions.

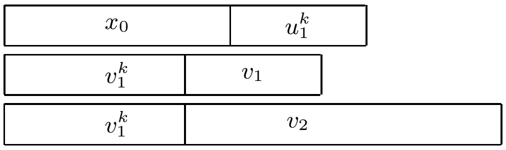


Let therefore $y_1 = \epsilon$.

If

$$|x_0 u_1^k| \geq \min\{|v_1^{k+1}|, |v_1^k v_2|\}$$

then the words v_1 and v_2 are comparable, i.e., one of them is a prefix of the other. Since the primitive roots of v_1 and v_2 are conjugated, they coincide, and v_1 and v_2 commute, again a contradiction with the global assumption.



Suppose, on the other hand, that

$$|x_0u_1^k| < \min\{|v_1^{k+1}|, |v_1^kv_2|\}.$$

Then the word $d = v_1^{-k}x_0$ is a prefix of both v_1 and v_2. Surely

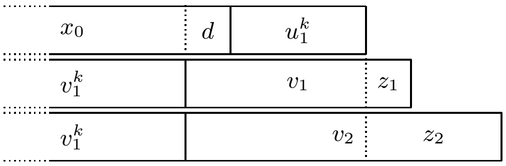
$$|u_1^k| < \min\{|v_1|, |v_2|\}.$$

From (1) we have

(4) $\quad du_1^ix_1u_2^ix_2\cdots u_m^ix_m = v_1^{i-k}v_2^iy_2\cdots v_n^iy_n \quad (i = k, k+1, k+2)$.

Let z_1 and z_2 be words such that

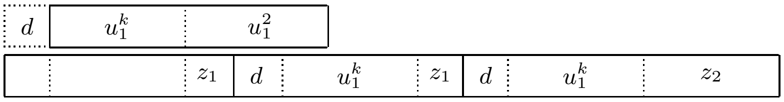
$$v_1 \;=\; du_1^kz_1 \qquad \text{and} \qquad v_2 \;=\; du_1^kz_2.$$



By (4),

(5) $\qquad u_1^ix_1u_2^i\cdots u_m^ix_m = (u_1^kz_1d)^{i-k}(u_1^kz_2d)^{i-1}u_1^kz_2y_2\cdots v_n^iy_n$

for $i = k, k+1, k+2$.



Consider the common prefix of u_1^{k+2} and $(u_1^kz_1d)^2u_1^k$.

If

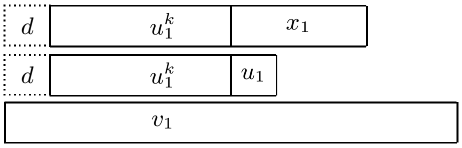
$$|u_1^{k+2}| > |u_1| + |u_1^kz_1d| - 1$$

then, by the Periodicity Lemma, the words u_1 and $u_1^kz_1d$ have the same primitive root t. Since v_1 and v_2 have conjugated primitive roots and their common prefix is longer than t, they commute.

Assume that

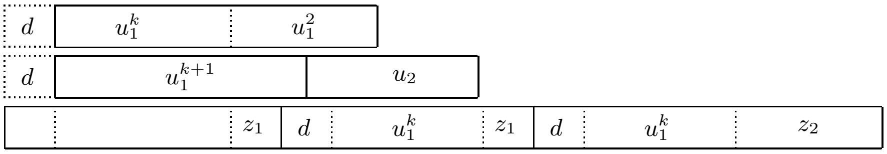
$$|v_1| = |u_1^kz_1d| > |u_1^{k+1}| + 1.$$

If $x_1 \neq \epsilon$, then the words u_1 and x_1 are not marked.



Suppose therefore that $x_1 = \epsilon$. Then (5) implies that u_1^{k+2} is a prefix of $u_1^kz_1du_1$, and $u_1^kz_1du_1$ is comparable with $u_1^{k+1}u_2$. Therefore also

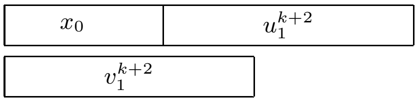
u_1^{k+2} and $u_1^{k+1}u_2$ are comparable, and since primitive roots of u_1 and u_2 are conjugated, they commute.



The second main case was $|x_0| \leq |v_1^k|$. If

(6) $\quad |u_1^{k+2}| \geq |u_1| + |v_1| - 1 \quad$ and $\quad |v_1^{k+2}| - |x_0| \geq |u_1| + |v_1| - 1$

then, by the Periodicity Lemma, primitive roots of u_1 and v_1 are conjugated. Clearly they are conjugated by x_0.



Now the number $n + m$ can be decreased by eliminating u_1 (if $|u_1| > |v_1|$) or v_1 (if $|v_1| > |u_1|$) or both (if $|u_1| = |v_1|$), and we are through by induction.

Let us be more more rigorous. Using Lemma 1, let $t = t_1t_2$ be a primitive word, and q, r and s positive integers such that $u_1 = (t_1t_2)^q$, $v_1 = (t_2t_1)^r$ and $x_0 = t_2(t_1t_2)^s$. Suppose that $q + s \geq r$ (the opposite case being similar). Now (1) allows us to deduce that

(7) $\; t_2(t^{q+s-r})^i x_2 u_2^i \cdots u_m^i x_m = y_1 v_2^i y_2 \cdots v_n^i y_n \quad (i = k, k+1, k+2)$.

By induction, we deduce that

(8) $\quad t_2(t^{q+s-r})^i x_2 u_2^i \cdots u_m^i x_m = y_1 v_2^i y_2 \cdots v_n^i y_n \quad (i = 0, 1, 2, \ldots)$

is true. Obviously, also

(9)

$$t_2(t^{q+s})^i x_2 u_2^i \cdots u_m^i x_m = ((t_2t_1)^r)^i y_1 v_2^i y_2 \cdots v_n^i y_n \quad (i = 0, 1, 2, \ldots)$$

holds, and we are done.

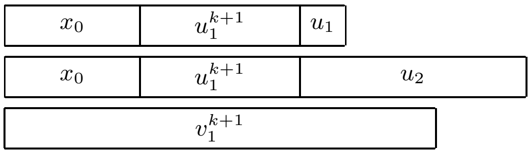
Assume that (6) does not hold because of

(10) $$|v_1| > |u_1^{k+1}| + 1.$$

If $x_1 \neq \epsilon$, the words u_1 and x_1 are not marked. Suppose that $x_1 = \epsilon$. If

$$|v_1^{k+1}| \geq |x_0| + |u_1^{k+2}|$$

then u_1 and u_2 commute.

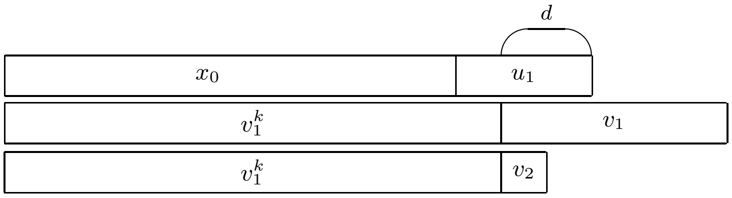


Suppose

$$|v_1^{k+1}| < |x_0| + |u_1^{k+2}|.$$

This implies, together with (10), that $|v_1^k| < |x_0 u_1|$. Let $d = v_1^{-k} x_0 u_1$. Note that d is a prefix of v_1.

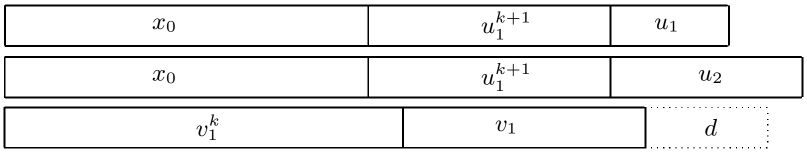
If $y_1 \neq \epsilon$ then v_1 and y_1 are not marked. Therefore $y_1 = \epsilon$ and d is comparable with v_2. If $|d| \geq |v_2|$ then v_1 and v_2 commute.



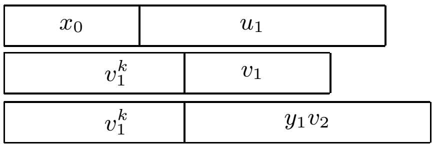
Suppose the contrary, which implies that d is a prefix of v_2 (as well as of v_1). Then both $x_0 u_1^{k+2}$ and $x_0 u_1^{k+1} u_2$ are comparable with $v_1^{k+1} d$. Since

$$|v_1^{k+1} d| = |x_0 u_1| + |v_1| > |x_0 u_1^{k+2}|,$$

the words u_1 and u_2 are comparable, and therefore commute.



Suppose then that the second inequality of (6) is not true, that is $|v_1^{k+1}| < |x_0 u_1| - 1$. Then either v_1 and y_1 are not marked, or (if $y_1 = \epsilon$) the words v_1 and v_2 commute.



The proof is now complete. $\square$

In the rest of the paper we shall prove our second result:

Theorem 2. *Let $k \geq 2$ be a positive integer. The system of equations S:*

$$\{\mathbf{x}_0 \mathbf{u}_1^i \mathbf{x}_1 \mathbf{u}_2^i \mathbf{x}_2 \cdots \mathbf{u}_m^i \mathbf{x}_m = \mathbf{y}_0 \mathbf{v}^i \mathbf{y}_1 \mid i \in \mathbb{N}\} \tag{11}$$

is equivalent to its subsystem T_k given by $i \in \{k, k+1, k+2\}$.

4. Characteristic equation

In this section we explain the method to be used in the proof of the Theorem 2. It was first introduced in [7].

Let $X = \{x_1, \ldots, x_k\}$ be a set of unknowns, and $e = (w_1, w_2) \in X^* \times X^*$ an equation, such that $\mathrm{alph}(e) = X$.

Consider a non-erasing morphism $\varphi : X^* \to \Sigma^*$ solving e, i.e., $\varphi(w_1) = \varphi(w_2)$, and denote $d_i = |\varphi(x_i)|$.

Having got such a solution we choose a new alphabet of unknowns H, construct a new equation $\overline{e} = (\overline{w}_1, \overline{w}_2) \in H^* \times H^*$, and define a length-preserving morphism $\overline{\varphi} : H^* \to \Sigma^*$.

The set H consists of letters $x_{i,j}$, for $i = 1, \dots, k$ and $j = 1, \dots, d_i$. Informally, alphabet H is a set of names of all positions in images of φ. This naturally induces the morphism $\psi : X^* \to H^*$ defined by

$$\psi(x_i) = x_{i,1} \cdots x_{i,d_i}.$$

With help of that morphism, the equation $\overline{e}$ is given by

$$\overline{w}_i = \psi(w_i),$$

$i = 1, 2$. The equation $\overline{e} = (\overline{w}_1, \overline{w}_2)$ is called the *characteristic equation* of e with respect to the morphism φ. Clearly the characteristic equation only depends on the values $d_i, \dots, d_k$.

Finally, the morphism $\overline{\varphi}$ is defined by

$$\overline{\varphi} \circ \psi = \varphi.$$

It should be clear that $\overline{\varphi}$ is well defined and length-preserving. Indeed, it maps H into Σ, since $\overline{\varphi}(x_{i,j})$ is the jth letter of $\varphi(x_i)$ for each j and i.

The definition also immediately implies that $\overline{\varphi}$ is a solution of $\overline{e}$:

$$\overline{\varphi}(\overline{w}_1) = \overline{\varphi} \circ \psi(w_1) = \varphi(w_1) = \varphi(w_2) = \overline{\varphi} \circ \psi(w_2) = \overline{\varphi}(\overline{w}_2).$$

Example. Consider equation $\mathbf{yzxy} = \mathbf{xyyz}$ and its solution φ:

$$\varphi(\mathbf{x}) = ab, \qquad \varphi(\mathbf{y}) = a, \qquad \varphi(\mathbf{z}) = ba.$$

Then we may denote letters in the new alphabet by

$$H = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{z}_1, \mathbf{z}_2\},$$

the characteristic equation is

$$\mathbf{y}_1\mathbf{z}_1\mathbf{z}_2\mathbf{x}_1\mathbf{x}_2\mathbf{y}_1 = \mathbf{x}_1\mathbf{x}_2\mathbf{y}_1\mathbf{y}_1\mathbf{z}_1\mathbf{z}_2,$$

morphism ψ is defined by

$$\psi(\mathbf{x}) = \mathbf{x}_1\mathbf{x}_2, \qquad \psi(\mathbf{y}) = \mathbf{y}_1, \qquad \psi(\mathbf{z}) = \mathbf{z}_1\mathbf{z}_2,$$

and $\overline{\varphi}$ by

$$\begin{aligned} \overline{\varphi}(\mathbf{x}_1) &= a, & \overline{\varphi}(\mathbf{x}_2) &= b, \\ \overline{\varphi}(\mathbf{z}_1) &= b, & \overline{\varphi}(\mathbf{z}_2) &= a, \\ \overline{\varphi}(\mathbf{y}_1) &= a. \end{aligned}$$

□

The reason for introducing the characteristic equation $\overline{e}$ is that it allows to produce linear equalities, which can yield—as we shall see in the next section— important information about e.

The linear equalities are obtained in the following way. Let p be a factor of the word $w = \varphi(w_1) = \varphi(w_2)$. The number of occurrences of p in w can be expressed in two different ways, using $\overline{w}_1$ and $\overline{w}_2$, respectively.

Let's first introduce some more notation. By $\mathbf{F}(w)$ denote the set of all factors of a word w, and by $|w|_p$ the number of occurrences of the word p in w.

Now, given an arbitrary word $p \in \Sigma^*$, we have

$$\sum_{\overline{\varphi}(\alpha)=p} |\overline{w}_1|_\alpha = \sum_{\overline{\varphi}(\alpha)=p} |\overline{w}_2|_\alpha = |w|_p. \tag{12}$$

Proof of (12). Fix $i \in \{1, 2\}$. Recall that $\varphi = \overline{\varphi} \circ \psi$ and $\overline{w}_i = \psi(w_i)$. Each occurrence of p in $\varphi(w_i)$ is therefore an image of some $\alpha \in \mathbf{F}(\psi(w_i))$ mapped by $\overline{\varphi}$. The number $|w|_p$ is given by the number of such preimages α in $\overline{w}_i$. □

Example continued. Consider $p = aa$. The word

$$w = \varphi(\mathbf{yzxy}) = \varphi(\mathbf{xyyz}) = abaaba$$

contains one occurrence of p. There are nine words $\alpha \in H^*$ satisfying $\overline{\varphi}(\alpha) = aa$, namely

$$\begin{array}{lll} \alpha_1 = \mathbf{x}_1\mathbf{x}_1, & \alpha_2 = \mathbf{x}_1\mathbf{y}_1, & \alpha_3 = \mathbf{x}_1\mathbf{z}_2, \\ \alpha_4 = \mathbf{y}_1\mathbf{x}_1, & \alpha_5 = \mathbf{y}_1\mathbf{y}_1, & \alpha_6 = \mathbf{y}_1\mathbf{z}_2, \\ \alpha_7 = \mathbf{z}_2\mathbf{x}_1, & \alpha_8 = \mathbf{z}_2\mathbf{y}_1, & \alpha_9 = \mathbf{z}_2\mathbf{z}_2. \end{array}$$

Therefore (12) has the form

$$\sum_{i=1}^{9} |\psi(\mathbf{yzxy})|_{\alpha_i} = \sum_{i=1}^{9} |\psi(\mathbf{xyyz})|_{\alpha_i}. \tag{13}$$

The equality holds, since $|\psi(\mathbf{yzxy})|_{\alpha_i}$ is equal to one for $i = 7$, and is zero otherwise, while $|\psi(\mathbf{xyyz})|_{\alpha_i}$ is one just for $i = 5$.

Informally, we can say that the factor aa comes on the left side of the equation from a different source than on the right side. The formalism of the characteristic equation is designed to express and exploit that fact. □

5. One loop systems

We are now ready to prove Theorem 2. The theorem deals with the systems S and T_k when $n = 1$, hence we define

$$X = \{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{v}_1, \mathbf{x}_0, \ldots, \mathbf{x}_m, \mathbf{y}_0, \mathbf{y}_1\}.$$

Fix $k \geq 2$, and a morphism φ, which solves the system T_k. Define H, morphisms ψ and $\overline{\varphi}$ as in the previous section. Our task is to show that φ solves S as well. It will be done by showing that the primitive roots of all $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_m)$ are conjugated. Theorem 1 then applies.

Denote

$$\ell_i = \mathbf{x}_0\mathbf{u}_1^i\mathbf{x}_1\mathbf{u}_2^i\mathbf{x}_2\cdots\mathbf{u}_m^i\mathbf{x}_m,$$
$$r_i = \mathbf{y}_0\mathbf{v}^i\mathbf{y}_1$$

for $i = k, k+1, k+2$. Recall that, for each i,

$$(\overline{\ell}_i, \overline{r}_i) = (\psi(\ell_i), \psi(r_i))$$

is the characteristic equation of (ℓ_i, r_i) with respect to φ.

Define the word p, whose number of occurrences will be counted. Let t be the shortest among the primitive roots of words $\varphi(\mathbf{u}_1), \varphi(\mathbf{u}_2), \ldots, \varphi(\mathbf{u}_m)$. Then p is defined by the following conditions:

(i) The word p is a factor of t^ω.
(ii) There exist a word $\alpha \in H^+$ such that
- α is a factor of $\overline{\ell}_{k+2}$,
- $\psi(\mathbf{u}_j^{k+2})$ is a factor of α for some $j \in \{1, 2, \ldots, m\}$; and
- $\overline{\varphi}(\alpha) = p$;

(iii) If p' satisfies (i) and (ii) then $|p| \geq |p'|$.

Example. We shall illustrate the definition of p. Let $k = 2$, $m = 2$ and

$$\varphi(\mathbf{x}_0) = b \qquad \varphi(\mathbf{x}_1) = aba^6b \qquad \varphi(\mathbf{x}_2) = b$$
$$\varphi(\mathbf{u}_1) = a \qquad \varphi(\mathbf{u}_1) = ab.$$

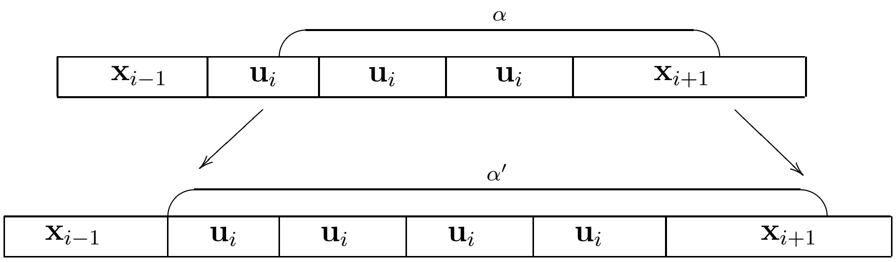
Note that φ is not a solution of the considered system, but it is not important for the definition of p.

In this case $t = a$, and we look for the largest power of a in ℓ_4, which covers the image of some $\varphi(\mathbf{u}_i)$ as required by the condition (ii). Therefore $p = a^5$. Although a^6 is also a factor of ℓ_4, it does not satisfy (ii). □

Lemma 5. *Let i be in $\{k, k+1\}$ and $\alpha \in \mathbf{F}(\overline{\ell}_i)$ be a word such that $\overline{\varphi}(\alpha) = p$. Then*

$$|\overline{\ell}_{k+1}|_\alpha - |\overline{\ell}_k|_\alpha = |\overline{\ell}_{k+2}|_\alpha - |\overline{\ell}_{k+1}|_\alpha. \tag{14}$$

Proof. We first show that no factor of $\psi(u_j^{k+1})$, longer than $|\psi(u_j^2)|$, is a factor of α. Suppose the contrary. Then, by the Periodicity Lemma, the word $\varphi(u_j)$ commutes with a conjugate of t. This implies that we can find a factor α' of $\overline{\ell}_{k+2}$, longer than α, such that $\overline{\varphi}(\alpha')$ is also a factor of t^∞. It is enough, informally speaking, to extend in α each factor of $\psi(u_j^{k+1})$, longer than $|\psi(u_j^2)|$, to $\psi(u_j^{k+2})$. This is a contradiction with the maximality of p.



This implies that α hits some $\psi(x_j)$ for at most one j. Therefore if it contains at least one letter of some $\psi(x_j)$ then it occurs exactly once in all ℓ_k, ℓ_{k+1} and ℓ_{k+2}, i.e.,

$$|\overline{\ell}_k|_\alpha = |\overline{\ell}_{k+1}|_\alpha = |\overline{\ell}_{k+2}|_\alpha = 1.$$

Note that the previous argument would not work for $k = 1$.

The only remaining possibility is that α is a factor of $\psi(u_j^{k+1})$, shorter than $\psi(u_j^2)$.

Then it is easy to see that

$$|\overline{\ell}_{k+1}|_\alpha - |\overline{\ell}_k|_\alpha = |\overline{\ell}_{k+2}|_\alpha - |\overline{\ell}_{k+1}|_\alpha = 1.$$

The proof is now complete. $\square$

Equality (12) yields

$$|\varphi(\ell_i)|_p = \sum_{\overline{\varphi}(\alpha)=p} |\overline{\ell}_i|_\alpha$$

for $i = k, k+1, k+2$. In this point we shall exploit the requirement (ii) in the definition of p. The condition guarantees that there is at least one word $\alpha \in H^+$ satisfying $\overline{\varphi}(\alpha) = p$, which is a factor of $\overline{\ell}_{k+2}$ and is neither a factor of $\overline{\ell}_k$ nor of $\overline{\ell}_{k+1}$. That implies, together with (14), that

$$|\varphi(\ell_{k+2})|_p - |\varphi(\varphi(\ell_{k+1})|_p > |\varphi(\ell_{k+1})|_p - |\varphi(\ell_k)|_p. \tag{15}$$

Confronting the last inequality with the structure of the right side of our equations we get the following claim.

Lemma 6. *The primitive root of $\varphi(\mathbf{v}_1)$ is conjugated with t.*

Proof. Let α be a word from $\mathbf{F}(\overline{r}_k) \cup \mathbf{F}(\overline{r}_{k+1})$ satisfying $\overline{\varphi}(\alpha) = p$. In a similar manner as in Lemma 5 one can show that for our α the equality

$$|\overline{r}_{k+1}|_\alpha - |\overline{r}_k|_\alpha = |\overline{r}_{k+2}|_\alpha - |\overline{r}_{k+1}|_\alpha. \tag{16}$$

holds. Then from (15) we deduce that there must exist at least one factor α of $\overline{r}_{k+2}$, which is neither a factor of $\overline{r}_k$ nor of $\overline{r}_{k+1}$, such that $\overline{\varphi}(\alpha) = p$. Such an α necessarily contains the factor $\psi(v^{k+1})$. The Periodicity Lemma concludes the proof. $\square$

Now, it can be intuitively clear that there cannot exist a loop, the primitive root of which is not conjugated with t. A proof of this fact is given in the following lemma.

Lemma 7. *For any* $i \in \{1, 2, \dots, m\}$ *the primitive root of* $\varphi(\mathbf{u}_i)$ *is conjugated with* t.

Proof. Let $j \in \{1, 2, \dots m\}$ and γ be a factor of $\psi(\mathbf{u}_j^2)$ of length $|t|$ such that $s = \overline{\varphi}(\gamma)$ is not conjugated with t. From the structure of $\overline{\ell}_k$ and $\overline{\ell}_{k+1}$ it is straightforward to see that $|\varphi(\ell_k)|_s < |\varphi(\ell_{k+1})|_s$.

Let us now turn our attention to $\overline{r}_k$ and $\overline{r}_{k+1}$. Their structure clearly implies that the equality $|\varphi(\ell_k)|_s = |\varphi(\ell_{k+1})|_s$ holds; the preimages of s have to hit either y_0 or y_1, otherwise s is conjugated with t. We have achieved a contradiction, therefore for any $j \in \{1, 2, \dots, m\}$ all factors of $\varphi(\mathbf{u}_j^2)$ of length $|t|$ are conjugated with t. Lemma 4 and the Periodicity Lemma conclude the proof. □

By the results above, the primitive roots of words $u_1, u_2, \dots, u_m$ are conjugated and, by Theorem 1, we are done.

6. Some open problems

The following problem still remains open:

Open Problem 1. Does there exist $q \in \mathbb{N}$ such that (for any m and n in $\mathbb{N}$), the system S is equivalent to the subsystem induced by $i = 0, 1, 2, \dots, q$?

We also wish to mention

Open Problem 2. Is the system $\{u_1^i = v_1^i v_2^i \cdots v_n^i \mid i \in \mathbb{N}\}$ equivalent to the subsystem induced by $i = 1, 2, 3$?

References

[1] K. I. Appel and F. M. Djorup, On the equation $z_1^n z_2^n \cdots z_k^n = y^n$ in a free semigroup. *Trans. Amer. Math. Soc.* **134** (1968), 461–470.
[2] M. H. Albert and J. Lawrence, A proof of Ehrenfeucht‘s Conjecture. *Theoret. Comput. Sci.* **41** (1985), 121–123.
[3] N.J. Fine and H.S. Wilf, Uniqueness theorem for periodic functions. *Proc. Amer. Math. Soc.* **16** (1965), 109–114.
[4] V.S. Guba, Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems, *Mat. Zametki* **40** (1986), 321-324.
[5] I. Hakala and J. Kortelainen, On the system of word equations $x_0 u_1^i x_1 u_2^i x_2 u_3^i x_3 = y_0 v_1^i y_1^i v_2^i y_2 v_3^i y_3$ $(i = 0, 1, 2, \dots)$ in a free monoid. *Theoret. Comput. Sci.* **225** (1999), 149–161.
[6] T. Harju, D. Nowotka, On the Equation $x_k = z_1^{k_1} z_2^{k_2} \dots z_n^{k_n}$ in a free femigroup. *TUCS Tecnical report* **602**, 2004.
[7] Š. Holub, Local and global cyclicity in free semigroups. *Theoret. Comput. Sci.* **262** (2001), 25–36.
[8] V. Keränen, On the k-freeness of morphisms on free monoids. *Ann. Acad. Sci. Fenn. Math. Diss.* **61**, 1986.

[9] J. Kortelainen, On the system of word equations
$x_0u_1^ix_1u_2^ix_2\cdots u_m^ix_m = y_0v_1^iy_1v_2^iy_2\cdots v_n^iy_n \quad (i = 0, 1, 2, ...)$
in a free monoid. *J. Autom. Lang. Comb.* **3** (1998), 43–357.

[10] M. Lothaire, *Combinatorics on Words*, Addison-Wesley, Reading Massachusetts, 1983.

[11] A. Salomaa, The Ehrenfeucht conjecture: A proof for language theorist. *Bull. EATCS* **27** (1985),

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic

Department of Information Processing Science, University of Oulu, Oulu, Finland