Local and global cyclicity in free semigroups

Štěpán Holub

Department of mathematics, Charles University, Sokolovská 83, 186 75 Praha

Abstract

It is shown that the system of equations $\{(x_1^r \dots x_n^r)^s = (x_1^s \dots x_n^s)^r \mid r,s \in \mathbf{N}\}$ is equivalent to its two-element subset $\{(x_1^a \dots x_n^a)^b = (x_1^b \dots x_n^b)^a,\ (x_1^a \dots x_n^a)^c = (x_1^c \dots x_n^c)^a\}$, whenever a,b,c are integers such that $1 < a < b < c$. The result implies that the language $L = \{x_1^k \dots x_n^k \mid k \in \mathbf{N}\}$ has a three-element test set $T = \{x_1^k \dots x_n^k \mid k = a, a+1, a+2\}$, with an integer $a > 1$.

Introduction

Ehrenfeucht's Conjecture, proved in [2], states that every infinite system of equations in free monoids, with finitely many unknowns, has an equivalent finite subset. The most simple example is a system of non-trivial equations in two unknowns, equivalent to any of its elements, a consequence of the Defect Theorem (see e.g. [5]).

Clearly the system

$$\{(x_1^r \dots x_n^r)^s = (x_1^s \dots x_n^s)^r \mid r,s \in \mathbf{N}\} \tag{1}$$

is equivalent to its (infinite) subset

$$\{(x_1 \dots x_n)^r = x_1^r \dots x_n^r \mid r \in \mathbf{N}\}. \tag{2}$$

We consider the system (1) to express our result in its most general form. It is not difficult to see that both systems have only cyclic solutions. Therefore a subset of (1) is equivalent to the whole system if and only if it forces the

[1] Partially supported by the University Development Fund of Czech Republic, grant 1379/1998

cyclicity of the solution. For every exponent $k \in \mathbf{N}$ there exist a number of unknowns n such that the equation

$$(x_1 \dots x_n)^k = x_1^k \dots x_n^k$$

has a non-cyclic solution. Put, for example, $n = 2k - 1$ and

$$x_i = \begin{cases} A & i = 2j, \quad 1 \le j \le k-1 \\ A^{k-j} B A^{j-1} & i = 2j-1,\ 1 \le j \le k, \end{cases}$$

with some letters A, B. There exists also a non-cyclic solution (see [8]) of the equation

$$(x_1^2 \dots x_n^2)^3 = (x_1^3 \dots x_n^3)^2.$$

On the other hand, it was shown (see [1]) that the equation $y^n = x_1^n \dots x_n^n$ has only cyclic solutions. Especially the cyclicity of the solution is forced by the single equation

$$(x_1 \dots x_n)^k = x_1^k \dots x_n^k \tag{3}$$

from the system (2), if $k \ge n$.

In [6] it is shown that the system (2) is equivalent to its subset where $r = 2, 3, \dots \lceil n/2 \rceil + 1$. In the same paper it is shown that if $n = 3, 4$ or 5 then the system (3) with $k = 2, 3$ forces cyclicity, and if $n = 7$ then (3) with $k = 2, 3, 4$ does so. Interesting results regarding more general equational systems can be found in [9].

All above results could suggest that the size and/or the maximal exponent of an equivalent subsystem of (2) depends on the number of unknowns. In contrast to the expectation we prove that already the pair of equations

$$(x_1^2 \dots x_n^2)^3 = (x_1^3 \dots x_n^3)^2$$
$$(x_1^2 \dots x_n^2)^4 = (x_1^4 \dots x_n^4)^2$$

is good enough for arbitrary n.

A consequence of the result for the existence of a test set is proved in the Section 4.

1 Factors, instances and equations

Let Σ be a finite *alphabet*. Elements of Σ are called *letters* and sequences of letters are called *words*. The sequence of length zero is called the *empty word*. The set of all words (all non-empty words, resp.) is denoted by Σ^* (Σ^+, resp.). It is a monoid (semigroup, resp.) under the operation of concatenation. The length of a word u will be denoted by $|u|$. We say that a word u is a *factor* of a word v if and only if there exist words z, $z' \in \Sigma^*$ such that $v = zuz'$. The set of all non-empty factors of a word v we shall denote by $F(v)$. A factor u of a word v can occur in v in different *instances* (each of those determined by the length of the word preceding u in v). The number of instances of a non-empty word u in v will be denoted by $f(u, v)$.

By a *cyclic factor* of v we shall understand every factor u of vv with $|u| \leq |v|$. An instance of a cyclic factor will be sometimes called a *cyclic instance* of u, and it corresponds to an instance of u in vv that starts within the first copy of v. The set of all non-empty cyclic factors of v will be denoted by $C(v)$. The number of cyclic instances of a non-empty word u in v will be denoted by $c(u, v)$. If u is not a factor (a cyclic factor resp.) of v, set $f(u, v) = 0$ ($c(u, v) = 0$ resp.).

We shall say that the word v is *p-cyclic* if and only if it is power of a word u, $|u| = p$. Note that every word v is $|v|$-cyclic.

Let T be a finite set of unknowns. Each pair

$$(e, e') \in T^+ \times T^+$$

we shall call an *equation* in unknowns from T. For a particular equation we often use the suggestive notation $e = e'$.

We shall say that a morphism $\varphi : T^+ \to \Sigma^+$ is a *solution* of the system of equations $S \subseteq T^+ \times T^+$ in the semigroup Σ^+ if and only if for every $(e, e') \in S$ the equality $\varphi(e) = \varphi(e')$ holds. Two systems of equations S, S' are called *equivalent* if and only if they have the same set of solutions.

We shall say that a morphism $\varphi : T^+ \to \Sigma^+$ is *length-preserving* if and only if $|\varphi(t)| = 1$ for each $t \in T$ (i.e. $\varphi[T] \subseteq \Sigma$).

We shall say that a solution $\varphi : T^+ \to \Sigma^+$ is *cyclic* if and only if there exists a word $v \in \Sigma^+$ such that $\varphi(x)$ is a power of v for every $x \in T$.

Now we introduce two easy lemmas that allow to count the number of cyclic instances of given word in another word.

Lemma 1.1 *Let $u, v, w \in \Sigma^+$ be words such that $w \in F(v)$ and $v \in C(u)$.*

Suppose that every cyclic instance of w in u is contained in exactly one cyclic instance of v in u. Then $c(w,u) = f(w,v) \cdot c(v,u)$.

Proof. Let W be the set of all cyclic instances of w in u, and V the set of all cyclic instances of v in u. By assumptions, there exists a mapping $\varphi : W \to V$ that maps an instance of w to the instance of v that contains the instance of w as a factor. Every element of V is an image of exactly $f(w,v)$ instances of w. □

Lemma 1.2 *Let $u, v, w \in \Sigma^+$ be words and $k \geq 1$ an integer such that $c(w,u) = 1$, $w \in F(v)$ and $v \in C(u^k)$. Then $c(v,u^k) = k$.*

Proof. Cyclic shifts by $i|u|$ elements, $1 \leq i \leq k$, give exactly k different cyclic instances of v in u^k. Let us suppose, for contradiction, that we have $k+1$ different cyclic instances of v in u^k. Then there are two different cyclic instances of v, and thus also of w, starting within the same copy of u, a contradiction with $c(w,u) = 1$. □

The following lemma is highly intuitive and is crucial for the method described in Section 2.

Lemma 1.3 *Let $\psi : T^+ \to \Sigma^+$ be a length-preserving morphism, and $v \in T^+$, $u \in \Sigma^+$ words such that $\psi(v) = u$. Then for each $\alpha \in \Sigma^+$,*

$$c(\alpha, u) = \sum_{w \in \psi^{-1}(\alpha)} c(w,v) = \sum_{w \in \psi^{-1}(\alpha) \bigcap C(v)} c(w,v).$$

Proof. Every cyclic instance of α in u determines a unique cyclic instance of some $w \in \psi^{-1}(\alpha)$ in v. On the other hand, every cyclic instance of a $w \in \psi^{-1}(\alpha)$ in v determines a unique cyclic instance of $\psi(w) = \alpha$ in u. If the word $w \in \psi^{-1}(\alpha)$ is not in $C(v)$ then, by the definition, $c(w,v) = 0$ and it can be omitted. □

An important result in the elementary theory of words is the periodicity lemma of Fine and Wilf (see [3]). We shall use the following formulation of the lemma:

Lemma 1.4 *Assume u, $v \in \Sigma^+$ and let some their powers u^p, v^q have a common factor of length $|v| + |u| - d$ (d being the greatest common divisor of $|u|$ and $|v|$). Then both u and v are d-cyclic.*

Next lemma is a direct consequence of the above mentioned Defect Theorem and it allows us to restrict ourselves to the equations with at least three unknowns.

Lemma 1.5 *Every equation (e, e') in two unknowns and with $e \neq e'$, has only cyclic solutions.*

2 Quantitative equalities

In this section we introduce the method that will yield in Section 3 the main result of this paper. Let R be a non-empty finite set of positive integers. Denote by P the product of all integers in R. For each $r \in R$, let $\bar{r} = P/r$. We shall consider the system of equations

$$(x_1^r \dots x_n^r)^s = (x_1^s \dots x_n^s)^r;\ r, s \in R. \tag{4}$$

For our purposes, however, it will be more convenient to study an equivalent equational system

$$(x_1^r \dots x_n^r)^{\bar{r}} = (x_1^s \dots x_n^s)^{\bar{s}};\ r, s \in R, \tag{5}$$

in which all equations have the same length.

Suppose we have an arbitrary, but fixed solution $\varphi : X^+ \to \Sigma^+$, $X = \{x_1, \dots, x_n\}$, of (5). Denote the word $\varphi(x_i)$ by u_i and the length of it by d_i. Note that the word $\varphi((x_1^r \dots x_n^r)^{\bar{r}})$ is independent of the choice of $r \in R$. Denote that word by u_P.

We shall construct quantitative equalities connected to the system (5), by means of Lemma 1.3. To do this, choose a word $\alpha \in C(u_P)$ and trace back all its preimages in words $(x_1^r \dots x_n^r)^{\bar{r}}$, $r \in R$. In order to classify these preimages according to their structure, we introduce a new alphabet Y consisting of new letters $y_{i,j}$, with $1 \le i \le n$, $1 \le j \le d_i$. Denote by η_j the word $y_{j,1} \dots y_{j,d_j}$ for every j, $1 \le j \le n$, and by z_r the word $(\eta_1^r \dots \eta_n^r)^{\bar{r}}$. The system of equations

$$z_r = z_s;\ r, s \in R \tag{6}$$

can be obtained from (5) substituting x_i by η_i, but note that it is a system in d unknowns, with $d = \sum_{i=1}^n d_i$.

The most natural thing to do now is to define a morphism $\psi : Y^+ \to \Sigma^+$ by the equality

$$\psi(\eta_1 \dots \eta_n) = u_1 \dots u_n.$$

Clearly the definition is correct,

$$\begin{aligned} \varphi(x_i) &= \psi(\eta_i),\ 1 \le i \le n, \\ u_P &= \psi(z_r),\ r \in R \end{aligned}$$

holds and the morphism ψ is a length-preserving solution of (6). We can now classify preimages of α in ψ rather than in φ. Denote by W the set

$$W = W_R = \bigcup (C(z_r) \mid r \in R). \tag{7}$$

of all non-empty cyclic factors of words z_r (and potential preimages of α in ψ).

For elements of the set W we define two parameters (N.B.: sums $j+1$, $j-1$ will be further understood modulo n):
For every $w \in W$ denote by $J(w)$ the set of all integers j, $1 \leq j \leq n$, for which there exists an integer i, $1 \leq i \leq d_j$, such that $y_{j,i}$ occurs in w.

The second parameter of a word $w \in W$ we denote by $\sigma(w)$. First note that w belongs to just one $C(z_r), r \in R$, if $|J(w)| \geq 3$. In such a case put

$$\sigma(w) = r.$$

If $J(w) = \{j\}$, then put

$$\sigma(w) = \min\{s \mid w \in F(\eta_j^s)\}.$$

If $|J(w)| = 2$, then clearly $J(w) = \{j, j+1\}$, for some $1 \leq j \leq n$, and put

$$\sigma(w) = \min\{s \mid w \in F(\eta_j^s \eta_{j+1}^s)\}.$$

Observe that $1 \leq \sigma(w) \leq \max R$ holds for every $w \in W$.

We can summarize that $|J(w)|$ says how many different words η_j are "affected" by w, while $\sigma(w)$ says how many copies of the same η_j are "affected" by w.

Using the values $|J(w)|$ and $\sigma(w)$ we shall classify the words from W. For k and s with $1 \leq k \leq 2$ and $1 \leq s \leq \max R$ put

$$W(k,s) = \{w \in W \mid |J(w)| = k \text{ and } \sigma(w) = s\}, \text{ and}$$
$$W(3,s) = \{w \in W \mid |J(w)| \geq 3 \text{ and } \sigma(w) = s\}.$$

It is clear from the definition that the above classification is correct, i.e. it is disjoint factorization of W. The fact is expressed in the following lemma.

Lemma 2.1 *Assume* $1 \leq k_i \leq 3$ *and* $1 \leq s_i \leq \max R$, $i \in \{1,2\}$. *Then*

$$W(k_1, s_1) \bigcap W(k_2, s_2) \neq \emptyset \text{ if and only if } (k_1, s_1) = (k_2, s_2).$$

Furthermore,

$$W = \bigcup (W(k,s) \mid 1 \leq k \ \leq 3 \text{ and } 1 \leq s \ \leq \max R).$$

The main motivation of the classification is that words from the same class have the same number of instances in words z_r. The number of these instances is counted in the following lemma.

Lemma 2.2 *Assume $r \in R$ and $w \in C(z_r)$.*

(i) If $w \in W(1,s)$, then $s \leq r$ and $c(w,z_r)$ equals $(r-s+1)\bar{r}$.
(ii) If $w \in W(2,s)$, then $s \leq r$ and $c(w,z_r)$ equals $\bar{r}$.
(iii) If $w \in W(3,s)$, then $s = r$ and $c(w,z_r)$ equals $\bar{r}$.

Proof. (i) Suppose $J(w) = \{j\}$ and $s > r$. By the definition of $W(1,s)$, the word w is not a factor of η_j^r in contradiction with $w \in C(z_r)$. By Lemma 1.1,

$$c(\eta_j^s, z_r) = f(\eta_j^s, \eta_j^r) c(\eta_j^r, z_r) = (r-s+1)\bar{r}$$

holds and

$$c(w, z_r) = f(w, \eta_j^s) c(\eta_j^s, z_r) = c(\eta_j^s, z_r),$$

by Lemma 1.1 again.

(ii) Suppose $J(w) = \{j, j+1\}$ and $s > r$. By the definition of $W(2,s)$, the word w is not a factor of $\eta_j^r \eta_{j+1}^r$ in contradiction with $w \in C(z_r)$. Using again Lemma 1.1 we obtain

$$c(w, z_r) = f(w, \eta_j^r \eta_{j+1}^r) c(\eta_j^r \eta_{j+1}^r, z_r) = c(\eta_j^r \eta_{j+1}^r, z_r) = \bar{r}.$$

(iii) The equality $s = r$ is clear. Furthermore there exists an integer j, $1 \leq j \leq n$ such that

$$y_{j-1,d_{j-1}} \eta_j^r y_{j+1,1} \in F(w).$$

We have

$$c(y_{j-1,d_{j-1}} \eta_j^r y_{j+1,1}, \eta_1^r \dots \eta_n^r) = 1,$$

and hence $c(w, z_r) = \bar{r}$, by Lemma 1.2. □

For each $1 \leq k \leq 3$, $1 \leq s \leq \max R$ and $r \in R$ define

$$c(k,s,r) = c(w, z_r), \tag{8}$$

with $w \in W(k,s)$. The definition is independent of the choice of the word w in $W(k,s)$, according to Lemma 2.2.

Lemma 2.3 *Let $1 \leq k \leq 3$, $1 \leq s \leq \max R$ and $r \in R$ be integers. Then*

(i) c(k,s,r)=0 if and only if $C(z_r) \bigcap W(k,s)$ is empty, i.e. if either $s > r$ or $k = 3$ and $s \neq r$.
(ii) If $C(z_r) \bigcap W(k,s)$ is not empty then $W(k,s) \subseteq C(z_r)$.

Proof. It is a direct consequence of the Lemma 2.2. □

The desired quantitative equalities are constructed in the following lemma.

Lemma 2.4 *Assume $\alpha \in C(u_P)$. For each $1 \leq k \leq 3$ and $1 \leq s \leq \max R$ denote*

$$\tilde{\alpha}(k,s) = card(\psi^{-1}(\alpha) \bigcap W(k,s)). \tag{9}$$

Then

$$c(\alpha, u_P) = \sum_{k=1}^{3} \sum_{s=1}^{\max R} c(k,s,r)\tilde{\alpha}(k,s)$$

for each $r \in R$.

Proof. Fix $r \in R$.

$$\begin{aligned}
c(\alpha, u_P) &\overset{\text{Lemma1.3}}{=} \sum_{w \in \psi^{-1}(\alpha)} c(w, z_r) \\
&\overset{(7)}{=} \sum_{w \in \psi^{-1}(\alpha) \bigcap W} c(w, z_r) \\
&\overset{\text{Lemma2.1}}{=} \sum_{k=1}^{3} \sum_{s=1}^{\max R} \sum_{w \in \psi^{-1}(\alpha) \bigcap W(k,s)} c(w, z_r) \\
&\overset{(8)}{=} \sum_{k=1}^{3} \sum_{s=1}^{\max R} \sum_{w \in \psi^{-1}(\alpha) \bigcap W(k,s)} c(k,s,r) \\
&\overset{(9)}{=} \sum_{k=1}^{3} \sum_{s=1}^{\max R} c(k,s,r)\tilde{\alpha}(k,s).
\end{aligned}$$

□

Every $r \in R$ gives another expression of $c(\alpha, u_P)$ by means of coefficients $c(k,s,r)$ and variables $\tilde{\alpha}(k,s)$. We thus obtain $|R|$ different quantitative equalities.

3 The main theorem

In this section we shall assume that

$$R = \{a, b, c\},$$

where a, b, c are integers such that $1 < a < b < c$. According to the notation used in Section 2 we denote $P = abc$, $\bar{a} = bc$, $\bar{b} = ac$, $\bar{c} = ab$. Fix an integer n and define

$$X = \{x_1, \ldots, x_n\},$$

a set of unknowns.

We want to prove the following theorem:

Theorem 3.1 *The system of equations*

$$(x_1^a \ldots x_n^a)^b = (x_1^b \ldots x_n^b)^a \tag{10}$$
$$(x_1^a \ldots x_n^a)^c = (x_1^c \ldots x_n^c)^a \tag{11}$$

in unknowns $x_1, \ldots, x_n$ admits only cyclic solutions.

Proof. Once more we will work with an equivalent system

$$(x_1^a \ldots x_n^a)^{bc} = (x_1^b \ldots x_n^b)^{ac} \tag{12}$$
$$(x_1^a \ldots x_n^a)^{cb} = (x_1^c \ldots x_n^c)^{ab} \tag{13}$$

rather than with (10), (11).

If $n = 1$, then the statement is trivial. Thank to Lemma 1.5, we can assume $n \geq 3$.

Let now $\varphi : X^+ \to \Sigma^+$ be a solution of S. Define u_i, d_i, η_i, d, Y, W, z_a, z_b, z_c as in Section 2.

The crucial point of the proof is the following definition of α.

Denote by m the smallest integer for which there exists i, $1 \leq i \leq n$, such that u_i is m-cyclic. Denote by $B \subset W$ the set of all $\beta \in C(z_c)$ for which there exists an integer i, $1 \leq i \leq n$, with $\eta_i^c \in F(\beta)$, and, furthermore, $\psi(\beta)$ is m-cyclic. The set B is non-empty, as it contains η_i^c, for any i with $1 \leq i \leq n$, for which u_i is m-cyclic. Choose $\beta_{\max} \in B$ in such a way that

$$|\beta_{\max}| = \max\{|\beta| \mid \beta \in B\},$$

and put

$$\alpha = \psi(\beta_{\max}).$$

Now suppose that u_P is m-cyclic. By the definition, $m \leq d_i$ and every u_i^2 is a factor of u_P, for each $1 \leq i \leq n$. We deduce from Lemma 1.4 and from the minimality of m that every u_i, $1 \leq i \leq n$, is a power of a word of length m. As u_P is, by the assumption, also a power of such a word, the solution φ is cyclic.

To prove that u_P is m-cyclic we first prove a consequence of Lemma 1.4.

Lemma 3.2 *Assume $v \in Y^+$, $\psi(v)$ is m-cyclic and $\eta_i^2 \in F(v)$ for some $1 \leq i \leq n$. Denote by v' the word that results from v when the factor η_i^2 is replaced by η_i^k, $k \geq 1$. Then $\psi(v')$ and u_i are also m-cyclic.*

Proof. Obviously the word u_i^2 is a factor of $\psi(v)$. As $2|u_i| \geq |u_i|+m$, by Lemma 1.4, the word u_i is $\gcd(m, d_i)$-cyclic. The minimality of m yields $\gcd(m, d_i) = m$ and from the construction of v' we deduce that $\psi(v')$ is m-cyclic. □

The proof of the Theorem 3.1 will be completed by following Lemma.

Lemma 3.3 *The word u_P is m-cyclic.*

Proof. As $u_P = (u_1^a \dots u_n^a)^{bc}$ is ad-cyclic and $m < ad$, Lemma 1.4 implies that it is far enough to show $|\beta_{\max}| = |\alpha| \geq 2ad$. Assume, on the contrary, that $|\alpha| < 2ad$.

Consider

$$v \in \psi^{-1}(\alpha) \bigcap W(3, t), \text{ with } 2 \leq t < c.$$

By the definition of $W(3, t)$, there exists an integer j, $1 \leq j \leq n$, such that $\eta_j^t \in F(v)$ and $v \in C(z_t)$. Denote by v' the word that results from v when every factor of the form η_j^t is replaced by η_j^c. The length of v' is less than

$2cd < abcd = |z_c|$ and from its construction we deduce that it belongs to $C(z_c)$. However by Lemma 3.2, v' belongs to B as well, and that contradicts the maximality of $|\beta_{\max}|$. Thus the set $\psi^{-1}(\alpha) \bigcap W(3,t)$ must be empty and $\tilde{\alpha}(3,t) = 0$, as soon as $2 \leq t < c$.

Let us now consider

$$v \in \psi^{-1}(\alpha) \bigcap W(2,t), \text{ with } 3 \leq t < c.$$

We have $v = v_j v_{j+1}$ with $v_j \in F(\eta_j^t)$ and $v_{j+1} \in F(\eta_{j+1}^t)$. As $t \geq 3$, $\eta_j^2 \in F(v_j)$ or $\eta_{j+1}^2 \in F(v_{j+1})$ holds. For symmetrical reasons we can suppose $\eta_j^2 \in F(v_j)$. Put $v' = \eta_j^c v_{j+1}$. Then, as above, $v' \in C(z_c)$, and $\psi(v') \in B$, a contradiction to maximality of $|\beta_{\max}|$ again. Hence $\tilde{\alpha}(2,t) = 0$, $3 \leq t < c$.

Consider finally

$$v \in \psi^{-1}(\alpha) \bigcap W(1,t) \text{ with } \ 4 \leq t < c.$$

As $t \geq 4$, there exists an integer j, $1 \leq j \leq n$, such that $\eta_j^2 \in F(v)$. The word $\eta_j^c \in C(z_c)$ is longer than v, as $t \leq c-1$, and $\psi(\eta_j^c)$ belongs to B. A contradiction with the maximality of $|\beta_{\max}|$ yields $\tilde{\alpha}(1,t) = 0$, $4 \leq t < c$.

Using the above knowledge, Lemma 2.2 and Lemma 2.4 yield the following quantitative equalities:

$$\begin{aligned}
& c(\alpha, u_P) = \\
&= P\tilde{\alpha}(1,1) + \bar{a}(a-1)\tilde{\alpha}(1,2) + \bar{a}(a-2)\tilde{\alpha}(1,3) + \bar{a}\tilde{\alpha}(2,1) + \bar{a}\tilde{\alpha}(2,2) \quad (14)\\
&= P\tilde{\alpha}(1,1) + \bar{b}(b-1)\tilde{\alpha}(1,2) + \bar{b}(b-2)\tilde{\alpha}(1,3) + \bar{b}\tilde{\alpha}(2,1) + \bar{b}\tilde{\alpha}(2,2) \quad (15)\\
&= P\tilde{\alpha}(1,1) + \bar{c}(c-1)\tilde{\alpha}(1,2) + \bar{c}(c-2)\tilde{\alpha}(1,3) + \bar{c}\tilde{\alpha}(2,1) + \bar{c}\tilde{\alpha}(2,2) \\
&\quad + \bar{c}\tilde{\alpha}(1,c) + \bar{c}\tilde{\alpha}(2,c) + \bar{c}\tilde{\alpha}(3,c). \quad (16)
\end{aligned}$$

Substituted $\bar{a}$, $\bar{b}$ and $\bar{c}$ with bc, ac and ab respectively, equalities (14)=(15) and (15)=(16) yield

$$\begin{aligned}
&\tilde{\alpha}(2,1) + \tilde{\alpha}(2,2) = \tilde{\alpha}(1,2) + 2\tilde{\alpha}(1,3), \text{ and} \\
&\tilde{\alpha}(2,1) + \tilde{\alpha}(2,2) = \tilde{\alpha}(1,2) + 2\tilde{\alpha}(1,3) + \tfrac{b}{c-b}(\tilde{\alpha}(1,c) + \tilde{\alpha}(2,c)) + \tilde{\alpha}(3,c)).
\end{aligned}$$

We obtain $\tilde{\alpha}(1,c) + \tilde{\alpha}(2,c) + \tilde{\alpha}(3,c) = 0$. However $\psi^{-1}(\alpha) \bigcap W(k,c)$ must be non-empty for at least one integer k, $1 \leq k \leq 3$, since $\beta_{\max} \in \psi^{-1}(\alpha) \bigcap W$ and some η_i^c, $1 \leq i \leq n$ is a factor of $\beta_{\max}$.

We have found a contradiction to $|\alpha| < 2ad$. □

Theorem 3.1 is now proved. □

4 Test sets

Let L be a set of words from Σ^+. We say that $T \subset L$ is a *test set* of L if and only if any two morphisms g, h to a monoid agree on L, as soon as they agree on T.

Using Theorem 3.1 we can prove following theorem.

Theorem 4.1 *Denote $L = \{x_1^i \dots x_n^i \mid i \in \mathbf{N}\}$, a subset of Σ^+. If $a > 1$ is an integer, then the set $T = \{x_1^k \dots x_n^k \mid k = a, a+1, a+2\}$ is a (three-element) test set of L.*

This is a special case ($n = m$) of the following statement.

Theorem 4.2 *Let $u_1, \dots, u_n,\ v_1, \dots, v_m \in A^+$ be words over an alphabet A and $a > 2$ an integer such that*

$$u_1^k \dots u_n^k = v_1^k \dots v_m^k \tag{17}$$

for $k = a, a+1, a+2$. Then (17) holds for all $k \in \mathbf{N}$.

Proof. First, let $n = 1$ or $m = 1$. Then the statement follows from the Theorem 3.1. Indeed, if e.g. $m = 1$ then

$$(u_1^r \dots u_n^r)^s = (u_1^s \dots u_n^s)^r = v_1^{rs}$$

for all $r, s \in \{a, a+1, a+2\}$.

Suppose $m, n > 1$ and proceed by induction on $m + n$.

If there exist $i, j \in \mathbf{N}$ such that $|u_1 \dots u_i| = |v_1 \dots v_j|$, then the equation (17) splits into two shorter cases.

Suppose finally that no such i, j exist. For symmetrical reasons, we can suppose $|u_1| < |v_1|$. Let $j > 1$ be the integer for which

$$|u_1 \dots u_{j-1}| < |v_1| < |u_1 \dots u_j|.$$

From (17) we deduce that there exist non-empty words $z_1, \dots, z_{a+2}$ of the uniform length $|v_1| - |u_1 \dots u_{j-1}|$, such that

$$u_1^a \dots u_{j-1}^a z_1 \dots z_a = v_1^a \tag{18}$$

$$u_1^{a+1} \dots u_{j-1}^{a+1} z_1 \dots z_{a+1} = v_1^{a+1} \tag{19}$$

$$u_1^{a+2} \dots u_{j-1}^{a+2} z_1 \dots z_{a+2} = v_1^{a+2}. \tag{20}$$

Furthermore

$$z_1 \dots z_a = z_2 \dots z_{a+1} = z_3 \dots z_{a+2},$$

as all three words are a suffix of v_1^a. Thus

$$z_1 = z_2 = \dots = z_{a+2}$$

and we can write (18),(19),(20) as

$$u_1^a \dots u_{j-1}^a z_1^a = v_1^a \tag{21}$$
$$u_1^{a+1} \dots u_{j-1}^{a+1} z_1^{a+1} = v_1^{a+1} \tag{22}$$
$$u_1^{a+2} \dots u_{j-1}^{a+2} z_1^{a+2} = v_1^{a+2}. \tag{23}$$

This is already discussed case $m = 1$ and the Theorem 3.1 implies that all words $u_1, \dots, u_j$, v_1, $z_1, \dots, z_{a+2}$ are powers of a common word, say z. Let $p, q \in \mathbf{N}$ be such that

$$z_1 = z^p,\ u_1 \dots u_{j+1} = z^q,\ v_1 = z^{p+q}.$$

Substituted in (17), we obtain that

$$(z^q)^k u_j^k \dots u_n^k = (z^{p+q})^k v_2^k \dots v_n^k, \tag{24}$$

and thus, cancelled z^q, also

$$u_j^k \dots u_n^k = (z^p)^k v_2^k \dots v_n^k \tag{25}$$

hold for $k = a, a+1, a+2$. By induction, the equality (25), and therefore also (24), hold for all $k \in \mathbf{N}$. □

5 Final observations and acknowledgments

The proof of Theorem 3.1 does not work if $a = 1$, i.e. if $R = \{1, b, c\}$, with $1 < b < c$. The question whether the system of equations (3), $k = b, c$ has a non-cyclic solution remains open. However, the method described in this paper puts some restriction on the eventual non-cyclic solution (see [7]).

The fact that the equation

$$(x_1 \dots x_n)^2 = x_1^2 \dots x_n^2$$

has a non-cyclic solution was used in [4] to construct an independent system of equations over n variables of the size $\Omega(n^4)$. Theorem 3.1 implies that similar approach cannot furnish an independent system of equations of the size $\Omega(n^6)$, in particular not an exponential one.

The present paper was motivated by the question whether the equational system

$$(x_1 \dots x_n)^2 = x_1^2 \dots x_n^2 \tag{26}$$
$$(x_1 \dots x_n)^3 = x_1^3 \dots x_n^3 \tag{27}$$

has a non-cyclic solution in a free semigroup. This question was introduced by Aleš Drápal in a Student algebraic seminar as a problem which Juha Kortelainen was interested in and which has its roots as early as in [1]. As we said, the original question turned out to be more difficult than expected but handling it, author discovered the method described in this paper. Partial results were discussed in the seminar and the remarks and suggestions of the seminar participants have been very helpful to progress of the work. Aleš Drápal has decisively influenced the formulation and formalization of the presented ideas. While writing this paper, author was in direct contact with Juha Kortelainen who helped to put the result in a wider context of word equations and to improve the exposition. Moreover, he pointed out the consequence in the theory of test sets. The content of this paper corresponds to the first part of author's M.D. thesis ([7]), the second part of which is dedicated to the partial results regarding the system (26),(27).

References

[1] K. I. Appel, F. M. Djorup, *On the equation $z_1^n z_2^n \dots z_k^n = y^n$ in a free semigroup*, Trans. Am. Math. Soc. **134** (1968) 461–470.

[2] M. H. Albert, J. Lawrence, *A proof of Ehrenfeucht's conjecture*, Theoret. Comput. Sci. **41** (1985) 121–123.

[3] N. J. Fine, H. S. Wilf, *Uniqueness theorem for periodic functions*, Proc. Am. Math. Soc. **16** (1965) 109–114.

[4] J. Karhumäki, Plandowski W., *On the size of independent systems of equations in semigroups*, in: Proc. MFCS'94, Lecture Notes in Computer Science, Vol. 841 (Springer, Berlin, 1994) 443–452.

[5] M. Lothaire, *Combinatorics on words* (Cambridge University Press, 1983).

[6] I. Hakala and J. Kortelainen, *On the system of word equations* $x_1^i x_2^i \cdots x_m^i = y_1^i y_2^i \cdots y_n^i$ $(i = 1, 2, \ldots)$ *in a free monoid*, Acta Inform. **34** (1997) 217–230.

[7] Š. Holub, *O rovnicích* $(x_1^s \ldots x_n^s)^r = (x_1^r \ldots x_n^r)^s$ *ve volných pologrupách*, M.D. thesis, Charles University, Prague, 1998.

[8] Š. Holub, *A solution of the equation* $(x_1^2 \ldots x_n^2)^3 = (x_1^3 \ldots x_n^3)^2$, in: Contributions to general algebra **11** (Johannes Heyn, Klagenfurt, 1999) 105–111.

[9] J. Kortelainen, *On the system of word equations* $x_0 u_1^i x_1 u_2^i x_2 \ldots u_m^i x_m = y_0 v_1^i y_1 v_2^i y_2 \ldots v_m^i y_m$ $(i = 0, 1, 2, \ldots)$ *in a free monoid*, J. Autom. Lang. Comb. **3** (1998) 43–57.