IN SEARCH FOR A WORD WITH SPECIAL COMBINATORIAL PROPERTIES

ŠTĚPÁN HOLUB

Abstract. In Section 1, notion of canonical and principal solution of an equation in free monoid are discussed. In Section 2 it is proved that if a non-cyclic solution α of the system of equations $(x_1 \dots x_n)^s = x_1^s \dots x_n^s$, $s = 2, 3$, exists, no $\alpha(x_i)$ is a power of a letter. It is also shown that in such a case the shortest non-cyclic solution is principal and of rank two. In Section 3 some similar results are presented without proof.

Introduction

The equality

$$(u_1 \dots u_n)^s = u_1^s \dots u_n^s \tag{0.1}$$

trivially holds for all integers s if every pair u_i, u_j commutes. In a free semigroup it means that all words u_i, $1 \le i \le n$, are powers of a common word v. However, for any k there exists an integer n and words $u_1, \dots, u_n$ such that (0.1) holds just for $s = k$ (and $s = 1$). Take for example $n = 2k - 1$ and

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

with some letters A, B.

The question is whether there exists an n-tuple $u_1, \dots, u_n$ such that (0.1) holds for more that one integer $s > 1$ but does not hold for each $s \in \mathbb{N}$. (It is not difficult to see that if (0.1) holds for each $s \in \mathbb{N}$, the $u_1, \dots, u_n$ are powers of a common word.) It was shown (see [3]) that (0.1) holds for all $s \in \mathbb{N}$ as soon as it holds for three integers greater than one. The question whether there exists an n-tuple of words $u_1, \dots, u_n$ such that (0.1) holds for exactly two integers greater than one, remains open. We shall show a condition that such an eventual n-tuple must satisfy.

1. Equations and their solutions

In this section we introduce some concepts regarding equations in free semigroups and their solutions.

1.1. **Basic notions.** Let A be a finite *alphabet*. Elements of A are called *letters* and sequences of letters are called *words*. The sequence of length zero is called the *empty word*, denoted ε. The set of all words (all non-empty words resp.) is denoted by A^* (A^+, 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

Partially supported by the University Development Fund of Czech Republic.

word u is a factor of a word v if and only if there exist words z, $z' \in A^*$ such that $v = zuz'$.

By a *cyclic factor* of v we shall understand every factor u of vv with $|u| \leq |v|$. 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).An instance of a cyclic factor will be 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 cyclic factors of v will be denoted by $C(v)$.

Let X be a finite set of unknowns. Every

$$(e, e') \in X^+ \times X^+$$

we shall call an *equation* in unknowns from X. We shall always suppose that X contains only unknowns occuring in (e, e'). For a particular equation (e, e') we shall often use the suggestive notation $e = e'$.

We say that a morphism $\alpha : X^+ \to A^+$ is a *solution* of the system of equations $S \subseteq X^+ \times X^+$ in the semigroup A^+, if and only if for every $(e, e') \in S$ the equality $\alpha(e) = \alpha(e')$ holds. By *alph*(α) we denote the set of letters occuring in $\alpha[X] = \{\alpha(x); x \in X\}$. We shall always suppose that *alph*$(\alpha) = A$. Two systems of equations S, S' are called *equivalent* if and only if they have the same set of solutions.

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

We say that two solutions $\alpha : X^+ \to A^+$ and $\beta : X^+ \to B^+$ are isomorphic if and only if there exists a bijection $\theta : A \to B$ such that $\beta = \theta \circ \alpha$.

1.2. **Ranks.** A subset S of a free semigroup A^+ closed under the operation of concatenation is called subsemigroup of A^+. Subsemigroup S is not necessarily free. For example the subsemigroup of $\{a, b\}^+$ generated by elements $\{a, ab, ba\}$ is not free as $a(ba) = (ab)a$. However, as the set of free subsemigroups is closed under intersection (see [2], p.6), there exists the smallest free subsemigroup containing a subset $S \subset A^+$, called *free hull* of S. The cardinality of the basis of the free hull is called the *rank* of S. The rank of a morphism $\alpha : X^+ \to A^+$ is the rank of the set $\alpha[X]$. The basis of the free hull of the set $\alpha[X]$ is called the basis of the morphism α. Finally we say that the rank of an equation is the maximal rank of its solutions. The rank of an equation is one if and only if the equation admits only cyclic solutions.

1.3. **Canonical solution.** Let $\alpha : X^+ \to A^+$ be a solution of an equation (e, e'). Suppose $X = \{x_1, \ldots, x_n\}$. The n-tuple $(d_1, \ldots, d_n)$, with $d_i = |\alpha(x_i)|$, shall be called the *type* of α. The solution α is called *canonical solution of the type* $(d_1, \ldots, d_n)$(or simply *canonical*) if and only if for every solution $\beta : X^+ \to B^+$ of (e, e') and every mapping $\theta : B \to A$, such that $\alpha = \theta \circ \beta$, the mapping θ is a bijection. In other words, α is canonical if and only if the cardinality of *alph*(α) is maximal among all solutions of (e, e') of the same type. All non-canonical solutions of given type result from a canonical solution by identification of some letters. It is easy to see that all canonical solutions are isomorphic.

The notion of canonical solution was introduced by Appel and Djorup in [1], for the particular equation $z_1 \ldots z_n = y^n$. The definition they use is different from the above presented and is more intuitive. In fact it describes the construction of the canonical solution of given type and can be generalized as follows. Let $(d_1, \ldots, d_n)$ be the type for which we wish to construct the canonical solution of an equation

(e, e') in unknowns $\{x_1, \ldots, x_n\}$. We introduce alphabet Y consisting of new letters $\eta_{i,j},\ 1 \leq i \leq n,\ 1 \leq j \leq d_i$ and define morphism $\psi : X^+ \to Y^+$ by equalities

$$\psi(x_i) = \eta_{i,1} \ldots \eta_{i,d_i},\ 1 \leq i \leq n.$$

Obviously we suppose that $|\psi(e)| = |\psi(e')|$, otherwise the equation has no solution of the type $(d_1, \ldots, d_n)$. We shall call the equation $(\psi(e), \psi(e'))$ *the type equation associated with* (e, e') *and* $(d_1, \ldots, d_n)$.

Let $\sim$ be the smallest equivalence relation on Y such that $\eta_{i,j} \sim \eta_{k,l}$, as soon as $\psi(e) = v\eta_{i,j}w$ and $\psi(e') = v'\eta_{l,k}w'$ for some $v, v', w, w' \in Y^*$ such that $|v| = |v'|$, $|w| = |w'|$. Let A be the set of equivalence classes of $\sim$ and $\pi : Y^+ \to A^+$ the natural projection $\pi(\eta_{i,j}) = [\eta_{i,j}]_\sim$. Then $\pi \circ \psi : X^+ \to A^+$ is a canonical solution of the type $(d_1, \ldots, d_n)$.

Let $\alpha : X^+ \to A^+$ be a canonical solution. Denote by L the set of all left letters, i.e. all letters $a \in A$ such that $\alpha(x) = av$, for some $x \in X$ and $v \in A^+$. Similarly denote by R the set of all right letters. Denote by H the set of all words $v \in A^+$, such that v begins with a left letter, ends with a right letter and does not contain any other left or right letter. (If $a \in R \bigcap L$, than $a \in H$). It can be proved (see [1]) that H is the basis of α.

1.4. **Principal solution.** On the set of all solutions of an equation (e, e') we define a partial ordering $\leq$. Given two solutions $\alpha : X^+ \to A^+$ and $\beta : X^+ \to B^+$ we say that $\alpha \leq \beta$ if and only if there exists a morphism $\theta : A^+ \to B^+$ such that $\beta = \theta \circ \alpha$. If θ is an isomorphism (i.e. it is generated by a bijection $A \to B$) then both $\alpha \leq \beta$ and $\beta \leq \alpha$, as $\alpha = \theta^{-1} \circ \beta$. Any minimal element of this ordering is called *principal solution* of (e, e'). In other words a solution α is principal if and only if θ is an isomorphism as soon as $\theta \circ \alpha$ is a solution of (e, e'). It results that every principal solution is canonical, but not vice versa. All canonical solutions $\beta : X^+ \to B^+$ can be expressed like $\theta \circ \alpha$, where $\alpha : X^+ \to A^+$ is a principal solution and $\theta : A^+ \to B^+$ is a morphism such that for a_1,$a_2 \in A$, $a_1 \neq a_2$, the words $\theta(a_1)$, $\theta(a_2)$ have no common letter.

The rank of a principal solution $\alpha : X^+ \to A^+$ is equal to the cardinality of A. Indeed, if $\{v_1, \ldots, v_m\}$ is the basis of α, we can introduce an alphabet B, consisting of new letters $b_1 \ldots b_n$, and define a morphism $\theta : B^+ \to A^+$ by equalities $\theta(b_i) = v_i$, $1 \leq i \leq n$. Then $\alpha = \theta \circ \beta$ is a solution of (e, e') and θ is an isomorphism.

One can see that a solution $\alpha : X^+ \to A^+$ is principal if and only if it is canonical and A is the basis of α. In other words α is principal if and only if the following condition is satisfied: Let $\beta : X^+ \to B^+$ be a canonical solution of the same type as α. Then every $b \in B$ is both right and left letter.

2. Shortest counterexample

Consider now following system of equations

$$\begin{aligned} (x_1 \ldots x_n)^2 &= x_1^2 \ldots x_n^2, \\ (x_1 \ldots x_n)^3 &= x_1^3 \ldots x_n^3, \end{aligned} \tag{2.1}$$

in unknowns $X = \{x_1, \ldots, x_n\}$. Henceforward we shall suppose that there exists a positive integer n such that the system (2.1) has a non-cyclic solution (i.e. its rank is greater than one) and let n be the smallest one. Surely $n > 2$, because all equations (e, e') in two unknowns, such that $e \neq e'$, have only cyclic solutions in free semigroups (see e.g. [2], p.164). We say that α is a *shortest counterexample* if and only if it is a non-cyclic solution of (2.1) and for every non-cyclic solution α' the inequality

$$|\alpha(x_1 \dots x_n)| \leq |\alpha'(x_1 \dots x_n)|$$

holds.

Lemma 2.1. *Let α be a shortest counterexample. Then it is a principal solution of rank two.*

Proof. Note that ever every solution of the same type as α is a shortest counterexample. First, suppose that $\alpha : X^+ \to A^+$ is a canonical solution and let C be a basis of α. We can understand α like a morphism $X^+ \to C^+$ and, thank to the minimality of $|\alpha(x_1 \dots x_n)|$, we have $C = A = \{a_1, \dots, a_m\}$. Suppose that $rank(\alpha) = card(A) = m$ is greater than two. Denote by A' the set $\{a_1, a_2\}$ and define a morphism $\theta : A^+ \to (A')^*$ by

$$\theta(a_i) = \begin{cases} a_i & 1 \leq i \leq 2 \\ \\ \varepsilon & 3 \leq i \leq m. \end{cases}$$

If we omit all x_i such that $\theta \circ \alpha(x_i) = \varepsilon$ we get a solution $\alpha' = \theta \circ \alpha : X^+ \to (A')^+$ of (2.1) with some $n' \leq n$. If α' is not cyclic, we have a contradiction with the fact that α is a shortest counterexample. Suppose that α' is cyclic, and let $v = b_1 \dots b_l$, $l \geq 2$, $b_i \in A'$, $1 \leq i \leq l$, be the shortest word such that all $\alpha'(x_i)$, $1 \leq i \leq n'$, are a power of v. It is not difficult to see that α' is canonical (as α is) and therefore $b_i \neq b_j$, $1 \leq i < j \leq l$. It follows that b_1 is not the final letter of any $\alpha(x_i)$, a contradiction with the fact that A is the basis of α. We have proved that if a shortest counterexample is canonical, it is of rank two.

Suppose now, for a contradiction, that $\alpha : X^+ \to A^+$ is a general shortest counterexample that is not a principal solution. Let $\beta : X^+ \to B^+$ be a solution of (2.1) and $\theta : B^+ \to A^+$ a morphism, such that $\alpha = \theta \circ \beta$ and θ is not an isomorphism. Clearly

$$|\alpha(x_1 \dots x_n)| \geq |\beta(x_1 \dots x_n)|$$

and the equality must hold, because α is a shortest counterexample and β is not cyclic. We deduce that θ maps B onto A. Suppose that θ is not injective. Then the cardinality of B must be at least three. As the cardinality of the alphabet of a canonical solution is maximal among all solutions of given type, the canonical solution of the type $(d_1, \dots, d_n)$, with $d_i = |\alpha(x_i)| = |\beta(x_i)|$, is of a rank greater then two and in the same time it is a shortest counterexample, a contradiction with what we proved above. Therefore any shortest counterexample is principal, it implies it is canonical it implies it is of rank two. □

Lemma 2.2. *Let $\alpha : X^+ \to A^+$, $A = \{a, b\}$, be a shortest counterexample. Then for all $1 \leq i \leq n$, the word $\alpha(x_i)$ contains both letter a and b.*

Proof. First put

$$u_1 = (x_1 \dots x_n)^6,\ u_2 = (x_1^2 \dots x_n^2)^3,\ u_1 = (x_1^3 \dots x_n^3)^2,$$

and note that the system (2.1) is equivalent to the system

$$\begin{aligned} &(u_1, u_2), \\ &(u_1, u_3). \end{aligned} \tag{2.2}$$

Put $d_i = |\alpha(x_i)|$, $1 \leq i \leq n$. Define Y and $\psi : X^+ \to Y^+$ in such a way that

$$\begin{aligned} &(\psi(u_1), \psi(u_2)),\\ &(\psi(u_1), \psi(u_3)) \end{aligned} \tag{2.3}$$

are the type equations associated with (2.2) and $(d_1 \dots d_n)$. Denote

$$y_i = \eta_{i,1} \dots \eta_{i,d_i},\ 1 \leq i \leq n,$$

and

$$w_i = \psi(u_i),\ 1 \leq i \leq 3.$$

Denote by $\pi : Y^+ \to A^+$ the morphism satisfying $\pi(y_i) = \alpha(x_i)$. Such a morphism is determined uniquely and $\pi(\eta) \in A$ for all $\eta \in Y$. It implies that $|\pi(w)| = |w|$. Denote $F = \bigcup_{1 \leq i \leq 3} C(w_i)$ the set of all factors that can be found in equations (2.3). We will proceed by contradiction. Suppose (without lack of generality) that for some i, $1 \leq i \leq n$, $\alpha(x_i)$ is a power of a. Let m be the biggest integer for which there exists a word $w \in F$ of length m such that $\pi(w) = ba^m b$, and y_i^3 is a factor of w for some $1 \leq i \leq n$. Let Z be the set of all words $w \in F$ such that $\pi(w) = ba^m b$. If $w \in Z$ then

$$|w| = m + 2 \leq |y_1 \dots y_n| = \sum_{i=1}^{n} d_i.$$

Now we shall define a disjoint factorization of Z, according to the complexity of its elements. Let $w \in Z$. Denote by $i(w)$ the number of different first indices of letters occuring in w. It is the number of different words y_i affected by w. Denote by $\sigma(w)$ the minimal exponent k such that w is a cyclic factor of ${y^k}_1 \dots y_n^k$. Obviously $\sigma(w) \leq 3$ for $w \in Z$. Denote by $W(i,j)$, $1 \leq i \leq 2$, $1 \leq j \leq 3$, the set of all words $w \in Z$, such that $i(w) = i$ and $\sigma(w) = j$. Also denote by $W(3,j)$ the set of all words $w \in Z$, such that $i(w) \geq 3$ and $\sigma(w) = j$. It follows from definitions that $W(i,j)$, $1 \leq i \leq 3$, $1 \leq j \leq 3$, is really a disjoint factorization of Z.

The definition of sets $W(i,j)$ is motivated by the fact that w, w' belong to the same set if and only if, in all three words w_1, w_2, w_3, the number of cyclic instances of w is the same as the number of cyclic instances of w'. Indeed if we denote $o(i,j,k)$ the number of cyclic instances of a word $w \in W(i,j)$ in the word w_k, we can easily verify following values:

$$\begin{array}{lcl}
(1,2,1)=(1,3,1)=(1,3,2)=(2,2,1)=(2,3,1)=(2,3,2)= & & \\
(3,1,2)=(3,1,3)=(3,2,1)=(3,2,3)=(3,3,1)=(3,3,2) & = & 0 \\
(1,3,3)=(2,1,3)=(2,2,3)=(2,3,3)=(3,3,3) & = & 2 \\
(1,2,2)=(2,1,2)=(2,2,2)=(3,2,2) & = & 3 \\
(1,2,3) & = & 4 \\
(1,1,1)=(1,1,2)=(1,1,3)=(2,1,1)=(3,1,1) & = & 6.
\end{array}$$

Suppose that $w \in W(3,1)$. Then w has at least one factor $\eta_{i-1,d_{i-1}} y_i \eta_{i+1,d_{i+1}}$, with $1 \leq i \leq n$, and $i-1$, $i+1$ considered modulo n. For such an i we have $\pi(y_i) = a^l$, $l \geq 1$. If we substitute in the word w all such words y_i by y_i^3, we get a word w' such that $\pi(w') = ba^p b$, $p > m$, a contradiction with the maximality of m. It follows that $W(3,1)$ is empty. Similarly we can see that $W(3,2)$, $W(2,2)$, $W(2,3)$, $W(1,3)$ are also empty.

Denote by P the number of cyclic occurences of the word $ba^m b$ in the word $u = \alpha(u_1) = \alpha(u_2) = \alpha(u_3)$. Looking at a word w_k, $1 \leq k \leq 3$, we can see that P

is equal to the total number of cyclic instances of elements from Z in w_k. Thank to the disjoint factorization of Z, we can express P in three ways (for $1 \leq k \leq 3$) like a sum

$$\sum_{1\leq i,j\leq 3} |W(i,j)|o(i,j,k).$$

Using all above knowledge we get equalities

$$\begin{aligned} P &= 6|W(1,1)| + 6|W(2,1)| = \\ &= 6|W(1,1)| + 3|W(2,1)| + 3|W(1,2)| = \\ &= 6|W(1,1)| + 2|W(2,1)| + 4|W(1,2)| + 2|W(3,3)|. \end{aligned} \tag{2.4}$$

From these equalities easily results $|W(3,3)| = 0$, a contradiction with the definition of the set Z. □

3. Further results and remarks

The method used to prove Lemma 2.2 is described in the most general form in [3]. Thank to that method, some other results were achieved. First, the statement of Lemma 2.2 is valid for all systems of equations

$$\begin{aligned} (x_1 \dots x_n)^r &= x_1^r \dots x_n^r, \\ (x_1 \dots x_n)^s &= x_1^3 \dots x_n^s, \end{aligned} \tag{3.1}$$

with $r > s > 1$.

In the proof of Lemma 2.2 the fact that α is a shortest counterexample was not used. For a general solution the lemma can be reformulated as follows.

Theorem 3.1. *Let $\alpha : X^+ \to A^+$ be a solution of (3.1) and v be an element of the basis of α. Then v is a factor of each $\alpha(x_i)$, $1 \leq i \leq n$.*

The proof of this theorem is mutatis mutandis the same as that of Lemma 2.2.

The proof of following lemma is a bit technical (see [4]).

Lemma 3.2. *Let $\alpha : X^+ \to A^+$ be a solution of (3.1) with $A = \{a,b\}$. Let $v = ba^m b$, $m \geq 1$, be a cyclic factor of $\alpha(x_1 \dots x_n)$. Then v is a cyclic factor of every $\alpha(x_i)$, $1 \leq i \leq n$.*

Finally, the most important result (see [3]), mentioned in the Introduction, is that the rank of the equational system

$$(x_1^{k_1} \dots x_n^{k_1})^{k_2 k_3} = (x_1^{k_2} \dots x_n^{k_2})^{k_1 k_3} = (x_1^{k_3} \dots x_n^{k_3})^{k_1 k_2},$$

$k_1 > k_2 > k_3 > 1$, is one.

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), pp. 461–470.
2. M. Lothaire, *Combinatorics on words*, Cambridge University Press, 1983.
3. Š. Holub, *Local and global cyclicity in free monoids*, submitted.
4. Š. Holub, *O rovnicích $(x_1^s \dots x_n^s)^r = (x_1^r \dots x_n^r)^s$ ve volných pologrupách*, M.D. thesis, Charles University, Prague, 1998.

Department of mathematics, Charles University, Sokolovská 83, 186 75 Praha
E-mail address: holub@karlin.mff.cuni.cz