On Conjugacy of Languages

Supported by the Academy of Finland under grant 44087.

Julien Cassaigne

Institut de Math. de Luminy, Luminy Case 907,
F–13288 Marseille Cedex 9, France
(cassaign@iml.univ-mrs.fr)

Juhani Karhumäki

Dept. of Math. and TUCS, Univ. of Turku,
FIN–20014 Turku, Finland
(karhumak@cs.utu.fi)

Ján Maňuch

TUCS and Dept. of Math., Datacity, Lemminkäisenkatu 14A,
FIN–20520 Turku, Finland
(manuch@cs.utu.fi)

Turku Centre for Computer Science
TUCS Technical Report No 422
October 2001

ISBN 952-12-0891-0
ISSN 1239-1891

Abstract

We say that two languages X and Y are conjugated if they satisfy the *conjugacy equation* $XZ = ZY$ for some language Z. We study several problems associated to this equation. For example, we characterize all sets which are conjugated via a two-element biprefix set Z, as well as all two-element sets which are conjugates.

TUCS Research Group
Mathematical Structures in Computer Science

1 Introduction

Since a seminal paper of Makanin in 1976, cf. [Ma], word equations have been studied quite intensively. Despite of the fact that many fundamental problems, such as the exact complexity of the satisfiability problem, cf. [Pl], or the maximal size of independent systems of equations in n variables, are not solved, cf. [HKP], one can say that there exists a deep and rich theory on word equations.

If language equations, as extensions of word equations, are considered the situation changes drastically: almost nothing is known about those. The goal of this paper is to initiate a research on a particular language equation, namely on the conjugacy equation $XZ = ZY$. We point out differences from the word case, solve it in certain simple cases, as well as formulate some interesting open problems.

Recently a special case of the conjugacy equation, namely the commutation equation $XZ = ZX$ for languages has been studied in a number of papers. In certain cases, for example when X is a two-element set or X is a prefix set, cf. [CKO] and [Ra], it is completely solved: Z must be of the form $Z = \cup_{i \in I} X^i$ with $I \subseteq \mathbb{N}$. On the other hand, the answer to an old Conway's Problem, cf. [Co], asking whether the (unique) maximal set Z commuting with a given rational X is also rational, is known only in some very special cases, like in the cases when X is a three-element set or X is an ω-code, cf. [KP], [HP] or [Ka] for a survey. Consequently, the conjugacy equation for languages cannot be easy.

Let us recall that the conjugacy equation $xz = zy$ for words has a well known general solution:

$$\exists p, q \in \Sigma^* \text{ such that } x = pq,\ y = qp \text{ and } z \in (pq)^* p.$$

As is immediate to check the words can be replaced by languages (or finite languages) to obtain solutions of the conjugacy equation $XZ = ZY$ for languages: triples

$$X = PQ,\ Y = QP \text{ and } Z = \bigcup_{i \in I} (PQ)^i P$$

for $P, Q \subseteq \Sigma^*$ and $I \subseteq \mathbb{N}$, are solutions. They are referred to as *word type solutions*. However, not all solutions are of word type even in the case when Z is a two-element prefix set, cf. Examples 1 and 2.

We associate with the conjugacy equation $XZ = ZY$ the following four different basic problems:

Problem 1. Given a set $Z \subseteq \Sigma^+$, describe all pairs (X, Y) such that $XZ = ZY$, i.e., X and Y are conjugated via Z.

Problem 2. Given sets $X, Y \subseteq \Sigma^+$, describe all sets Z such that $XZ = ZY$, i.e., X and Y are conjugated via Z.

Problem 3. Describe all sets $X, Y \subseteq \Sigma^+$ which are conjugates, i.e., there exists a non-empty set Z such that $XZ = ZY$.

Problem 3 can be stated as a decision problem as well:

Problem 4. Decide whether two finite sets are conjugates, i.e., there exists a non-empty set Z such that $XZ = ZY$.

What we are able to say about these problems is as follows. In Section 3 we solve Problem 1 for two-element biprefix codes Z, as well as show, via examples, that for arbitrary two-element sets the problem looks essentially more complicated. In Section 4 we characterize when two-element sets X and Y are conjugates, thus giving an implicit solution to this special case of Problem 3.

Finally, we emphasize that we consider language equations as generalizations of word equations, that is to say as equations with only one associative operation, the product. For certain special equations with two operations — union and product — a nice theory can be built based on a general fixed point approach. Computing a rational expression for a given finite automaton is an example of that, cf. [Ei] or [Le] for a general treatment.

2 Preliminaries

Let Σ be a finite alphabet, and Σ^* (resp. Σ^+) the free monoid (resp. semigroup) generated by Σ. We use lowercase letters to denote words, i.e., elements of Σ^*, and capital letters to denote languages, i.e., subsets of Σ^*. Mostly we consider finite languages. The empty word is denoted by 1, and the length of a word w by $|w|$. For a set X by $|X|$ we mean its cardinality. Occasionally we consider infinite words, i.e., elements of Σ^ω or infinite powers of languages.

By the *conjugacy equation* we mean the equation

$$XZ = ZY . \tag{1}$$

As is well known, in the case of words it characterizes when two words x and y are conjugates, i.e., of the forms $x = pq$ and $y = qp$ for some words p and q (and moreover in this case $z \in (pq)^*p$). For languages we take it as a definition of conjugacy. We say that languages X and Y are *conjugates*, in symbols $X \sim Y$, if there exists a language Z such that (X, Y, Z) is a solution of (1). If this is the case we also say that X and Y are *conjugated via* Z, and we write $X \sim_Z Y$.

Obviously, if $X_1 \sim_Z Y_1$ and $X_2 \sim_Z Y_2$ then also $X_1 \cup X_2 \sim_Z Y_1 \cup Y_2$. Consequently, for a given Z there exists the unique solution of (1) which is maximal with respect to both components. We call this solution the *maximal* solution of (1). Dually, we call a solution (X, Y) of (1), for a given Z, *minimal*, if there are no sets $X_1, X_2 \subseteq X$ and $Y_1, Y_2 \subseteq Y$ such that

$$X = X_1 \cup X_2, \quad Y = Y_1 \cup Y_2, \quad (X_1, Y_1) \neq (X, Y), \quad (X_2, Y_2) \neq (X, Y),$$
$$X_1 Z = Z Y_1 \quad \text{and} \quad X_2 Z = Z Y_2 \,. \tag{2}$$

Of course, there might be several minimal solutions. Moreover, all solutions, including the maximal one, are obtained as component-wise unions of minimal solutions. We say that a solution (X_1, Y_1) is *contained* in a solution (X, Y), if $X_1 \subseteq X$, $Y_1 \subseteq Y$ and $(X_1, Y_1) \neq (X, Y)$.

We mainly concentrate to study (1) in the cases when

(i) Z or X and Y are two-element sets; or

(ii) Z is a biprefix code, i.e., no word of Z is a prefix or suffix of another word of Z.

One can easily prove the following simple facts which we will use many times later on.

Proposition 1. *The sets X, Y and Z satisfy the following properties:*

a. for every positive integer n, $X^n Z = Z Y^n$;

b. $Z \subseteq \mathrm{Pref}(X^+) \cap \mathrm{Suff}(Y^+)$;

3 The conjugacy via a given Z

In this section we study Problem 1, i.e., given a set Z we would like to describe all pairs of sets (X, Y) such that $XZ = ZY$.

If Z has only one element z, then each element of X is conjugated via z to an element of Y. Consequently, minimal pairs are pairs of singletons, $(\{x\}, \{y\})$, such that $xz = zy$: this is the word case, so that $x = pq$, $y = qp$ and $z = (pq)^m p$ for some integer $m \geq 0$ and words p and q.

If (X, Y) is a union of singleton pairs $(\{x_i\}, \{y_i\})_{i \in I}$ such that $m = 0$ for all of them, then $p_i = z$ for all i, and if $Q = \{q_i : i \in I\}$, then $X = zQ = ZQ$ and $Y = Qz = QZ$. Conversely, for any Z and Q, $X = ZQ$ and $Y = QZ$ is a solution. On the other hand, the union of minimal solutions for which $m \neq 0$ cannot usually be described in such a compact way. As a conclusion we obtain:

Proposition 2. *If $Z = \{z\}$ is a singleton, then the maximal solution is $X = Z\Sigma^* \cup \{pq : \exists m > 0, z = (pq)^m p\}$ and $Y = \Sigma^* Z \cup \{qp : \exists m > 0, z = (pq)^m p\}$.*

As we already noted the conjugacy equation (1) has always word type solutions

$$X = PQ, \quad Y = QP, \quad \text{and} \quad Z = \bigcup_{i \in I} (PQ)^i P$$

for $P, Q \subseteq \Sigma^*$ and $I \subseteq \mathbb{N}$. In some cases these are the only possible solutions. For example, if the sets X and Y are uniform, i.e., consist of words of a fixed length, then the equation (1) has only word type solutions. This follows from the fact that the monoid of uniform non-empty languages is free:

Proposition 3. *If sets X and Y are uniform, then there exist sets $P, Q \subseteq \Sigma^*$ and $I \subseteq \mathbb{N}$ such that $X = PQ$, $Y = QP$ and $Z = \cup_{i \in I} (PQ)^i P$.*

However, not all solutions are of the word type, even for unary Z:

Example 1. $Z = \{aa\}$, $X = Y = \{a, aaa\}$ is a solution, but not a minimal one.

The corresponding example for binary Z, where Z is a prefix code, is as follows:

Example 2. $Z = \{a, ba\}$, $X = \{a, ab, abb, ba, babb\}$, $Y = \{a, ba, bba, bbba\}$ is a solution. This is a minimal solution, but not of word type. Indeed, the only solutions contained in (X, Y) are: $X_1 = Y_1 = \{a, ba\}$ and $X_2 = \{abb, babb\}$, $Y_2 = \{bba, bbba\}$, and their union does not form the whole (X, Y).

However, if we set $Q' = \{1, bb\}$ and $Q = \{1, b, bb\}$, then we have $ZQ' \subseteq X \subseteq ZQ$ and $Y = QZ = Q'Z$. Note also that $|X| \neq |Y|$.

In general, if there exist three sets P, Q', Q such that $Z = \cup_{i \in I} (PQ)^i P$ for some $I \subseteq \mathbb{N}$ and $PQ' \subseteq X \subseteq PQ$, $QP \subseteq Y \subseteq Q'P$, then this is a solution. This follows since the conditions imply that $PQ'P = PQP$.

Example 2 shows one interesting property of the relation $\sim$ for languages.

Claim 1. *The relation $\sim$ for language is reflexive, transitive, but not symmetric.*

Proof. It is easy to check reflexivity and transitivity. To prove that $\sim$ is not symmetric, consider the sets X, Y, Z from Example 2. Assume for a contradiction that there exists a non-empty set W such that $WX = YW$. Take a $w \in W$. It can be written in the form

$$w = b^{n_0} a b^{n_1} a \ldots a b^{n_k},$$

where $k, n_0, \ldots, n_k \geq 0$. Now, $wab = b^{n_0} a b^{n_1} a \ldots a b^{n_k} ab \in WX = YW$, which is possible only if $n_0 \in \{0, 1, 2, 3\}$ and $b^{n_1} a \ldots a b^{n_k} ab \in W$. Repeating the same argument several times we get that $b(ab)^k \in W$. Now again, $bbbab(ab)^k \in YW = WX$, which implies that $bbb(ab)^k \in W$. Since $bbb \notin \mathrm{Suff}(X^+)$, we have also $bbb(ab)^k \notin \mathrm{Suff}(X^+)$. But this is a contradiction, since by Proposition 1b, $W \subseteq \mathrm{Suff}(X^+)$. $\square$

On the other hand the relation $\sim$ for words is clearly equivalence relation, i.e., it is reflexive, transitive and symmetric.

3.1 The case when Z is a finite biprefix set.

We now assume that Z is a biprefix code. Then both products XZ and ZY are unambiguous, i.e., for all $(x, z) \in X \times Z$, there exists exactly one pair $(z', y) \in Z \times Y$ such that $xz = z'y$, and conversely. This allows a more detailed analysis.

Let X, Y, Z with Z a biprefix code be a solution of the conjugacy equation. This yields instances of word equations of types:

$$xz = z'y \quad \text{with } x \in X,\ y \in Y \text{ and } z, z' \in Z. \tag{3}$$

We call such an instance *overlapping* or *non-overlapping* depending on whether $|x| < |z'|$ or $|x| \geq |z'|$, respectively.

Now, let $Z = \{z_i\}_{i \in I}$ and $x \in X$ fixed. For all $k \in I$ we can write $xz_k = z'_k y_k$. We claim that if one of these instances, say $xz_i = z'_i y_i$, is non-overlapping, so are all, and moreover all z'_k's are equal. Indeed, if $xz_j = z'_j y_j$, then z'_j is a prefix of xz_j and since z'_i is a prefix of x, necessarily $z'_i = z'_j$; otherwise Z would not be biprefix.

The above allows us to write $X = X_1 \cup X_2$ and $Y = Y_1 \cup Y_2$, where X_1 and Y_1 consist of exactly those x- and y- values of (3) which come from overlapping instances. Then, clearly, $X_1 Z \subseteq ZY_1$, and symmetrically $ZY_1 \subseteq X_1 Z$. Therefore $X_1 Z = ZY_1$, and similarly $X_2 Z = ZY_2$.

As a conclusion we obtain:

Proposition 4. *Let Z be a biprefix set. The minimal solutions consist entirely of x- and y- values of either overlapping or non-overlapping instances of* (3).

We proceed by analysing the two disjoint cases of Proposition 4. In the non-overlapping case, z' is uniquely determined by x, and symmetrically z is uniquely determined by y. Moreover, for a given $x \in X_1$, there exists a unique q such that $x = z'q$ and $y = qz$. Further, we can choose arbitrary $z \in Z$, and therefore $qZ \subseteq Y_1$. Now, by denoting

$$Q = \{q : \ x = z'q, z' \in Z, x \in X_1\},$$

we see that $QZ \subseteq Y_1$. But also the reverse inclusion $Y_1 \subseteq QZ$ holds, since any $y \in Y_1$ can be written in the form $y = qz$ with $q \in Q$ and $z \in Z$.

So we obtain:

Proposition 5. *Let Z be a finite biprefix code. The solutions of* (1) *corresponding to non-overlapping instances of* (3) *are of the form: $Y_1 = QZ$ and $X_1 = ZQ$, for some $Q \subseteq \Sigma^*$. Conversely, every pair (X_1, Y_1) of this form is conjugated via Z.*

The message of the above proposition is that solutions obtained from non-overlapping instances of (3) are of word type. For the other solutions this need not be the case even in the case when Z is a biprefix code as shown in the following examples.

Example 3. $Z = \{aaa, aabaa\}$, $X = \{a, aab\}$, $Y = \{a, baa\}$ is a solution of (1) corresponding to overlapping instances. It is not of word type.

Example 4. $Z = \{aabaabaa, aabaaabaa\}$, $X = \{aab, aaba\}$, $Y = \{baa, abaa\}$ is another similar solution, as in Example 3, not of word type.

We are not able to characterize all solutions corresponding to overlapping instances of (3), except in the case when $|Z| = 2$. This is done in Section 3.2, as an application of the following general considerations.

Again we assume that Z is a biprefix code and $X \sim_Z Y$. We assume that neither X nor Y contains the empty word. This can be assumed since $(\{1\}, \{1\})$ is always a minimal solution and if one of those sets contains 1 so does the other due to the fact that Z is a biprefix code. By Proposition 1a, $X^n Z = ZY^n$ for all n. Now, when n tends to infinity, we have $ZY^\omega \subseteq X^\omega$ and ${}^\omega XZ \subseteq {}^\omega Y$. Hence, any element of Z is a prefix of a word in X^ω and a suffix of a word in ${}^\omega Y$. Conversely, any word in X^ω has an element of Z as a prefix, and this element is unique since Z is a prefix code. Indeed, take an infinite word $\tilde{x} = x_1 x_2 \cdots \in X^\omega$ and an arbitrary $z \in Z$. Since $X^n Z = ZY^n$ for all n, there are words $z' \in Z$ and $y_1, \ldots, y_n \in Y$ such that $x_1 \ldots x_n z = z' y_1 \ldots y_n$. If we take n such that $n \min_{y \in Y} |y| \geq |z|$, then z' is a prefix of $x_1 \ldots x_n$ which is a prefix of $\tilde{x}$. Since Z is a prefix code, such z' is unique. Similarly, any word in ${}^\omega Y$ has a unique element of Z as a suffix.

Now, fix an x in X, and let z be the element of Z which is a prefix of x^ω. Then $xz = z'y$ for some $z' \in Z$ and $y \in Y$. But z' is a prefix of xz which is a prefix of x^ω, and so by the uniqueness $z' = z$. Thus $x^n z = zy^n$ for all n and z is also the unique suffix of ${}^\omega y$.

We have defined two maps, $f : X \to Y$, $x \mapsto y$, and $g : X \to Z$, $x \mapsto z$. Moreover, f is a bijection, because y is uniquely defined from x, and symmetrically starting from y we find an x' such that $x'z = zy = xz$, implying that $x' = x$.

Lemma 1. *If Z is a biprefix code, then there exist two unique maps: $f : X \to Y$ and $g : X \to Z$ such that for every $x \in X$, the elements $y = f(x)$ and $z = g(x)$ satisfy $xz = zy$. Moreover, the map f is a bijection.*

Proof. Above we have shown that such maps exist. Now we prove that they are unique. Hence, assume for contrary that for some $x \in X$ there are $z_1, z_2 \in Z$ and $y_1, y_2 \in Y$ such that $xz_1 = z_1 y_1$ and $xz_2 = z_2 y_2$. Since for any integer n, $x^n z_1 = z_1 y_1^n$ and $x^n z_2 = z_2 y_2^n$, this would imply that both z_1 and z_2 are prefixes of x^ω and we know that x^ω has the unique prefix from Z. Hence, the map g is unique.

For $x \in X$ and $z \in Z$, we have unique y such that $xz = zy$, as already shown above. ☐

Lemma 1 has a nice consequence, cf. also Example 2.

Corollary 1. *If Z is a biprefix code and $X \sim_Z Y$, then necessarily $|X| = |Y|$.*

3.2 The case when Z is a binary biprefix set.

We now assume that $Z = \{z_1, z_2\}$ is a **binary** biprefix code and f and g are the mappings of Lemma 1. Let $X_1 = g^{-1}(z_1)$, $Y_1 = f(X_1)$, $X_2 = g^{-1}(z_2)$ and $Y_2 = f(X_2)$, where, however, X_i's and Y_i's are not as in the last section. Then $X_1 z_1 = z_1 Y_1$ and $X_2 z_2 = z_2 Y_2$. Since the products XZ and ZY are unambiguous, we have $X_1 z_2 \cup X_2 z_1 = z_2 Y_1 \cup z_1 Y_2$. But it is impossible to have $x_1 z_2 = z_2 y_1$ with $x_1 \in X_1$ and $y_1 \in Y_1$, since the map g is unique. Therefore $X_1 z_2 = z_1 Y_2$ and $X_2 z_1 = z_2 Y_1$.

Now, given $x_1 \in X_1$, let $y_1 = f(x_1)$, so that $x_1 z_1 = z_1 y_1$, $y_2 \in Y_2$ such that $x_1 z_2 = z_1 y_2$, and $x_2 = f^{-1}(y_2)$, so that $x_2 z_2 = z_2 y_2$. Finally, let $y_3 \in Y_1$ such that $x_2 z_1 = z_2 y_3$. Then we have $|x_1| = |y_1|$, $|x_2| = |y_2|$, $|z_1| - |z_2| = |x_1| - |y_2| = |y_3| - |x_2|$, hence $|y_3| = |y_1|$. If $|z_1| \geq |y_1|$, then y_1 is a suffix of z_1, which is a suffix of $z_2 y_3$, hence $y_3 = y_1$. If $|z_1| < |y_2|$, then y_1 and y_3 have a common suffix z_1. Let then t be a word such that $y_1 = t z_1$ and $x_1 = z_1 t$. This implies $y_2 = t z_2$ and $x_2 = z_2 t$, and consequently $y_3 = t z_1 = y_1$. In both cases, we concluded that $y_3 = y_1$, therefore $(\{x_1, x_2\}, \{y_1, y_2\})$ is a minimal solution, and all minimal solution have this form. As a conclusion, there exist words p_1, q_1, p_2, q_2 and integers m_1, m_2 such that

$$\begin{aligned} x_1 &= p_1 q_1, & y_1 &= q_1 p_1, & z_1 &= (p_1 q_1)^{m_1} p_1, \\ x_2 &= p_2 q_2, & y_2 &= q_2 p_2, & z_2 &= (p_2 q_2)^{m_2} p_2, \end{aligned} \tag{4}$$

since $x_1 z_1 = z_1 y_1$ and $x_2 z_2 = z_2 y_2$. The other relations $x_1 z_2 = z_1 y_2$ and $x_2 z_1 = z_2 y_1$ provide the equations

$$q_1 (p_2 q_2)^{m_2} = (q_1 p_1)^{m_1} q_2, \qquad q_2 (p_1 q_1)^{m_1} = (q_2 p_2)^{m_2} q_1, \tag{5}$$

which are sufficient and necessary conditions for $(\{x_1, x_2\}, \{y_1, y_2\})$ to be a solution. So we have proved:

Theorem 1. *Let Z be a binary biprefix code. Then all the minimal solutions are of the form $(\{x_1, x_2\}, \{y_1, y_2\})$ such that there exist words p_1, q_1, p_2, q_2 and integers m_1, m_2 satisfying* (4) *and* (5).

From the definition of a minimal solution we immediately obtain:

Corollary 2. *Let Z be a binary biprefix code. Then all sets X and Y which are conjugated via Z are obtained as component-wise unions of sets satisfying* (4) *and* (5).

Next, we will refine our considerations by analysing when and how (5) can be satisfied. Without loss of generality we can assume that $m_1 \geq m_2$.

We have the following cases:

Case $m_1 = m_2 = 0$. Then the equations reduce to $q_1 = q_2 = q$, $p_1 = z_1$ and $p_2 = z_2$, and we have the minimal solution (Zq, qZ), already found in Proposition 5.

Case $m_2 = 0$ and $m_1 > 0$. Then the equations become $q_1 = (q_1p_1)^{m_1}q_2 = q_2(p_1q_1)^{m_1}$, which is only possible if $m_1 = 1$ and $p_1 = q_2 = 1$. Then $x_1 = y_1 = z_1 = q_1$ and $x_2 = y_2 = z_2 = p_2$: this is a particular case of the previous solution (Zq, qZ), with $q = 1$.

Further on, we can suppose that $m_1 > 0$ and $m_2 > 0$. Now, both Equations in (5) reduce to

$$(p_1q_1)^{m_1-1}p_1 = (p_2q_2)^{m_2-1}p_2\,, \tag{6}$$

and then $Xt = tY$ with $t = (p_1q_1)^{m_1-1}p_1$.

Case $m_1 = m_2 = 1$. Then $p_1 = p_2 = p$. Let $Q = \{q_1, q_2\}$. Then $Z = pQp$ and the minimal solution is (pQ, Qp), i.e., a solution of word type.

Case $m_2 = 1$ and $m_1 > 1$. Then $p_2 = (p_1q_1)^{m_1-1}p_1$. Example 3 is of this type with $m_1 = 2$, $p_1 = a$, $q_1 = 1$, $q_2 = b$.

Case $m_1 = m_2 = 2$. Then $p_1q_1p_1 = p_2q_2p_2$. Assuming that $|p_1| \le |p_2|$, there are words r and s and an integer l such that $p_1 = (rs)^l r$, $p_2 = (rs)^{l+1}r$, $q_1 = srq_2rs$. Then

$$z_1 = (rs)^{l+1}rq_2(rs)^{l+2}rq_2(rs)^{l+1}r \quad \text{and} \quad z_2 = (rs)^{l+1}rq_2(rs)^{l+1}rq_2(rs)^{l+1}r\,.$$

Example 4 is of this type with $l = 0$, $r = a$, $s = 1$, $q_2 = b$.

Case $m_1 > 2$ and $m_2 > 2$. Then the word $w = (p_1q_1)^{m_1-1}p_1 = (p_2q_2)^{m_2-1}p_2$ has two periods $|p_1q_1|$ and $|p_2q_2|$, and its length is more than $|p_1q_1| + |p_2q_2|$. Hence, according to Fine&Wilf theorem, there is a common period t for p_1q_1 and p_2q_2. But then t is a common period for z_1 and z_2, hence one is a prefix of the other, which contradicts the fact that Z is a biprefix. So there are no solutions of this type.

Case $m_2 = 2$ and $m_1 > 2$. Then $p_2q_2p_2 = (p_1q_1)^{m_1-1}p_1$. If $|p_2| \ge |p_1q_1|$, the above argument also applies. Let us therefore assume that $|p_2| < |p_1q_1|$, hence $|q_2| > |(p_1q_1)^{m_1-3}p_1|$. If $|p_2| \le |p_1|$, there are words r and s and an integer l such that $p_2 = (rs)^l r$, $p_1 = (rs)^{l+1}r$, $q_2 = srq_1(p_1q_1)^{m_1-2}rs$. Then

$$\begin{aligned} z_1 &= [(rs)^{l+1}rq_1]^{m_1}(rs)^{l+1}r \quad \text{and} \\ z_2 &= [(rs)^{l+1}rq_1]^{m_1-1}(rs)^{l+2}r[q_1(rs)^{l+1}r]^{m_1-1}\,. \end{aligned}$$

The following example shows the simplest solution of this case:

Example 5. With $l = 0$, $m_1 = 3$, $r = a$, $s = 1$, $q_1 = b$ we get $Z = \{aabaabaabaa, aabaabaaabaabaa\}$, $X = \{aab, aabaaba\}$, $Y = \{baa, abaabaa\}$.

For the case $|p_2| > |p_1|$ we do not have an exhaustive analysis. In this case more complicated solutions are possible, for instance:

Example 6. For $p_1 = a$, $q_1 = aba$, $p_2 = aa$, $q_2 = baaab$ and $m_1 = 3$ we have $Z = \{aabaaabaaabaa, aabaaabaabaaabaa\}$, $X = \{aaba, aabaaab\}$, $Y = \{abaa, baaabaa\}$. Note that here $|p_1q_1| > |p_2| > |p_1|$.

4 When binary sets X and Y are conjugates

In this section we study when two sets X and Y are conjugates. That is to say, we want to characterize all pairs (X, Y) which are conjugates, as well as characterize all sets Z such that $X \sim_Z Y$. We start with a few general observations.

Whenever $X \sim Y$, then necessarily

$$\min_{x \in X} |x| + \min_{z \in Z} |z| = \min_{z \in Z} |z| + \min_{y \in Y} |y|,$$

and therefore also $\min_{x \in X} |x| = \min_{y \in Y} |y|$. Moreover, the sets

$$X_1 = \{x_1 \in X : \quad |x_1| = \min_{x \in X} |x|\}$$

and

$$Y_1 = \{y_1 \in Y : \quad |y_1| = \min_{y \in Y} |y|\}$$

are conjugated via $Z_1 = \{z_1 \in Z : \quad |z_1| = \min_{z \in Z} |z|\}$. Further since all the sets X_1, Y_1 and Z_1 are uniform, by Proposition 3 necessarily

$$X_1 = PQ, \quad Y_1 = QP, \quad \text{and} \quad Z_1 = (PQ)^i P$$

for some non-negative integer i and uniform sets P and Q. Hence, we have the following proposition:

Proposition 6. *There exist uniform sets P and Q and an integer $i \geq 0$ such that $X_1 = PQ$, $Y_1 = QP$, and $Z_1 = (PQ)^i P$. In particular, if $|X_1| = 1$ or $|Y_1| = 1$, then P and Q must be singletons and $X_1 = \{(uv)^m\}$, $Y_1 = \{(vu)^m\}$, $Z_1 = \{(uv)^{k_1} u\}$ for some words u and v, where uv is primitive, and some integers $m \geq 1$ and $k_1 \geq 0$.*

In what follows we characterize the relation $X \sim Y$ for two-element sets X and Y. Let $X = \{x_1, x_2\}$ and $Y = \{y_1, y_2\}$ with $|x_1| \leq |x_2|$ and $|y_1| \leq |y_2|$. We assume that the set Z is a non-empty subset of Σ^+ such that $XZ = ZY$. By Proposition 6, clearly, $|x_1| = |y_1|$.

We divide the set Z into the pairwise disjoint layers:

$$Z = Z_1 \uplus Z_2 \uplus Z_3 \uplus \dots,$$

where for all $z_1, z_2 \in Z_i$, $|z_1| = |z_2|$ and for all $z_1 \in Z_i, z_2 \in Z_{i+1}$, $|z_1| < |z_2|$. Hence, for instance, the set Z_1 contains all shortest elements of the set Z.

First, we state a simple result which will be used several times later. Then, we will distinguish two main cases depending on whether x_1 and x_2 commute or not. In the second case we will further consider cases $|x_1| = |x_2|$ and $|x_1| < |x_2|$, which by Proposition 6 coincide with the cases $|y_1| = |y_2|$ and $|y_1| < |y_2|$, respectively. As a consequence, of several lemmas, each solving one of previously stated cases, we finally get a theorem characterizing all binary conjugated sets X and Y.

The following lemma can be easily proved by using the standard technique for solving word equations.

Lemma 2. *The solutions of equation $w_1w_2w_3 = w_3w_2w_1$ are of the form $w_1, w_3 \in (pq)^*p$ and $w_2 \in q(pq)^*$ for some words $p, q \in \Sigma^*$. Moreover, pq can be chosen primitive.*

The lemma implies the following interesting result.

Corollary 3. *If a word z satisfies the equation $(uv)^k z = z(vu)^k$ with uv primitive and $k \geq 1$, then $z \in (uv)^*u$.*

Proof. Let us choose $w_1 = (uv)^{k-1}u$, $w_2 = v$ and $w_3 = z$ in Lemma 2. Then there exist $p, q \in \Sigma^*$ such that pq is primitive, $(uv)^{k-1}u, z \in (pq)^*p$ and $v \in q(pq)^*$. Hence, we have $(uv)^k \in (pq)^*$. Since both uv and pq are primitive, $uv = pq$. This implies $v = q$ and $u = p$, or $v = p$ and $u = q = 1$, in which case $z \in (pq)^*p = v^+ \subseteq (uv)^*u$. Therefore, we have $z \in (pq)^*p = (uv)^*u$. □

4.1 The commutative case

Now, let us consider the case when x_1 and x_2 commute.

Lemma 3. *If $x_1, x_2 \in t^+$, where t is primitive, then there is a word s such that $y_1, y_2 \in s^+$ and words t and s are conjugates, i.e., $t = uv$ and $s = vu$ for some $u, v \in \Sigma^*$. Moreover, the set Z satisfies that $Z \subseteq (uv)^*u$.*

Proof. Take a word $z_1 \in Z_1$. By Proposition 1a, for any positive integer n and $i = 1, 2$ there are integers $i_1, \ldots, i_n \in \{1, 2\}$ and $z \in Z$ such that

$$z_1 y_i^n = x_{i_1} \ldots x_{i_n} z \in t^+ z\,.$$

If we take n such that $|z_1| + 2|y_i| \leq n|x_1|$, then $z_1 y_i^2$ is a prefix of t^ω. This implies that $z_1 = t^m u$, where $t = uv$, and y_i^2 is prefix of s^ω, where $s = vu$. By Fine&Wilf theorem we conclude that $y_1, y_2 \in s^+$.

The proof of the second part of the claim is a bit more difficult. By Proposition 1b we have immediately:

$$Z \subseteq \mathrm{Pref}(X^+) \cap \mathrm{Suff}(Y^+) = \mathrm{Pref}(t^+) \cap \mathrm{Suff}(s^+)\,.$$

This implies that Z has at most one element of each length, therefore the sets Z_i are singletons. Let $Z_l = \{z_l\}$ for all $l \geq 1$. Let i, j, k be positive integers such that

$$\begin{aligned} x_1 &= (uv)^i, & y_1 &= (vu)^i, \\ x_2 &= (uv)^j, & y_2 &= (vu)^k. \end{aligned}$$

Note that $i < j$ and $i < k$. By Proposition 6, $(uv)^i z_1 = x_1 z_1 = z_1 y_1 = z_1 (vu)^i$. Corollary 3 implies that $z_1 \in (uv)^* u$. Now assume that $Z_1 \cup \cdots \cup Z_{l-1} \subseteq (uv)^* u$. Let $z \in Z_l$. Either $x_1 z = z' y_1$, or $x_1 z = z' y_2$ for some $z' \in Z$. If $x_1 z = z' y_1$, then $|z'| = |z|$. Hence $z' = z$ since the Z_l is a singleton, and by Corollary 3, $z \in (uv)^* u$. If $x_1 z = z' y_2$, then $|z'| < |z|$, hence $z' \in (uv)^* u$, and this yields immediately that $z \in (uv)^* u$. By induction on l, we have that $Z \subseteq (uv)^* u$. □

4.2 The non-commutative case

In what follows we will assume that x_1 and x_2, and similarly, y_1 and y_2, do not commute. As an immediate consequence of Proposition 6 we have that the lengths of x_1 and x_2 are equal if and only if the lengths of y_1 and y_2 are so:

Corollary 4. *Words x_1 and x_2 have the same length, if and only if words y_1 and y_2 have so.*

Now, we will consider the simplest case when the sizes of words in X and Y are equal.

Lemma 4. *If $|x_1| = |x_2| = |y_1| = |y_2|$, then there are words u, v and p such that $|u| = |v|$ and a set $I \subseteq \mathbb{N}$ such that one of the following conditions is satisfied:*

(i) $X = \{pu, pv\}$, $Y = \{up, vp\}$ *and* $Z = \bigcup_{i \in I} \{pu, pv\}^i p$,

(ii) $X = \{up, vp\}$, $Y = \{pu, pv\}$ *and* $Z = \bigcup_{i \in I} \{up, vp\}^i \{u, v\}$.

Proof. Notice that the sets X and Y are uniform, so as a consequence of Proposition 3 there are sets $P, Q \subseteq \Sigma^*$ and $I \subseteq \mathbb{N}$ such that $X = PQ$, $Y = QP$ and $Z = \cup_{i \in I} (PQ)^i P$. Now, if $|X| = 2$, then either $|P| = 1$ and $|Q| = 2$ (case *(i)* with $P = \{p\}$ and $Q = \{u, v\}$), or $|P| = 2$ and $|Q| = 1$ (case *(ii)* with $P = \{u, v\}$ and $Q = \{p\}$). □

In the case when length of words in X and Y are not all the same we need the following 2 lemmas:

Lemma 5. *Let $z_1 \in Z_1$. If $|x_2| < |y_2|$ and $x_2 z_1 = z y_1$ with $|z_1| < |z|$, then x_1 and x_2 commute. Similarly, if $|x_2| > |y_2|$ and $z_1 y_2 = x_1 z$ with $|z_1| < |z|$, then y_1 and y_2 commute.*

Proof. We will prove only the first part of the claim; the proof of the second part is similar. Hence, assume that $|x_2| < |y_2|$ and $x_2 z_1 = z y_1$, where $z \in Z_i$, $i > 1$. By Proposition 1a, for any positive integer n, $x_1^n x_2 z_1$ belongs to the set ZY^{n+1}. Since $|y_2| > |x_2|$, we have $x_1^{n-1} x_1 x_2 z_1 = x_1^n x_2 z_1 = z' y_1^{n+1}$, where $z' \in Z_i$. Similarly, we obtain $x_1^{n-1} x_2 x_1 z_1 = z'' y_1^{n+1}$, where $z'' \in Z_i$. If we take an integer n such that $(n-1)|x_1| \geq |z| = |z'| = |z''|$, these two equalities imply $x_1 x_2 = x_2 x_1$. Hence, x_1 and x_2 commute. $\square$

Lemma 6. *If $|x_1| < |x_2|$ and $|y_1| < |y_2|$, then either x_1 and x_2 commute, or y_1 and y_2 commute, or x_2 and y_2 are conjugates. Moreover, in the last case there exists a word t such that either $x_1 \sim_t y_1$ and $x_2 \sim_t y_2$, or $y_1 \sim_t x_1$ and $y_2 \sim_t x_2$.*

Proof. First, we prove that either $|x_2| = |y_2|$, or we have one of the commuting cases. Take $z_1 \in Z_1$. Assume that $|x_2| < |y_2|$. We have $x_2 z_1 \in XZ = ZY$. The only possibility is that $x_2 z_1 = z y_1$, where $|z| > |z_1|$, since $|x_2| > |x_1| = |y_1|$. By Lemma 5, the word x_1 commutes with x_2.

Similarly, if $|x_2| > |y_2|$, then $z_1 y_2 = x_1 z$ with $|z| > |z_1|$, and by Lemma 5, the words y_1 and y_2 commute.

Now, consider the case $|x_2| = |y_2|$. By Proposition 6 we know that there exist words u and v and integers k_1 and m such that uv is primitive, $x_1 = (uv)^m$, $y_1 = (vu)^m$ and $Z_1 = \{z_1\}$, where $z_1 = (uv)^{k_1} u$. Note that $x_1 \sim_{(uv)^i u} y_1$ for any $i \geq 0$. We have either $x_2 z_1 = z_1 y_2$, or $x_2 z_1 = z_k y_1$, where $z_k \in Z_k$ and $k > 1$. In the first case, we have immediately that x_2 and y_2 are conjugates via z_1. Similarly, we have either $z_1 y_2 = x_2 z_1$, or $z_1 y_2 = x_1 z'_k$, where $z'_k \in Z_k$. In the first case we are again done. Next, we will consider two following equalities:

$$x_2 z_1 = z_k y_1, \qquad\qquad z_1 y_2 = x_1 z'_k. \tag{7}$$

We construct a sequence $\{z_k^{(i)}\}_{i \geq 1}$ in Z_k. Let $z_k^{(1)} = z_k$. For any $i \geq 1$ we have, either $x_1 z_k^{(i)} = z_k^{(i+1)} y_1$, or $x_1 z_k^{(i)} = z_1 y_2$. First, assume that the second case never happens. We have $x_1^i z_k^{(j)} = z_k^{(i+j)} y_1^i$ for all $i \geq 1$ and $j \geq 1$. Hence all $z_k^{(j)}$ are suffixes of y_1^i for some integer i, and therefore they are equal. Then $x_1 z_k = z_k y_1$, and by Corollary 3, we have $z_k \in (uv)^* u$. Using the first of Equations (7) we obtain $x_2 \in (uv)^+$, hence x_1 and x_2 commute.

Now, assume that there is a non-negative integer n such that for all $i = 1, \ldots, n$, $x_1 z_k^{(i)} = z_k^{(i+1)} y_1$ and $x_1 z_k^{(n+1)} = z_1 y_2$. The last equality together with Equation (7) implies that $z'_k = z_k^{(n+1)}$. The first n equalities imply that

$$x_1^n z_k = x_1^n z_k^{(1)} = z_k^{(n+1)} y_1^n = z'_k y_1^n. \tag{8}$$

Equations (7) and (8) imply that

$$(uv)^{m(n+1)} x_2 (uv)^{k_1} u = x_1^{n+1} x_2 z_1 = z_1 y_2 y_1^{n+1} = (uv)^{k_1} u y_2 (vu)^{m(n+1)}.$$

Now if $m(n+1) \leq k_1$, then we have that $x_1 \sim_t y_1$ and $x_2 \sim_t y_2$ for $t = (uv)^{k_1 - m(n+1)} u$. Otherwise, we have that $y_1 \sim_t x_1$ and $y_2 \sim_t x_2$ for $t = (vu)^{m(n+1)-k_1-1} v$. In both cases we have that x_2 and y_2 are conjugates. □

Combining all lemmas proved above we get the following characterization of all binary conjugated sets X and Y:

Theorem 2. *Let $X = \{x_1, x_2\} \subseteq \Sigma^+$ and $Y = \{y_1, y_2\} \subseteq \Sigma^+$ with $|x_1| \leq |x_2|$ and $|y_1| \leq |y_2|$ be conjugates, i.e., $X \sim Y$. Then at least one of the following conditions holds true:*

(i) $x_1 x_2 = x_2 x_1$, $y_1 y_2 = y_2 y_1$, i.e., words x_1 and x_2 (resp. y_1 and y_2) commute, $|x_1| = |y_1|$, and moreover, the words x_1 and y_1 are conjugates;

(ii) there exists a word t such that, for $i = 1$ or 2, either $x_1 \sim_t y_i$ and $x_2 \sim_t y_{3-i}$, or $y_i \sim_t x_1$ and $y_{3-i} \sim_t x_2$.

Conversely, if $X = \{x_1, x_2\}$ and $Y = \{y_1, y_2\}$ with $|x_1| \leq |x_2|$ and $|y_1| \leq |y_2|$ satisfy either (i) or (ii), then $X \sim Y$.

Proof. The first part of theorem is a consequence of Lemmas 3, 4 and 6. Conversely, assume that X and Y satisfy condition (i): there exist words p, q such that $x_1 = (pq)^{m_1}$, $x_2 = (pq)^{m_2}$, $y_1 = (qp)^{m_1}$ and $y_2 = (qp)^{m_3}$ with $m_1 < m_2$ and $m_1 < m_3$. Then the sets X and Y are conjugated via the set $Z = p(qp)^*$.

In case (ii), we have either $Xt = tY$ or $tX = Yt$. In the first case we have $XZ = ZY$ for $Z = \{t\}$. In the second case we take $Z = t^{-1}Y^n$, where n is large enough so that all elements of Y^n are longer than t. In case that Y contains the empty word, then we consider sets $X - \{1\}$ and $Y - \{1\}$ instead. Since $tX^n = Y^n t$, all elements of Y^n have t as a prefix, so we have $tZ = Y^n$. Then $tXZ = YtZ = Y^{n+1} = tZY$, i.e., $XZ = ZY$. Hence X and Y are conjugated. □

Corollary 5. *Let $X = \{x_1, x_2\}$ and $Y = \{y_1, y_2\}$ with $|x_1| = |y_1|$ and $|x_2| = |y_2|$. Then X and Y are conjugated if and only if there exists a single word t such that $Xt = tY$ or $tX = Yt$.*

Note that the notation $x \sim_z y$ means $xz = zy$, and therefore not necessarily implies that $y \sim_z x$. In fact, if words x, y, z satisfy both $x \sim_z y$ and $y \sim_z x$, then they all commute. Theorem 2 shows that the conjugacy of X and Y reduces to that of words. It provides a complete characterization, which, however, is not easy to state in a closed form.

References

[Ma] Makanin, G. S., *The problem of solvability of equations in a free semigroup*, Mat. Sb. **103**, 147–236, 1977 (English transl. in Math USSR Sb. 32, 129–198).

[Pl] Plandowski, W., *Satisfiability of word equations with constants is in* PSPACE, proceedings of FOCS'99, 495–500, 1999.

[HKP] Harju, T., Karhumäki, J., Plandowski, W., *Independent systems of equations*, Chapter 14, in: M. Lothaire, Algebraic combinatorics on words, Cambridge University Press, to appear.

[Ra] Ratoandramanana, B., *Codes et motifs*, RAIRO Inform. Theor., **23**:4, 425–444, 1989.

[CKO] Choffrut, C., Karhumäki, J., Ollinger, N., *The commutation of finite sets: a challenging problem*, Theoret. Comput. Sci. on "Words", (to appear; see TUCS Technical Report 303, 2000).

[Co] Conway, J. H., *Regular algebra and finite machines*, Chapman Hall, 1971.

[KP] Karhumäki, J., Petre, I., *On the centralizer of a finite set*, Proceedings of ICALP'00, LNCS 1853, 536–546, 2000.

[HP] Harju, T., Petre, I., *On commutation and primitive roots of codes*, TUCS Technical Report 402, 2001.

[Ka] Karhumäki, J., *Combinatorial and computational problems of finite sets of words*, Proceedings of MCU'01, LNCS 2055, 69–81, 2001.

[Ei] Eilenberg, S., *Automata, languages and machines*, Academic Press, 1974.

[Le] Leiss, E., *Language equations*, Springer, 1998.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**