Large Simple Binary Equality Words

Jana Hadravová and Štěpán Holub*

Faculty of Mathematics and Physics, Charles University
186 75 Praha 8, Sokolovská 83, Czech Republic
holub@karlin.mff.cuni.cz, hadravova@ff.cuni.cz

Abstract. Let w be an equality word of two nonperiodic binary morphisms $g, h : \{a, b\}^* \to \Delta^*$. Suppose that no overflow occurs twice in w and that w contains at least 9 occurrences of a and at least 9 occurrences of b.
Then either $w = (ab)^i a$, or $w = a^i b^j$ with $\gcd(i, j) = 1$, up to the exchange of letters a and b.

1 Introduction

An equality word, also called a solution, of morphisms $g, h : \Sigma^* \to \Delta^*$ is a word satisfying $g(w) = h(w)$. All equality words of the morphisms g, h constitute the set $\mathrm{Eq}(g, h)$, which is called the equality language of g and h. Natural concept of equality languages was introduced in [1], and since then it has been widely studied. It turns out that the equality languages are very rich objects; for example, each recursively enumerable language can be obtained as a morphic image of generating words of a set $\mathrm{Eq}(g, h)$, see [2].

It is also well known, due to [3], that it is undecidable whether an equality language contains a nonempty word (an algorithmic problem known as the Post Correspondence Problem, or the PCP).

A lot of attention has been paid to the binary case, that is, when $|\Sigma| = 2$. This is the smallest domain alphabet for which the structure of $\mathrm{Eq}(g, h)$ is not completely trivial, and in the same time the largest for which there is any reasonable knowledge about the structure of the equality set. For $|\Sigma| = 3$ it is already a long-standing open problem whether the equality set has to be regular, see [4] and [5].

The structure of binary equality languages has been first studied in [6] and [7] and later in a series of papers [8–10]. It has been shown that binary equality languages are always generated by at most two words, provided that both morphisms are nonperiodic (the periodic case being rather easy). It is also known that if the set $\mathrm{Eq}(g, h)$ is generated by two distinct generators, then these generators are of the form ba^i and $a^i b$. Bi-infinite binary words were studied for example in [11]. It should be also mentioned that the binary case of the PCP is decidable, even in polynomial time ([12, 13]).

* Supported by the research project MSM 0021620839.

However, very little is known so far about words which are single generators of binary equality languages. In this paper we make a step towards a characterization of such words. Our research will be limited only to so-called simple solutions, that is, to solutions that do not have the same overflow twice.

It is well known, since the proof of the decidability of the binary PCP, that each binary equality word can be divided into a sequence of so-called blocks, which are simple in the aforementioned sense. Simple solutions therefore represent a natural starting point of the research. We characterize all simple solutions that are long enough, more precisely all such solutions that contain each of the letters a and b at least nine times. Due to space limits we do not prove all details, we rather explain the main ideas, and include proofs that, instead of being purely technical, illustrate the underlying concepts.

2 Basic Concepts and Ideas

We shall mostly use standard notation and terminology of combinatorics of words (see for example [14] and [15]). We suppose that the reader is familiar with basic folklore facts concerning periods and primitive words. In particular, let us recall the Periodicity lemma, which can be formulated in the following way. If p and q are two primitive words such that the words p^ω and q^ω have a common factor of length at least $|p| + |q| - 1$, then p and q are conjugate.

We shall write $u \leq_{\mathrm{p}} w$ to denote that u is a prefix of w. If, in addition, $u \neq w$, then we write $u <_{\mathrm{p}} w$. Similarly, we use $u \leq_{\mathrm{s}} w$ and $u <_{\mathrm{s}} w$ for suffixes.

Let two binary morphisms $g, h : \{a, b\}^* \to \Delta^*$ be given. We suppose that both morphisms are nonperiodic, that is, $g(a)$ and $g(b)$ ($h(a)$ and $h(b)$ resp.) do not commute.

A word w is called a *solution* of g and h if $g(w) = h(w)$. A solution w is called *simple* if whenever w_1, w_1u, w_2 and w_2u' are prefixes of w^ω such that

$$g(w_1)z = h(w_2), \qquad \text{and} \qquad g(w_1u)z = h(w_2u')$$

for some word z, then $|u| = |u'| = k|w|$, for some $k \in \mathbb{N}_+$. We shall be interested only in simple solutions.

It is easy to see that if w is a simple solution, then it is a primitive word, that is, it is not a power of a shorter word.

Example 1. Trivial examples of non-simple solutions are words composed of shorter solutions. Apart from these, we can also find non-simple solutions that are minimal, that is, they cannot be decomposed into shorter solutions. As an example, consider morphisms

$$\begin{aligned} g(a) &= bba, & g(b) &= bb, \\ h(a) &= b, & h(b) &= abbabb. \end{aligned}$$

They have a solution aab, which is not simple, since

$$g(\varepsilon)bb = h(aa) \qquad \text{and} \qquad g(aa)bb = h(aab).$$

We now formulate our main result.

Theorem 1. *Let $g, h : \{a, b\}^* \to \Delta^*$ be nonperiodic morphisms, and let w be their simple solution. If $|w|_b \geq 9$ and $|w|_a \geq 9$, then, up to the exchange of the letters a and b, either*

$$w = (ab)^i a$$

or

$$w = a^j b^i$$

with $\gcd(i, j) = 1$.

Example 2. Each word mentioned in Theorem 1 is indeed a simple solution for a pair of morphisms g and h. The word $w = (ab)^i a$ is a simple solution for example of morphisms:

$$\begin{aligned} g(a) &= (ab)^i a, & g(b) &= b, \\ h(a) &= a, & h(b) &= (ba)^{i+1} b. \end{aligned}$$

The word $a^j b^i$ is a simple solution for example of morphisms:

$$\begin{aligned} g(a) &= p^l, & g(b) &= a, \\ h(a) &= a^i b a^i, & h(b) &= s^m \end{aligned}$$

where

$$p = (a^i b a^i)^{j-1} a^i b, \qquad s = b a^i (a^i b a^i)^{j-1}$$

and $lj - mi = 1$.

It turns out that a lot of technical complications can be avoided if we work with cyclic words and cyclic solutions instead of ordinary ones. This motivates the following terminology.

Let $u = u_0 \dots u_{n-1}$ be a finite word of length n, and let $(i, j) \in \mathbb{Z}_n \times \mathbb{Z}_n$, $i \neq j$, be an ordered pair. We define an *interval* $u[i, j]$ by

$$u[i, j] = \prod_{k=0}^{(j-i-1) \bmod n} u_{(i+k) \bmod n}.$$

Note that $u_i = u[i, i + 1]$, and $u[i, i]$ is a word conjugate with u.

We denote an infinite word starting at the i-th position of u by

$$u[i, \infty] = u_i u_{i+1} \dots u_{n-1} u_0 u_1 \dots .$$

We have the following crucial definition.

Definition. Let $g, h : \{a, b\}^* \to \Delta^*$ be morphisms. A *cyclic solution* of g, h is an ordered quadruple $(w, \mathfrak{c}, G, H)$ where $w = w_0 w_1 \cdots w_{|w|-1} \in \{a, b\}^+$, $\mathfrak{c} \in \Delta^+$, $|\mathfrak{c}| = |g(w)| = h(w)$ and $G, H : \mathbb{Z}_{|w|} \to \mathbb{Z}_{|\mathfrak{c}|}$ are injective mappings such that

$$\mathfrak{c}[G(i), G(i + 1)] = g(w_i) \qquad \text{and} \qquad \mathfrak{c}[H(i), H(i + 1)] = h(w_i),$$

for all $i \in \mathbb{Z}_{|w|}$.

The concept of a simple solution is extended to cyclic solutions in the following definition.

Definition. Let $(w, \mathfrak{c}, G, H)$ be a cyclic solution of g, h. We say that $(w, \mathfrak{c}, G, H)$ is *simple* if

$$\mathfrak{c}[G(r_1), H(t_1)] = \mathfrak{c}[G(r_2), H(t_2)]$$

implies $(r_1, t_1) = (r_2, t_2)$.

The prior definitions can be better understood if we use the informal concept of an overflow. Given two prefix comparable words u and v, we have either an overflow $v^{-1}u$ of u, or an overflow $u^{-1}v$ of v, depending on whether v is prefix of u, or the other way round. Since the role of an overflow is played by the word z in the definition of a simple solution and by the word $\mathfrak{c}[G(r_1), H(t_1)]$ in the definition of a simple cyclic solution, one can see that both definitions are in fact expressing the same thing: the solution does not contain the same overflow twice.

Notice also that if $(w, \mathfrak{c}, G, H)$ is simple cyclic solution, then w has to be primitive, similarly as in the case of an (ordinary) simple solution.

We now wish to define *p-synchronized overflows*. We have already mentioned that overflows in a cyclic solution $(w, \mathfrak{c}, G, H)$ are words $\mathfrak{c}[G(r), H(t)]$ given uniquely by pairs $(r, t) \in \mathbb{Z}_{|w|}$. Therefore, p-synchronized overflows will be k-tuples of overflows with some additional properties. Although our definition is slightly technical, we will see later on that this concept plays very important role in the proof of the theorem.

Definition. We say that a cyclic solution $(w, \mathfrak{c}, G, H)$ of morphisms g, h has k *p-synchronized overflows* if there is a k-tuple

$$((r_1, t_1), \ldots, (r_k, t_k)) \in (\mathbb{Z}_{|w|} \times \mathbb{Z}_{|w|})^k$$

which has the following properties:

1. for all $i \in \{1, \ldots, k-1\}$ there is $l_i \in \mathbb{N}^+$ such that

$$\mathfrak{c}[G(r_i), H(t_i)] = p^{l_i}\mathfrak{c}[G(r_{i+1}), H(t_{i+1})];$$

2. r_i are pairwise distinct and t_i are pairwise distinct;
3. the word $\mathfrak{c}[G(r_k), H(t_k)]$ is a nonempty prefix of p^ω;
4. for each $i \in \{1, \ldots, k\}$ there is some $0 \leq m < |h(b)|$ such that

$$G(r_i) = H(t_i - 1) + m \bmod |\mathfrak{c}|,$$

and $w_{t_i-1} = b$.

The following example illustrates the previous definitions.

Example 3. Let g, h be morphisms given by:

$$g(a) = (aab)^2a, \qquad g(b) = ab,$$
$$h(a) = a, \qquad h(b) = (baa)^3ba.$$

They have a simple cyclic solution $((ab)^2a, \mathfrak{c}, G, H)$ where $\mathfrak{c} = (aab)^8a$, and the mappings $G, H : \mathbb{Z}_5 \to \mathbb{Z}_{25}$ are given by:

$$G(0) = 0, \quad G(1) = 7, \quad G(2) = 9 \quad G(3) = 16, \quad G(4) = 18,$$
$$H(0) = 1, \quad H(1) = 2, \quad H(2) = 13, \quad H(3) = 14, \quad H(4) = 0.$$

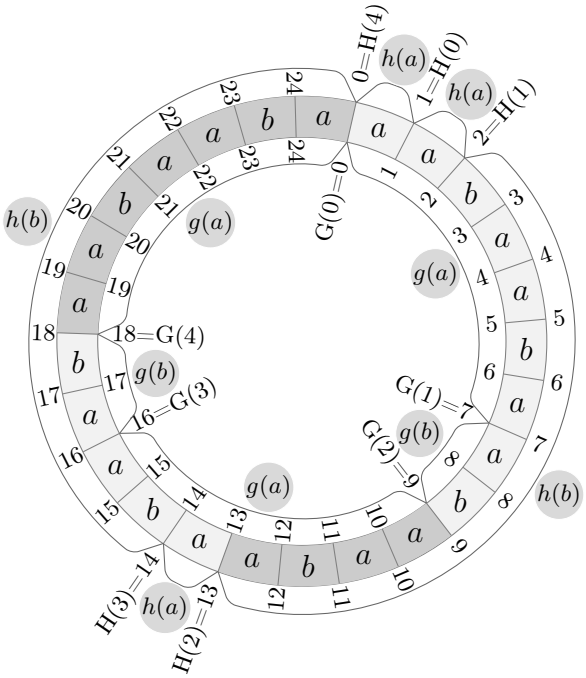
The solution is depicted by the diagram below.

It is possible to verify that g and h have no equality word. Notice, on the other hand, that if w is an equality word for some morphisms g' and h', then we can find mappings G' and H' with $G'(0) = H'(0) = 0$ such that $(w, g'(w), G', H')$ is a cyclic solution. This example therefore shows that the concept of a cyclic solution generalizes nontrivially the concept of an equality word.

The example also features two aab-synchronized overflows, which are emphasized in the diagram. They are given by pairs $(2, 2)$ and $(4, 4)$, since

$$\mathfrak{c}[G(2), H(2)] = \mathfrak{c}[9, 13] = (aab)a \quad \text{and} \quad \mathfrak{c}[G(4), H(4)] = \mathfrak{c}[18, 0] = (aab)(aab)a.$$

Notice that the cyclicity of the solution allows to speak easily for example about the overflow $(aab)^2a(aab)^4a$, which is given as $\mathfrak{c}[G(4), H(2)]$. One of the main advantages of simple cyclic solutions in comparison with (ordinary) simple solutions is that the definition of a simple cyclic solution does not need to employ infinite words.



It is not difficult to see the following properties of p-synchronized overflows. First, we have either

$$p \leq_{\mathrm{p}} \mathfrak{c}[G(r_i), H(t_i)], \qquad \text{or} \qquad p \leq_{\mathrm{s}} \mathfrak{c}[H(t_i), G(r_i)], \tag{*}$$

for all $i \in \{1, \ldots, k\}$.

Second, if we define s by

$$s = \mathfrak{c}[G(r_1), H(t_1)]^{-1} p \, \mathfrak{c}[G(r_1), H(t_1)], \tag{**}$$

then the following equations hold for all $i \in \{1, \ldots, k\}$:

$$\mathfrak{c}[G(r_i), \infty] \wedge p^{\omega} = \mathfrak{c}[G(r_i), H(t_i)](\mathfrak{c}[H(t_i), \infty] \wedge s^{\omega}). \tag{***}$$

A morphism g is called *marked* if the first letter of $g(x)$ is distinct from the first letter of $h(y)$ as long as x, y are two distinct letters. Advantages of marked morphisms are well known in the theory of equality languages, as well as of the PCP. The crucial advantage is that if both morphisms are marked, the continuation of a solution is uniquely determined by any nonempty overflow.

Fortunately, each binary morphism has a so-called *marked version*, defined by:

$$g_{\mathbf{m}}(x) = z_g^{-1} g(x) z_g, \tag{1}$$

for each $x \in \Sigma$ with

$$z_g = g(ab) \wedge g(ba).$$

It is an important property of binary morphisms that $g_{\mathbf{m}}$ is well defined by (1), which, moreover, holds for any word $x \in \Sigma^*$.

It is not difficult to see that marked morphisms have the following property.

Lemma 1. *Let g be a marked morphism and u, v, w be words satisfying*

$$g(u) \wedge w <_{\mathrm{p}} g(v) \wedge w.$$

Then $g(u) \wedge w = g(u \wedge v)$.

Working with the cyclic solution allows to switch easily between any of the given morphisms and its marked version, which is another very convenient property of cyclic solutions.

3 Properties of Cyclic Solutions

3.1 Many *b*s induce rich synchronized overflows

The first step of the proof of Theorem 1 is to show that long words have to contain many synchronized overflows.

Let us adopt a convention. We use the symmetry of g and h, and a and b, and henceforth we shall assume that $h(b)$ is the longest of all four image words, that is,

$$|g(a)| \leq |h(b)|, \quad |g(b)| \leq |h(b)|, \quad \text{and} \quad |h(a)| \leq |h(b)|.$$

A complicated combinatorial analysis, which we omit, yields that nine occurrences of the letter b are enough to enforce five p-synchronized overflows. This is formulated in the following lemma. Notice that we will be working with marked morphisms.

Lemma 2. *Let $(w, \mathfrak{c}, G, H)$ be a simple cyclic solution of marked morphisms $g, h : \{a, b\}^* \to \Sigma^*$. If $|w|_b \geq 9$, then there is a primitive word p such that*

- *$(w, \mathfrak{c}, G, H)$ has five p-synchronized overflows;*
- *$h(b)$ is a factor of p^ω; and*
- *at least one of the words $g(a)$ or $g(b)$ is longer than p.*

To give here just a basic hint of how the lemma is proved, we sketch the proof for a much more generous bound, namely $|w|_b \geq 25$.

We shall study the occurrences of $h(b)$ in $\mathfrak{c}$, which are of the form $\mathfrak{c}[H(i), H(i+1)]$, with $w_i = b$. We call them *true h-occurrences* of b. True g-occurrences are defined similarly.

Consider now the way a given true h-occurrence of b is covered by true g-occurrences of a and b. Since we are working with a simple cyclic solution, it is easy to see that if there are five distinct h-occurrences of b that are covered by the same pattern of g-occurrences of as and bs, then they produce the desired five p-synchronized overflows for a primitive word p.

It remains to show that only the following six types of covers are possible:

$$a^+ \qquad b^+ \qquad a^+b^+ \qquad b^+a^+ \qquad a^+b^+a^+ \qquad b^+a^+b^+. \tag{2}$$

The desired result is then obtained easily by the pigeonhole principle.

In order to prove the remaining part, we look at the starting and ending positions of true g-occurrences of b. We are interested in situations when these occurrences start (end resp.) in some true h-occurrence of b.

Suppose, for a contradiction, that there is a true h-occurrence of b that is covered by a sequence of $g(a)$s and $g(b)$s that is not listed in (2). Inspection of the list shows that in such case there is a true h-occurrence of b in which at least two true g-occurrences of b start, or end. Let us discuss the first case, the second being similar.

Since the number of true g-occurrences of b equals the number of true h-occurrences of b, we deduce that there is a true h-occurrence of b in which no true g-occurrence of b starts. That occurrence is then covered either by a^+ or by ba^+, which implies that a word from $g(a^+)\mathrm{pref}_1(g(b))$ is a factor of $g(a)^\omega$. We get a contradiction with g marked. □

It should not be too surprising that a much more detailed analysis of covers is possible, which leads eventually to the bound 9.

3.2 Impact of five synchronized overflows

The next step is to employ the existence of five synchronized overflows in order to obtain information about the word w. Its structure is revealed in the following three lemmas.

Lemma 3. *Let $(w, \mathfrak{c}, G, H)$ be a simple cyclic solution that has five p-synchronized overflows. Then the primitive root of $\mathfrak{c}$ is not conjugate with p.*

Proof. Suppose, for a contradiction, that the primitive root of $\mathfrak{c}$ and p are conjugate. Note that $h(b)$ is a factor of p^ω greater than $|p|$ by the existence of the synchronized overflows. It is not difficult to see that if ba^ib and ba^jb are two intervals in w, then $i = j$, unless $h(a)$ commutes with p. But if $h(a)$ commutes with p, then also $h(b)$ does, a contradiction. Therefore w is a power of $a^{i_1}ba^{i_2}$. This is a contradiction, since w has to be primitive because $(w, \mathfrak{c}, G, H)$ is simple. □

Next lemma is a consequence of Lemma 1 and is presented without proof.

Lemma 4. *Let $(w, \mathfrak{c}, G, H)$ be cyclic solution of binary marked morphisms g, h that has three p-synchronized overflows via $((r_1, t_1), (r_2, t_2), (r_3, t_3))$. Suppose that*

$$\mathfrak{c}[G(r_1), \infty] \wedge p^\omega = \mathfrak{c}[G(r_2), \infty] \wedge p^\omega = \mathfrak{c}[G(r_3), \infty] \wedge p^\omega. \tag{3}$$

Then $(w, \mathfrak{c}, G, H)$ is not simple.

The following characterization of w is already quite strong.

Lemma 5. *Let $(w, \mathfrak{c}, G, H)$ be a simple cyclic solution of binary marked morphisms g, h that has five p-synchronized overflows. Then there are words e and f conjugate with w, and primitive words u and v such that*

1. *$g(e) = h(f)$;*
2. *u is conjugate with a suffix of e and $g(u) \in p^+$; and*
3. *v is conjugate with a suffix of f and $h(v) \in s^+$, where s is given by (**).*

Proof. Let $((r_1, t_1), \ldots, (r_5, t_5))$ be a pentuple inducing p-synchronized overflows.

(1) Let $m \in \{1, \ldots, 5\}$ be chosen such that

$$|\mathfrak{c}[G(r_m), \infty] \wedge p^\omega| = \max_{k \in \{1,\ldots,5\}} \{|\mathfrak{c}[G(r_k), \infty] \wedge p^\omega|\}.$$

According to Lemma 4, each three words $\mathfrak{c}[G(r_k), \infty] \wedge p^\omega$ are of different lengths. Then, by the pigeonhole principle, we obtain inequalities

$$\mathfrak{c}[G(r_{k_j}), \infty] \wedge p^\omega <_{\mathrm{p}} \mathfrak{c}[G(r_m), \infty] \wedge p^\omega$$

for three different indices $k_1, k_2, k_3 \in \{1, \ldots, 5\}$; indeed, in the "maximal length hole" just two out of five lengths can be placed by Lemma 4.

Observe that $\left|\mathfrak{c}[G(r_{k_j}), \infty] \wedge p^\omega\right| < |\mathfrak{c}|$, otherwise p and the primitive root of $\mathfrak{c}$ are conjugate, which we excluded by Lemma 3. By Lemma 1, we can find $\ell_1, \ell_2, \ell_3 \in \mathbb{Z}_{|w|}$ such that

$$\mathfrak{c}[G(r_{k_j}), \infty] \wedge p^\omega = \mathfrak{c}[G(r_{k_j}), G(\ell_j)],$$

for all $j \in \{1, 2, 3\}$.

Since the cyclic solution is simple, words $\mathfrak{c}[H(t_{k_j}), G(\ell_j)]$, $j \in \{1, 2, 3\}$, are all of different lengths, and are prefix comparable, see (***). We can suppose that

$$\mathfrak{c}[H(t_{k_1}), G(\ell_1)] <_{\mathrm{p}} \mathfrak{c}[H(t_{k_2}), G(\ell_2)] <_{\mathrm{p}} \mathfrak{c}[H(t_{k_3}), G(\ell_3)].$$

Consequently, by Lemma 1, there are n_1, n_2 such that $H(n_1) = G(\ell_1)$ and $H(n_2) = G(l_2)$. Thus

$$g(w[\ell_1, \ell_1]) = h(w[n_1, n_1]).$$

The first part of the lemma has been proved.

(2) Since $H(n_1) = G(\ell_1)$ and $H(n_2) = G(l_2)$, we have from the definition of p-synchronized overflow $n_1 = n_2$ and $l_1 = l_2$. Therefore, $\mathfrak{c}[G(r_{k_1}), G(\ell_1)]$ and $\mathfrak{c}[G(r_{k_2}), G(\ell_1)]$ are both prefixes of p^ω. Since they are also suffix comparable, it can be inferred from primitivity of p and (*) that

$$\mathfrak{c}[G(r_{k_1}), G(r_{k_2})] \in p^+.$$

Consequently, $g(u) \in p^+$ where u is found as the primitive root of the word $w[r_{k_1}, r_{k_2}]$. Since the morphism g is marked, there is a word $u_1 \leq_{\mathrm{p}} u$ and $j \in \mathbb{N}$ such that

$$u \leq_{\mathrm{p}} w[r_{k_1}, \ell_1] = u^j u_1.$$

The word $u_1^{-1} u u_1$ is then a suffix of $w[\ell_1, \ell_1]$, which completes the proof of the second part.

(3) The proof of the third part can be approached in a similar way.

□

In view of the previous lemma it is reasonable to investigate the structure of words (e, f), since the word w is their conjugate. The claims 2 and 3 of the lemma imply that there is a suffix $\tilde{u}$ of e and a suffix $\tilde{v}$ of f, such that $g(\tilde{u})$ and $h(\tilde{v})$ commute and their common primitive root is conjugate with p.

It is interesting to note that, in particular, there are positive integers i and j such that

$$g(\tilde{u}^i) = h(\tilde{v}^j).$$

However, the pair $(\tilde{u}^i, \tilde{v}^j)$ is not the one we are looking for, because the primitive root of $\mathfrak{c}$ is not conjugate with p, as shown in Lemma 3.

We now have a piece of powerful information about the structure of w, which leads to the following claim.

Lemma 6. *Let $(w, \mathfrak{c}, G, H)$ be a simple cyclic solution of binary marked morphisms $g, h : \{a, b\}^* \to \Delta^*$. If $|w|_b \geq 9$, then there are words e, f conjugate with w such that $g(e) = h(f)$ and*

$$e = f = (ab)^i a \quad or \quad e = f = (ba)^i b \quad or \quad e = f = ab^i \quad or \quad (e, f) = (b^i a^j, a^j b^i)$$

with $\gcd(i, j) = 1$ *and* $j > i$.

Notice that in the foregoing lemma the condition $|w|_a \geq 9$ of Theorem 1 is missing. This is due to the fact that $h(b)$ is supposed to have the maximal length among the words $g(a)$, $g(b)$, $h(a)$ and $h(b)$. This distinguishes letters a and b and allows to drop the assumption on $|w|_a$.

Relaxing the assumptions of the theorem has impact on the final set of solutions. We can see from the previous lemma that the words conjugate with ab^i, that is, words $b^{i-j}ab^j$ are brought into question in the case that we do not suppose that $|w|_a \geq 9$.

Example 4. The word $w = b^{i-j}ab^j$, $j \leq i \in \mathbb{N}$, is a solution for example of

$$\begin{aligned} g(a) &= b^{i-j}ab^j, & g(b) &= b^i, \\ h(a) &= a, & h(b) &= b^{i+1}. \end{aligned}$$

The proof of the lemma, which we omit, is achieved by a combinatorial analysis, which is not very deep, but rather complicated and tedious.

3.3 From marked morphisms to ordinary morphisms

We will finally proceed to prove Theorem 1. With help of Lemma 6 it should not be difficult. Note that there are two differences between Theorem 1 and Lemma 6, which are counterparts of each other:

- The lemma requires that the morphisms are marked, while the theorem speaks about general morphisms.
- The theorem requires that the morphisms agree on the same word, while the lemma only guarantees that e and f are conjugate.

Suppose that we are given a pair of (not necessarily marked) morphisms g and h, with a simple solution w. Consider marked versions $g_{\mathbf{m}}$ and $h_{\mathbf{m}}$ of g and h. Clearly, w can be seen as a cyclic solution $(w, g(w), G, H)$ satisfying in addition that $G(0) = H(0)$. Morphisms $(g_{\mathbf{m}}, h_{\mathbf{m}})$ now have a cyclic solution $(w, g(w), G_{\mathbf{m}}, H_{\mathbf{m}})$ given by

$$\begin{aligned} G_{\mathbf{m}}(j) &= (G(j) + |z_g|) \bmod |g_{\mathbf{m}}(w)| \\ H_{\mathbf{m}}(j) &= (H(j) + |z_h|) \bmod |g_{\mathbf{m}}(w)| \,. \end{aligned} \tag{4}$$

Notice that $(w, g(w), G_{\mathbf{m}}, H_{\mathbf{m}})$ is a simple cyclic solution.

Lemma 6 yields that if $|w|_a \geq 9$ and $|w|_b \geq 9$, then w is a conjugate (up to the exchange of letters of alphabet) with $(ab)^i a$ or $a^i b^j$ with $\gcd(i,j) = 1$. It remains to exclude all conjugate words other than trivial. Therefore, in order to complete the proof, we need the following two claims.

Claim 1. If $e = f = (ab)^i a$, $i \geq 9$, then $w = (ab)^i a$.

Claim 2. If $(e, f) = (b^i a^j, a^j b^i)$ with $i, j \geq 9$, then $w = a^j b^i$ or $w = b^i a^j$.

We prove only the former one.

Proof (of Claim 1). Since $i \geq 9$, the Periodicity lemma together with

$$g_{\mathbf{m}}((ab)^i a) = h_{\mathbf{m}}((ab)^i a)$$

implies that the words $g_{\mathbf{m}}(ab)$ and $h_{\mathbf{m}}(ab)$ have the same primitive root t. Hence there are nonempty words t_1, t_2 such that $t_1 t_2 = t$ and

$$\begin{aligned} g_{\mathbf{m}}(a) &= t^{i_1} t_1, \qquad & g_{\mathbf{m}}(b) &= t_2 t^{i_2}, \\ h_{\mathbf{m}}(a) &= t^{j_1} t_1, \qquad & h_{\mathbf{m}}(b) &= t_2 t^{j_2}. \end{aligned} \tag{5}$$

Primitivity of t implies that the longest common suffix of $g_{\mathbf{m}}(ab)$ and $g_{\mathbf{m}}(ba)$ is shorter than $|t|$. Since $g_{\mathbf{m}}$ is by definition equal to $z_g^{-1} g z_g$, we obtain that $|z_g| < |t|$. Similarly $|z_h| < |t|$.

Suppose that the word w is conjugate with $(ab)^i a$ in a nontrivial way. Therefore $(ab)^i a = e_1 e_2 = f_1 f_2$ such that $w = e_2 e_1 = f_2 f_1$. It is obvious that $e_1 = f_1$ and $e_2 = f_2$ since $(ab)^i a$ is a primitive word. Then $G_{\mathbf{m}}(k) = H_{\mathbf{m}}(k)$, where $k = |e_2| = |f_2|$. Equalities (4) imply that

$$G(k) - H(k) = |z_g| - |z_h| \bmod |g_{\mathbf{m}}(w)|\,,$$

and therefore

$$G(k) - H(k) < |t| \bmod |g_{\mathbf{m}}(w)|\,.$$

However, from (5) it is easy to infer that $G(k) - H(k)$ is a multiple of $|t|$, a contradiction. (Note that if $G(k) - H(k) = 0$ we obtain a contradiction as well since w is a simple solution.) □

4 Towards a complete characterization

The main obstacle for the generality of our result is the assumption that the solution is simple. As noted in the introduction, a general solution is composed of blocks, which are simple. Blocks of marked morphisms are pairs (e, f) that satisfy $g(e) = h(f)$ where e is not necessarily equal to f. The techniques used in this paper can be applied also for blocks. The missing assumption that $e = f$ or, more precisely, that e and f are conjugate, makes the classification more complicated, but not essentially different. Investigation of blocks is therefore a

necessary further step towards a complete characterization of binary equality words.

Another missing part are the words with small number of one of the letters. This will probably require some ad hoc case analysis. It should be noted in this respect, that our proof requires essentially only $|w|_b \geq 9$ as soon as b is identified as the letter with the image of the maximal length, that is, as soon as $g(b)$ or $h(b)$ is the longest of the words $g(a)$, $g(b)$, $h(a)$ and $h(b)$. This makes the necessary case analysis of the short solutions a bit easier.

References

1. Salomaa, A.: Equality sets for homomorphisms of free monoid. Acta Cybern. **4** (1980) 127–139
2. Čulík II, K.: A purely homomorphic characterization of recursively enumerable sets. J. ACM **26**(2) (1979) 345–350
3. Post, E.: A variant of a recursively unsolvable problem. Bulletin of the American Mathematical Society **52** (1946) 264–268
4. Karhumäki, J.: On recent trends in formal language theory. In: ICALP '87: Proceedings of the 14th International Colloquium, on Automata, Languages and Programming, London, UK, Springer-Verlag (1987) 136–162
5. Karhumäki, J.: Open problems and exercises on words and languages (invited talk). In: Proceedings of Conference on Algebraic Information, Aristotle University of Thessaloniki (2005) 295–305
6. Čulík II, K., Karhumäki, J.: On the equality sets for homomorphisms on free monoids with two generators. ITA **14**(4) (1980) 349–369
7. Ehrenfeucht, A., Karhumäki, J., Rozenberg, G.: On binary equality sets and a solution to the test set conjecture in the binary case. J. Algebra **85**(1) (1983) 76–85
8. Holub, Š.: Binary equality sets are generated by two words. Journal of Algebra **259** (2003) 1–42
9. Holub, Š.: A unique structure of two-generated binary equality sets. In: Developments in Language Theory. (2002) 245–257
10. Holub, Š.: Binary equality languages for periodic morphisms. In: Algebraic Systems, Formal Languages and Conventional and Unconventional Computation Theory. Volume 1366 of Kokyuroku RIMS. (2002) 52–54
11. Maňuch, J.: Defect effect of bi-infinite words in the two-element case. Discrete Mathematics and Theoretical Computer Science **4**(2) (2001) 273–290
12. Ehrenfeucht, A., Karhumäki, J., Rozenberg, G.: The (generalized) Post Correspondence Problem with lists consisting of two words is decidable. Theor. Comput. Sci. **21** (1982) 119–144
13. Halava, V., Holub, Š.: Binary (generalized) Post Correspondence Problem is in **P**. Technical Report 785, TUCS (Sep 2006)
14. Lothaire, M.: Combinatorics on words. Addison-Wesley (1983)
15. Rozenberg, G., Salomaa, A., eds.: Handbook of formal languages, vol. 1: word, language, grammar. Springer-Verlag New York, Inc., New York, NY, USA (1997)