Binary equality sets are generated by two words.

Štěpán Holub

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

Abstract

We show that the equality set $\text{Eq}(g, h)$ of two non-periodic binary morphisms $g, h : A^* \rightarrow \Sigma^*$ is generated by at most two words. If the rank of $\text{Eq}(g, h) = \{\alpha, \beta\}$ is two, then $\alpha$ and $\beta$ start (and end) with different letters.

This in particular implies that any binary language has a test set of cardinality at most two.

About this version

This is a revised version of my paper published (with the same title) in Journal of Algebra 259 (2003), 1–42.

A nucleus of the paper was a part of my Ph.D. thesis supervised by Aleš Drápal ([15]). Hunting up all emerging cases, however, took another year and half. The proof was completed during the postdoctoral stay in Turku granted by Turku Centre for Computer Science (TUCS). I am grateful especially to Juhani Karhumäki for making that stay possible. When writing the paper I discussed the topic with Vesa Halava, Tero Harju, Juhani Karhumäki and Juha Kortelainen.

After the publication I have heard that the paper is not easy to read, whence there remains some room for doubts about whether the results are correct. Juhani Karhumäki, thanks to his scepticism, forced two of his students to read the paper carefully, namely Elena (Petre) Czeizler and later Markku Laine. I asked the same from my student Václav Flaška. I am indebted to all three for their effort, their comments and suggestions, which induced a couple of dozens smaller corrections and improvements.

The most important difficulty, arisen in this process, was Lemma 29, which does not hold as it stays in the published text. The corrected formulation given in the present version is, ironically, the one from an early draft of the paper. Later, I decided to use a stronger claim, which is in fact never needed in the paper, and which, as it turned out, is fallacious. Elena pointed out some
difficulties in the proof, and Markku found a counterexample, making it clear that the stronger claim cannot be rescued.

Recently, I noticed that Corollary 16 needs an additional assumption. However, it has no impact on the rest of the paper. Mirko Rahn pointed to me that Lemma 3 does not hold for erasing morphisms, which was not stated explicitly (however, an erasing morphism on the binary alphabet is periodic, and such morphisms are excluded implicitly within the whole paper).

During the revision I realized that the proof of one of the cases, namely the case of Subsection 10.2, can be substantially shortened. That is the most complicated case, which covered more than fourteen pages in the original paper, full of technicalities. The case remains the most complicated, but it turned out that it can be simplified, if several lemmas and techniques, present in the paper, are taken more seriously. That is something I suspected, but was unable to accomplish, until the recent revision. The simplification is therefore not due to any new discovery. However, I hope that the new version is critically more readable. I also reorganized parts of other sections, revised the terminology and rewrote some proofs. This also, hopefully, made the paper more friendly.

1 Introduction

Binary equality language, i.e. the set on which two binary morphisms agree, is the most simple non-trivial example of an equality language, the notion of which was introduced in [14]. Equality languages in general play an important role in formal language theory. For a survey and bibliography see [11], section 5.

In the binary case the morphisms are defined on a monoid generated by two letters. It was for the first time extensively studied by K. Čulík II and J. Karhumäki in [3]. There the main claim of our work was conjectured, viz. that a binary equality language is generated by at most two words as soon as at least one of the morphisms is non-periodic (or, equivalently, injective). An important step towards the proof of the conjecture was made in [5] where the following partial characterization was obtained.

**Theorem 1.** The equality set of two binary morphisms $g$ and $h$ has the following structure:

(A) If $h$ and $g$ are periodic, then either $E(h, g) = \{\varepsilon\}$ or

$$E(h, g) = \{\varepsilon\} \bigcup \{\alpha \in A^+ \mid \frac{|\alpha|_a}{|\alpha|_b} = k\}$$

for some $k \geq 0$ or $k = \infty$.

(B) If exactly one morphism is periodic, then

$$E(h, g) = \alpha^*$$

for some word $\alpha \in \Sigma^*$. 

2
If both $g$ and $h$ are non-periodic, then either
\[ E(h, g) = \{\alpha, \beta\}^* \]
for some words $\alpha, \beta \in \Sigma^*$, or
\[ E(h, g) = (\alpha\gamma^*\beta)^* \]
for some words $\alpha, \beta, \gamma \in \Sigma^+$.

The question remained open whether the second possibility of case (C), contradicting the conjecture, can actually occur. In the present paper we show that the answer is negative and, moreover, if $\alpha$ and $\beta$ are both non-empty, they start (and end) with different letters. This is formulated in the following main theorem.

**Theorem 2.** Let $g, h : A^* \to \Sigma^*$ be non-periodic binary morphisms.

(A) Let $\alpha$ and $\beta$, with $\alpha \neq \beta$, non-empty minimal elements of $\text{Eq}(g, h)$. Then
\[ \text{pref}_1(\alpha) \neq \text{pref}_1(\beta) \quad \text{and} \quad \text{suff}_1(\alpha) \neq \text{suff}_1(\beta). \]

(B) $\text{Eq}(g, h)$ is generated by at most two words.

Note that (B) is a trivial consequence of (A). Our proof does not deal directly with (B), but is focused on (A). The author is not aware of any way how to prove (B) not using (A).

**Remark.** Later, in [12], it has been shown that the equality sets generated by two words have a precise form. Namely, the following theorem holds true.

**Theorem.** Let $g$ and $h$ be distinct nonperiodic binary morphisms such that $\text{Eq}(g, h)$ is generated by two words. Then there is a positive integer $i$ such that
\[ \text{Eq}(g, h) = \{a^i b, b a^i\}^*, \]
up to renaming of the letters.

The proof is based on Theorem 2.

Let us mention two problems closely related to the question about the structure of binary equality sets. The first one is the binary case of the famous Post Correspondence Problem, shortly PCP(2). The cohesion of the two problems is obvious, as PCP(2) consists in deciding, given two binary morphisms, whether their equality set is empty. The proof that the question is algorithmically decidable (see [4]) was one of the important moments in the development of theoretical computer science. A survey of further results concerning PCP can be found in [6] and [7]. It was, especially, shown ([8]) that generalized PCP of arbitrary size is decidable if the morphisms are marked. Recently, it was proved that the binary PCP is decidable in polynomial time ([10]).
The second problem akin to the structure of binary equality languages is the existence of a test set for binary languages. Indeed, if two morphisms agree on a language, it must be a subset of an equality language. In [5] it is shown that all binary languages have a three element test set. Our result allows to cut down this bound to two. Let us remark that this improvement is not a simple consequence of the fact that the equality language is generated by two words — the difference in the first (or last) letter is a necessary ingredient.

2 Summary of the proof

In this section we give an overview of the rest of the paper, and a summary of the proof of Theorem 2. This seems to be convenient, since the proof is divided into several parts, which may obscure its course.

Section 3 contains basic terminology and some basic tools.

In Section 4 we explain the notion of principal morphisms. Their use allows to suppose that one of the morphisms $g$ and $h$ is marked.

Section 5 explains basic properties of binary morphisms, which are familiar to anybody who has ever worked on binary equality sets or binary PCP. The lesson can be summarized as follows: The solution $(x, y)$ of the equation $g(x) = h(y)$ can be constructed deterministically, except for a special situation called the critical overflow, where two continuations are possible.

This implies that any equality word can be divided into sequence of two different blocks. The existence of two blocks allows to define the concept of successor morphisms, which is extremely important in PCP. In this paper we need just basic properties of successor morphisms. They are used twice: in proof of Lemma 29 and in Claim 9. Some interesting properties of successors, not directly needed for the proof, are pushed away to Appendix.

The actual proof of Theorem 2 is given in Sections 7 – 10. It consists of nine claims, which gradually show that no counterexample to the statement of the theorem exists.

Finally, Section 11 uses Theorem 2 to show that any binary language has a test set of cardinality at most two. The application is quite straightforward.

We shall give an overview of the proof of the main theorem. For the terminology used in this sketch, see the appropriate place of the paper, mainly Section 3.

First, it is important to remark that the proof seems to be quite technical, but in fact it is based on three relatively simple steps. The complicated structure is then caused by the necessity to deal with several cases, each of them requiring a bit different approach, that is, a different way in which the three basic steps (in particular the first of them) are achieved. The steps are as follows:

1. Suppose that there is a counterexample to the theorem, and show that in such a case the critical overflow commutes with one of the image words.
2. Show that 1. implies that the critical overflow is in fact a power of the corresponding image word.

3. Show that the coincidence pairs implied by 2. lead to a contradiction.

Proof of Theorem 2, a sketch. The course of the proof is by contradiction. Suppose that the theorem does not hold, and let $g, h : A^* \rightarrow \Sigma^*$ be a pair of morphisms that disproves it. This means that $\text{eq}(g, h)$ contains two words $\alpha$ and $\beta$ starting or ending with the same letter.

This is the first of several places, where we can use the mirror symmetry. Choosing between $(g, h)$ and $(\overline{g}, \overline{h})$ we can suppose that $\text{pref}_1(\alpha) = \text{pref}_1(\beta)$.

The target alphabet of morphisms $g$ and $h$ is not too closely connected to the form of their equality set, and we can therefore modify it a bit. The natural choice is to keep it simple. This means here that we shall suppose that $\Sigma$ is the base of the free hull of the set $\{g(a), h(a), g(b), h(b)\}$. This choice implies that at least one of the morphisms is marked (Section 4).

On the other hand, the second morphism is not marked, since two marked morphisms could not have minimal equality words starting with the same letter. By symmetry, we can suppose that $g$ is marked, and $h$ is not. The remaining symmetry, the symmetry of $a$ and $b$, allows to suppose that $|g(a)| > |h(a)|$, and $|g(b)| < |h(b)|$. This yields the Definition 25 of the so called counterexample. We are going to show that such a counterexample does not exist.

A great majority of what follows is based on the combinatorial analysis of two places, where the counterexample structure is precisely known: the beginning of the equality words (which is the same for both of them), and the situation around the critical overflow (where the two words start to differ).

Proofs of all the below claims have the same basic structure. We suppose, for a contradiction, that there is a counterexample with certain properties, and show that this is not possible. We can always use previous claims, which enforce additional properties of the supposed counterexample.

Section 7 considers the situation, which may seem a bit hypothetical at the moment, when the critical overflow $z_h$ commutes with one of the words. This yields first two claims about non-existence of the counterexample:

- Claim 1: There is no counterexample such that $z_h$ commutes with $g(b)$ and $\text{pref}_1(\sigma) = b$.
- Claim 2: There is no counterexample such that $z_h$ commutes with $h(a)$, $\text{pref}_1(\sigma) = a$, and the common primitive root of $z_h$ and $h(a)$ is a suffix of $g(a)$.

The two claims depend on Lemma 29, which is mixed up in the printed version.

Section 8 shows that the above claims are useful, after all. It is possible to show that the situation described in Claim 1 or Claim 2 takes place if $\overline{g}$ is not marked. The section again exploits the mirror symmetry, choosing between $(g, h)$ and $(\overline{h}, \overline{g})$. Note that in the second pair the morphism $\overline{g}$ is at the rear,
since it is not marked, by assumption. On the other hand, then \( \overline{h} \) is marked, as it is possible to show. We therefore have the next claim:

• Claim 3: There is no counterexample with \( \overline{g} \) not marked.

Section 9 deals with the possibility that \( \overline{h} \) is not marked. In this case we simply consider the marked version of \( \overline{h} \), instead of \( \overline{h} \). This results in a rearrangement of the domino pieces that compose the equality words (and which are precisely described in the section). We obtain a claim that does not speak about non-existence. Instead, it says that the case when both \( \overline{g} \) and \( \overline{h} \) are marked is as good as the other:

• Claim 4: Let \((g, h)\) be a counterexample. Then there exists also a counterexample \((g_1, h_1)\) such that both \( \overline{g_1} \) and \( \overline{h_1} \) are marked.

In Section 10 we therefore deal with the situation when both \( \overline{g} \) and \( \overline{h} \) are marked. This has some advantages; for example, we know that both \( h(a) \) is a suffix of \( g(a) \), and \( g(b) \) a suffix of \( h(b) \). As a consequence, we can quite easily proof that \( \text{pref}_1(\sigma) = b \), and, by a mirror symmetry, also \( \text{suff}_1(\sigma) = b \) (where \( \sigma \) is the longest common prefix of the words \( \alpha \) and \( \beta \), which are supposed to contradict our theorem). This is formulated in the following claim.

• Claim 5: There is no counterexample such that both \( \overline{g} \) and \( \overline{h} \) are marked and \( \text{pref}_1(\sigma) = a \) or \( \text{suff}_1(\sigma) = a \).

The remaining case, Subsection 10.2, is most complicated, and all available tools are exploited, including a new one, which is needed in the following claim. For the meaning of variables \( \ell, \ell', k \) and \( k' \) see Convention 32. We shall further omit, for sake of simplicity, the assumption that \( \overline{g} \) and \( \overline{h} \) are marked.

• Claim 6: There is no counterexample such that \( g(b\ell a) \) is a prefix of \( h(b) \).

Similarly, there is no counterexample such that \( g(ab\ell') \) is a suffix of \( h(b) \).

This claim is the only place that uses a kind of global argument, not only the beginning (or the end), and the critical point. We consider relative positions of \( g(b)s \) and \( h(b)s \) in \( g(\sigma) \) and \( h(\sigma) \). This trick is responsible for a significant simplification of the proof compared to the printed version. Actually, it is used in the printed version as well, but not enough consistently. Oddly enough, the content of the claim is not very impressive.

The following two claims depend on the previous one. The technique of their proof is again a classical combinatorial analysis and they reduce the respective cases to Claim 1, i.e., we show that in that cases \( g(b) \) and \( z_h \) commute (another point where the new version is more assiduous in using known facts):

• Claim 7: There is no counterexample such that \( k > \ell \).

• Claim 8: There is no counterexample such that \( k < \ell \).

It is patent that the final analysis is divided according to the relation between \( k \) and \( \ell \), and that the remaining case is \( k = \ell \). This final case is however
once more accompanied by difficulties. The following claim is proved by a sophisticated use of successor morphisms of $\overrightarrow{f}$ and $\overrightarrow{h}$, and uses an induction on the length of the equality words.

- **Claim 9**: There is no counterexample such that $k = \ell$.

Claims 5–9 together show that there is no counterexample such that $\overrightarrow{f}$ and $\overrightarrow{h}$ are marked. The proof is complete.

\[
\square
\]

# 3 Preliminaries

By $\Sigma$ we denote an arbitrary alphabet, by $A$ the two-letter alphabet $\{a, b\}$. $\Sigma^*$ is the free monoid, and $\Sigma^+$ the free semigroup generated by $\Sigma$. The empty word is denoted by $\varepsilon$. Any subset of $\Sigma^*$ is called a language.

The symbol $|u|$ represents the length of the word, and $|u|_x$ the number of occurrences of the letter $x$ in $u$. A *prefix* of $u$ is any word $v \in \Sigma^*$ such that there exists a word $v' \in \Sigma^*$ with $u = vv'$. The set of all prefixes of $u$ is denoted by $\text{pref}(u)$. A prefix $v$ of $u$ is *proper* if $v \neq \varepsilon$ and $v \neq u$. Similarly *suffix* and *proper suffix* are defined. The set of all suffixes of $u$ is denoted by $\text{suff}(u)$. The first (the last resp.) letter of a non-empty word $u$ is also denoted by $\text{pref}_1(u)$ ($\text{suff}_1(u)$ resp.). A word $v$ is called a *factor* of $u$ if there exist words $w, w' \in \Sigma^*$ such that $u = w v w'$.

The positive powers $u^n$ of a word are defined as usually, with $u^0 = \varepsilon$. We shall also use negative powers to simplify notation, which should not cause any confusion.

The notion of prefix, suffix and factor can be extended to languages: a prefix (suffix, factor resp.) of a language is prefix (suffix, factor resp.) of some of its elements. Accordingly, $\text{pref}(L) = \bigcup_{u \in L} \text{pref}(u)$. Similarly for $\text{suff}(L)$. The language $\{u^i \mid i \in \mathbb{N}_+\}$ is denoted by $u^+$ and $u^* = u^+ \cup \{\varepsilon\}$.

If $L \subset \Sigma^*$ is a language, then by $L^+$ ($L^*$ resp.) we denote, as usual, the subsemigroup (the submonoid resp.) of $\Sigma^+$ generated by $L$. Note that this is a slight abuse of notation, since $L$ is in this case not understood as an alphabet.

A word $u$ is called *primitive* if and only if $u = v^n$ implies $u = v$. The *primitive root* of $u$ is the (uniquely given) primitive word $r$ such that $u \in r^+$. Words $u$ and $v$ are called *conjugates* if $u = w w'$ and $v = w' w$.

If we speak about minimality or maximality of some element, the implicit ordering is the prefix one, i.e. $v \preceq u$ if and only if $v \in \text{pref}(u)$. (While by the *shortest* word we mean the word with the smallest length!)

If $v \in \text{pref}(u)$ or $u \in \text{pref}(v)$, we say that they are *comparable*, denoted by $u \bowtie v$. The maximal common prefix of words $u$ and $v$ is denoted by $u \land v$. Their
maximal common suffix is denoted by \( u^\prec v \). If \( u \) and \( v \) are words, the maximal \( u \)-prefix of \( v \) is the maximal element of
\[
\text{pref}(v) \bigcap \text{pref}(u^+)\,.
\]

We say that two words are suffix-comparable if one is a suffix of the other.

Let \( u \in \Sigma^+ \) be a word \( u = l_1l_2 \ldots l_d \), with \( d = |u| \) and \( l_i \in \Sigma \). Then the mirror image of the word \( u \), denoted by \( \overline{u} \), is obtained by inverting the order of the letters, viz.
\[
\overline{u} = l_dl_{d-1} \ldots l_1.
\]

Let \( g \) be an arbitrary morphism. The mirror image of \( g \) is the morphism denoted by \( \overline{g} \), which has the same range and domain as \( g \), and is defined by
\[
\overline{g}(x) = g(\overline{x})
\]
for each \( x \in \Sigma \). Note that in general \( \overline{g}(u) \) does not equal to \( g(\overline{u}) \) nor to \( g(u) \). Instead
\[
\overline{g}(\overline{u}) = g(u).
\]

All concepts and reasonings regarding prefixes are valid dually for suffixes, mirror images considered. We shall often use the fact.

A morphism \( g \) defined on \( \Sigma \) is called erasing if \( g(x) \) is empty for some \( x \in \Sigma \). A morphism \( g \) is periodic if there is a word \( t \) such that \( g(x) \in t^* \), for all words \( x \) (or, equivalently, all letters \( x \)). Note that a binary morphism is periodic as soon as it is erasing.

Let \( S = M^+ \) be a subsemigroup of \( \Sigma^+ \) generated by a set \( M \). The rank of \( M \) is the cardinality of the minimal set generating \( S \). We can write
\[
\text{rank}(M) = \text{Card}(S \setminus S \cdot S).
\]

By the rank of a monoid \( M \) we mean the rank of the semigroup \( M \setminus \{\epsilon\} \).

It is well known fact that for each set \( M \subset \Sigma^+ \) there exist the smallest free subsemigroup of \( \Sigma^+ \) containing \( M \) and called its free hull.

Let \( g, h : \Sigma^* \rightarrow \Sigma^* \) be binary morphisms. Their equality set is defined by
\[
\text{Eq}(g, h) = \{ u \in \Sigma^* \mid g(u) = h(u) \}.
\]
It is easy to verify that the set \( \text{Eq}(g, h) \) is a free submonoid of \( \Sigma^* \) generated by the set of its minimal elements
\[
\text{eq}(g, h) = \text{Eq}(g, h) \setminus (\text{Eq}(g, h) \setminus \{\epsilon\})^2 \setminus \{\epsilon\}.
\]

Note that \( \text{eq}(g, h) \) is a bifix code.

Let \( g : A^* \rightarrow \Sigma^* \) be a nonperiodic binary morphism. By \( z_g \) we denote the maximal common prefix of \( g(ab) \) and \( g(ba) \), i.e.
\[
z_g = g(ab) \wedge g(ba).
\]
Since \( g \) is nonperiodic, we have \(|z_g| < |g(a)| + |g(b)|\), by Lemma 4 below. If \( \text{pref}_1(g(a)) \neq \text{pref}_1(g(b)), \) i.e. \( z_g = \varepsilon \), we say that \( g \) is marked.

Similarly we define \( z_g \) as a maximal common suffix of \( g(ab) \) and \( g(ba) \). Note that \( z_g = g(ab) \land g(ba) = z_g \) and \( z_g = \varepsilon \) is equivalent to \( g \) being marked.

Cartesian product \( A^* \times A^* \) is the set of ordered pairs \((u, v)\) of words. It can be seen as a monoid with operation of catenation defined by \((u, v)(u', v') = (uu', vv')\), with the unit \((\varepsilon, \varepsilon)\). Such a monoid is obviously not free, it is even not isomorphic to a submonoid of a free monoid.

Let \( g, h : A^* \to \Sigma^* \) be binary morphisms. The subset of \( A^* \times A^* \) denoted by \( \mathcal{C}(g, h) \) and defined by

\[
\mathcal{C}(g, h) = \{(u, v) \mid g(u) = h(v)\}
\]

will be called the coincidence set of morphisms \( g \) and \( h \). It is generated by the set

\[
c(g, h) = \mathcal{C}(g, h) \setminus (\mathcal{C}(g, h) \setminus \{(\varepsilon, \varepsilon)\})^2 \setminus \{(\varepsilon, \varepsilon)\}.
\]

It is not difficult, but quite important to note that

**Lemma 3.** Let \( g \) and \( h \) be non-erasing morphisms. Then \( \mathcal{C}(g, h) \) is, as a submonoid of \( A^* \times A^* \), freely generated by \( c(g, h) \). Moreover, the set \( c(g, h) \) is a bifix code.

Obviously \((u, u)\) is an element of \( \mathcal{C}(g, h) \) for each \( u \in \text{Eq}(g, h) \), and \( \text{Eq}(g, h) \) is given uniquely by \( \mathcal{C}(g, h) \) as

\[
\text{Eq}(g, h) = \{u \mid (u, u) \in \mathcal{C}(g, h)\}.
\]

We present several combinatorial lemmas for future (often implicit) reference. Following three lemmas are part of the folklore.

**Lemma 4.** The following conditions are equivalent:

- The words \( u \) and \( v \) commute.
- The words \( u \) and \( v \) have the same primitive root.
- The words \( u \) and \( v \) satisfy a nontrivial relation.

**Lemma 5** (Periodicity Lemma). Let \( u^+ \) and \( v^+ \) have a common prefix of length \(|u| + |v|\). Then the words \( u \) and \( v \) commute.

**Lemma 6.** The following conditions are equivalent:

1. Words \( u \) and \( v \) are conjugates.
2. There is a word \( z \) such that \( uz = zv \).
There are words $t_1$ and $t_2$ such that $t_2$ is non-empty, $t_1 t_2$ is primitive and
\[ u \in (t_1 t_2)^+, \quad v \in (t_2 t_1)^+, \quad |u| = |v|. \]

Moreover, if $t_1$ and $t_2$ are like in (iii) and $z$ is like in (ii), then $z \in (t_1 t_2)^* t_1$.

We shall often use the following lemma. It is based on the well known fact that a primitive word $t$ cannot satisfy equality $tt = utv$, with $u$ and $v$ non-empty.

**Lemma 7.**

(A) Let $sw$ be a factor of $w^+$. Then $s$ is a suffix of $w^+$.

(B) Let $wp$ be a factor of $w^+$. Then $p$ is a prefix of $w^+$.

(C) Let $uw$ be a prefix of $w^+$. Then $u$ and $w$ commute.

(D) Let $uw$ be a suffix of $w^+$ and let $w$ be a prefix of $uw$. Then $u$ and $w$ commute.

(E) Let $u_1, u_2, w, w' \in \Sigma^+$ be words such that $w'$ is a conjugate of $w$, $|u_1| \leq |u_2|$, and the words $u_1 w'$, $u_2 w'$ are prefixes of $w^+$. Then $u_1$ is a suffix of $u_2$ and $u_2u_1^{-1}$ commutes with $w$.

One more lemma, which is easy to prove:

**Lemma 8.** Let $g : A^* \to A^*$ be a marked morphism and let $u, v \in A^*$. Then there exist a word $w \in A^*$ such that $g(w) = g(u) \land g(v)$.

The following nice lemma is a key fact for binary morphisms.

**Lemma 9.** Let $X = \{x, y\} \subseteq \Sigma^+$ be nonperiodic set (i.e. $xy \neq yx$). Let $u \in xX^*$, $v \in yX^*$ be words such that $|u|, |v| \geq |xy \land yx|$. Then $u \land v = xy \land yx$.

The proof is not difficult (see [2], p. 348).

The lemma immediately implies that for a nonperiodic binary morphism $h$ and an arbitrary word $u \in A^+$ enough long, the word $z_h$ is a prefix of $h(u)$ and the $(|z_h| + 1)$-th letter of $h(u)$ indicates the first letter of $u$. For any $u, v \in A^*$ we have
\[ z_h = h(au)z_h \land h(bv)z_h. \]  \hfill (1)

It is now easy to see that the morphism $h_m$, such that
\[ h_m(u) = z_h^{-1}h(u)z_h, \]  \hfill (2)

$u \in A$, is well defined. Moreover it is marked, and the equality (2) holds for any $u \in A^*$. We shall call it the marked version of $h$.

**N.B.** The case $g = h$ is trivial. Throughout the paper we shall implicitly suppose $g \neq h$. 

10
4 Principal morphisms

In this section we show that at least one of the morphisms \( g \) and \( h \) can be supposed to be marked. As we shall see, this will make our research more convenient. The goal is achieved by choosing a suitable target alphabet.

**Definition 10.** We say that an (unordered) pair of binary morphisms \( g, h : A^* \to \Sigma^* \) is principal if the target alphabet \( \Sigma \) is the base of the free hull of the set \( \{g(a), g(b), h(a), h(b)\} \).

The previous definition reflects the use of the term “principal morphism” in literature (see for example [13], p. 170).

The advantages of principal morphisms stem from the following important property.

**Lemma 11.** Let \( X \) be a finite subset of \( \Sigma^* \) and let \( Y \) be the base of the free hull of \( X \). Then for each element \( y \in Y \) there is a word \( x \in X \) such that \( y \) is a prefix (suffix resp.) of \( x \).

For the proof see [1], Lemma 3.1. For our purpose note the following immediate corollary.

**Corollary 12.** Let \( X \) be a finite subset of \( \Sigma^* \) such that \( \Sigma \) is the base of the free hull of \( X \). Then

\[
\Sigma = \{\text{pref}_1(u) \mid u \in X\} = \{\text{suff}_1(u) \mid u \in X\}.
\]

It is quite intuitive that choosing the base of the free hull as the target alphabet has no influence on the coincidence set of the morphisms. The following lemma is formulated for binary morphisms, but it can be trivially extended to an arbitrary domain alphabet.

**Lemma 13.** Let \( g_1, h_1 \) be morphisms \( A^* \to \Sigma^* \). Then there is a principal pair of morphisms \( g, h, \) such that

\[
\mathcal{C}(g, h) = \mathcal{C}(g_1, h_1).
\]

Moreover, if \( g_1 \) (\( h_1 \), \( \overline{g}_1 \), \( \overline{h}_1 \) resp.) is marked, then such is also \( g \) (\( h \), \( \overline{g} \), \( \overline{h} \) resp.).

**Proof.** Let \( F \subset \Sigma^* \) be the free hull of the set \( \{g_1(a), g_1(b), h_1(a), h_1(b)\} \) and let \( C \) be an alphabet whose cardinality equals the rank of \( F \). Let \( \varphi : C^* \to F \) be an isomorphism. Define morphisms \( g, h : A^* \to C^* \) by

\[
g = \varphi^{-1} \circ g_1, \quad h = \varphi^{-1} \circ h_1.
\]

Then \( (g, h) \) is a principal pair of morphisms, the above diagram commutes, and \( \mathcal{C}(g, h) = \mathcal{C}(g_1, h_1) \). The rest is obvious.
The previous lemma shows that we can always, without loss of generality, suppose that the pair we work with is principal. We can now prove that this brings about markedness of one of the morphisms.

**Lemma 14.** Let \( g, h \) be nonperiodic principal morphisms, with nonempty \( \text{eq}(g, h) \). Then at least one of the morphisms \( g, h \) is marked, and at least one of the morphisms \( g^{-1}, h \) is marked.

**Proof.** Suppose that none of the morphisms is marked, therefore
\[
\text{pref}_1(g(a)) = \text{pref}_1(g(b)), \quad \text{pref}_1(h(a)) = \text{pref}_1(h(b)).
\]
Let \( x \) be a first letter of a word \( u \in \text{Eq}(g, h) \). Then
\[
\text{pref}_1(g(x)) = \text{pref}_1(h(x)),
\]
and Corollary 12 implies that the morphisms are periodic, a contradiction.

Obviously, the morphisms \( g, h \) are also principal, since the concept of the free hull is preserved under the mirror symmetry. This concludes the proof. \( \square \)

### 5 The block structure of the coincidence set

In this section we study the structure of the equality set of nonperiodic morphisms and their relation to the coincidence set. The previous section justifies why we shall always suppose that \( g \) is marked.

Let \( u, v \in \Sigma^* \) be words such that \( g(u) \triangleright h(v) \). Following lemmas show that the possibility to lengthen the words \( u, v \) to words \( u', v' \) such that \( g(u') = h(v') \) is very restricted.

**Lemma 15.** Let \( g \) and \( h \) be binary morphisms, and let \( g \) be marked. Let \( u, v \in A^* \) be words such that \( g(u) \triangleright h(v) \) and let
\[
g(u) \neq h(v)z_h.
\]
Let \( u_1, u_2, v_1, v_2 \in A^+ \) be words such that
\[
g(uu_1) = h(vv_1), \quad g(uu_2) = h(vv_2).
\]
Then \( \text{pref}_1(u_1) = \text{pref}_1(u_2) \) or \( \text{pref}_1(v_1) = \text{pref}_1(v_2) \).

**Proof.** If \( u_1, u_2, v_1 \) and \( v_2 \) satisfy the conditions of the lemma, then the same conditions are satisfied also by the words \( u_1uu_1, u_2uu_2, v_1vv_1 \) and \( v_2vv_2 \) resp. Hence we can suppose that each of the words \( u_1, u_2, v_1, v_2 \) is longer than \( z_h \).

Consider three cases.

1. First suppose that \( |g(u)| < |h(v)| + |z_h| \). By (1), \( h(v)z_h \) is a prefix of both \( h(vv_1) \) and \( h(vv_2) \) and
\[
\text{pref}_1(g(u_1)) = \text{pref}_1(g(u_2)) = \text{pref}_1(g^{-1}(u)h(v)z_h) = x.
\]

Since \( g \) is a marked morphism, this implies that \( \text{pref}_1(u_1) = \text{pref}_1(u_2) \).
2. Suppose on the other hand that $|g(u)| > |h(v)| + |z_h|$. Then $h(v_1), h(v_2)$ have the common prefix longer than $z_h$ and $\text{pref}_1(v_1) = \text{pref}_1(v_2)$ is determined by the letter $x = \text{pref}_1((h(v)z_h)^{-1}g(u))$.

3. If $|g(u)| = |h(v)| + |z_h|$, then, clearly, $g(u) = h(v)z_h$.

Previous lemma has the following corollary.

**Corollary 16.** Let $g$ and $h$ be binary morphisms, and let $g$ be marked. Let $(c, d)$ and $(c', d')$ be distinct elements of $c(g,h)$, and suppose that neither $c$ and $c'$ are comparable, nor $d$ and $d'$ are. Put

$$u = c \land c', \quad v = d \land d'.$$

Then

$$g(u) = h(v)z_h.$$
(i) \( z_h g(e) = h(f) z_h \)

(ii) The words \( e, f \) are minimal, i.e.: If \( u \) is a proper prefix of \( e \) and \( v \) is a proper prefix of \( f \) then \( z_h g(u) \neq h(v) z_h \).

Then, given the first letter of \( e \) or the first letter of \( f \), the words \( e \) and \( f \) are determined uniquely.

Proof. Suppose \( e, f \) and \( e', f' \) satisfy (i) and (ii), and \( \text{pref}_1(e) = \text{pref}_1(e') \). Put \( c = e \wedge e' \), \( d = f \wedge f' \). Since \( g \) is a marked morphism, we have

\[ z_h g(e) \wedge z_h g(e') = z_h g(c). \quad (3) \]

From (1) we deduce

\[ h(f) z_h \wedge h(f') z_h = h(d) z_h. \quad (4) \]

Since \( z_h g(e) = h(f) z_h \) and \( z_h g(e') = h(f') z_h \), the equalities (3), (4) yield

\[ z_h g(c) = h(d) z_h. \]

Since \( c \) is non-empty, we deduce from (ii) that \( c = e = e' \) and \( d = f = f' \).

Similarly if \( \text{pref}_1(f) = \text{pref}_1(f') \).

This implies the following lemma.

**Lemma 19.** Let \( g \) and \( h \) be binary morphisms, and let \( g \) be marked.

(A) The rank of \( C(g, h_m) \) is at most two.

(B) If the rank of \( C(g, h_m) \) is two and \( c(g, h_m) = \{(e, f), (e', f')\} \), then

\[ \text{pref}_1(e) \neq \text{pref}_1(e') \]
\[ \text{pref}_1(f) \neq \text{pref}_1(f'). \]

Proof. Recall that \( h_m(u) = z_h^{-1} h(u) z_h \) to see that

\[ C(g, h_m) = \{(u, v) \in A^* \times A^* \mid z_h g(u) = h(v) z_h \}. \]

The rest is a consequence of Lemma 18.  

Note that \((e, f) \in c(g, h_m)\) is just another formulation of the fact that \( e, f \) are minimal words satisfying \( z_h g(e) = h(f) z_h \), which are exactly conditions of Lemma 18. The pairs \((e, f)\) and \((e', f')\) are often called blocks of \( g \) and \( h \).

The question on the structure of the equality set \( \text{Eq}(g, h) \) can be seen as a special case of the above considerations. If conditions

\[ u = v, \quad u_1 = v_1, \quad u_2 = v_2, \quad c = d, \quad c' = d', \quad e = f, \quad e' = f', \]

are added, then we get the following modification of Lemma 15, Lemma 18 and Corollary 16 with analogical proofs, which we omit.
Lemma 20. Let $g$ and $h$ be binary morphisms, and let $g$ be marked. Let $u \in A^*$ be a word such that $g(u) \bowtie h(u)$ and
$$g(u) \neq h(u)z_h.$$ Let $u_1, u_2 \in A^+$ be words such that
$$g(uu_1) = h(uu_1),$$
$$g(uu_2) = h(uu_2).$$ Then $\text{pref}_1(u_1) = \text{pref}_1(u_2)$.

Corollary 21. Let $g$ and $h$ be binary morphisms, and let $g$ be marked. Let $c$ and $c'$ be distinct elements of $\text{eq}(g,h)$. Put $u = c \wedge c'$. Then
$$g(u) = h(u)z_h.$$ Let $e$ be an element of $A^+$ satisfying the following conditions:
(i) $z_h g(e) = h(e)z_h$
(ii) The word $e$ is minimal, i.e.: If $e_1$ is a proper prefix of $e$ then $z_h g(e_1) \neq h(e_1)z_h$.
Then the word $e$ is determined uniquely by its first letter.

Lemma 22. Let $g$ and $h$ be binary morphisms, and let $g$ be marked. Let the word $e \in A^+$ satisfy the following conditions:
(A) The rank of $\text{Eq}(g,h_m)$ is at most two.
(B) If the rank of $\text{Eq}(g,h_m)$ is two and $\text{eq}(g,h_m) = \{e, e'\}$, then $\text{pref}_1(e) \neq \text{pref}_1(e')$.

Note that the previous lemma proves Theorem 2 for morphisms, which are marked from both sides. In the rest of the paper we show that this is essentially the only situation in which the equality set can have rank greater than one.

Marked morphisms are in general much easier to deal with. That’s why it is convenient to work with principal pairs, where one of the morphisms, say $g$, is marked. Moreover, it is always possible to use the marked version $h_m$ instead of $h$ to get a marked pair, and thus a better insight into the coincidence set of $g$ and $h$.

The block structure of the coincidence set of marked morphisms leads to an important concept of successor morphisms. Consider marked morphisms $g$ and $h$, such that $c(g,h)$ consists of two blocks $(e,f)$ and $(e',f')$. Let $w$ be an element of $\text{Eq}(g,h)$. The equality $g(w) = h(w)$ can be uniquely split into a sequence of blocks. This means that $w$ is an element of $\{e,e'\}^+$, and in the same time an
element of $\{f, f'\}^+$. It is now natural to define the successor morphisms $(g_1, h_1)$ by
\[
\begin{align*}
g_1(a) &= e, & h_1(a) &= f, \\
g_1(b) &= e', & h_1(b) &= f',
\end{align*}
\]
and to formulate the previous considerations by the following lemma.

**Lemma 24.** Let $g, h$ be marked morphisms such that
\[
\mathcal{C}(g, h) = \{(e, f), (e', f')\}.
\]
Then the morphisms $g_1, h_1$ defined by (5) are marked. If $w \in \text{Eq}(g, h)$, then there is a unique word $w_1 \in \text{Eq}(g, h)$ such that
\[
g_1(w_1) = h_1(w_1) = w.
\]

**Proof.** The morphisms $g_1$ and $h_1$ are marked, by Lemma 19. The existence and uniqueness of the word $w_1$ follows from $(w, w) \in \mathcal{C}(g, h)$, and from Lemma 3.

The construction of successors can be iterated (that is the successor morphisms can themselves have successors). An interested reader can see the Appendix, where some properties of the sequence of successor morphisms are described.

## 6 The counterexample and its structure

We now have all necessary ingredients for the proof of our main claim, Theorem 2. The course of the prove will be essentially by contradiction. We shall assume that there exists a counterexample to the claim, and gradually show that such an assumption is contradictory. For a sketch of what follows see Section 2.

We first formulate what is understood as a counterexample.

**Definition 25.** We say that a pair of morphisms $(g, h)$ is a counterexample if
\begin{enumerate}
\item[(a)] The rank of $\text{Eq}(g, h)$ is at least two;
\item[(b)] $g$ is marked and $h$ is not marked;
\item[(c)] $|g(a)| > |h(a)|$ and $|g(b)| < |h(b)|$.
\end{enumerate}

The third condition takes advantage of the symmetry of letters $a$ and $b$. Note that the strict inequalities do not harm generality, since $|g(a)| = |h(a)|$ or $|g(b)| = |h(b)|$ would imply $g = h$. Since the letters $a$ and $b$ are not interchangeable anymore, we shall sometimes need the morphism $\pi$ defined by $\pi(a) = b$ and $\pi(b) = a$.

The following lemma yields basic information about the structure of the equality set of a counterexample.
**Lemma 26.** Let \((g, h)\) be a counterexample. Then there exist non-empty words \(\sigma, \nu_a\) and \(\nu_b\) such that

\[
\begin{align*}
\text{pref}_1(\nu_a) &= a, \\
\text{pref}_1(\nu_b) &= b,
\end{align*}
\]

the words \(\sigma \nu_a\), \(\sigma \nu_b\) are two distinct elements of \(\text{eq}(g, h)\) and

\[
\begin{align*}
g(\sigma) &= h(\sigma) z_h, \\
z_h g(\nu_a) &= h(\nu_a), \\
z_h g(\nu_b) &= h(\nu_b).
\end{align*}
\]

\(\text{(*)}
\)

\(\text{(**a)}
\)

\(\text{(**b)}
\)

\[
\begin{array}{c}
g: \\
\sigma \\
\downarrow \\
z_h \\
\nu_a \\
\uparrow \\
\nu_b \\
h:
\end{array}
\]

**Proof.** Let \(u\) and \(v\) be two distinct elements of \(\text{eq}(g, h)\). Put \(\sigma = u \land v\), and let \(u_1\) and \(v_1\) be such that \(\sigma u_1 = u\), \(\sigma v_1 = v\). Corollary 21 implies that \(\text{pref}_1(u_1) \neq \text{pref}_1(v_1)\). The choice of \(\nu_a\) and \(\nu_b\) is now obvious. The equalities \(\text{(*)}\), \(\text{(**a)}\) and \(\text{(**b)}\) are yielded by Corollary 21.

The equalities \(\text{(*)}\), \(\text{(**a)}\) and \(\text{(**b)}\) have special tags, since they are of a special importance, and will be used very often in the sequel. They represent two points, where the structure of a counterexample is well defined, and which therefore yield information for a combinatorial analysis.

The following lemma makes sure that the counterexample defined above deserves its name.

**Lemma 27.** Theorem 2 holds if and only if there is no counterexample.

**Proof.** Suppose that there is a counterexample. Then Theorem 2 does not hold, by Lemma 26.

Suppose that Theorem 2 does not hold, and let \(g\) and \(h\) be such that \(\text{eq}(g, h)\) contains two elements \(\alpha\) and \(\beta\) with the same first letter. By Lemma 13, we can suppose that the morphisms are principal, and by Lemma 14, we have that one of the morphisms is marked. We can suppose that \(g\) is marked, by symmetry. Similarly, by the symmetry of \(a\) and \(b\), we can suppose that the condition \(\text{(c)}\) of Definition 25 is satisfied. It remains to show that \(h\) is not marked. If \(h\) is marked, the both morphisms are marked, and \(\text{pref}_1(\alpha) \neq \text{pref}_1(\beta)\), by Lemma 23.

The further strategy is to show that there is no counterexample. We shall divide the investigation into several stages.

### 7 When \(z_h\) commutes

In this section we investigate two special situations, in which \(z_h\) commutes with one of the image words. We show that those situations lead to a contradiction.
We start with a technical lemma, which will be the core of the proof. In the original version of this paper the claim had the following general form:

**Lemma.** Let $g, h : A^* \to A^*$ be two marked morphisms. Let $u, u', v$ and $v' \in A^*$ be words, and $s, r, q$ positive integers, such that

$$g(a^s bu) = h(a^s bu'), \quad g(a^r bv) = h(a^q bv').$$

Then $s = r = q$.

However, as Markku Laine pointed out by constructing an example, this claim does not hold. The example is as follows.

**Example 28.** Let

$$g(a) = a^2 b^2, \quad h(a) = a,$$

$$g(b) = b, \quad h(b) = b^2.$$  

Then

$$g(a^2 b^2) = h(a^3 b^2 b) = a^2 b^2 a^2 b^4,$$

and

$$g(ab^2) = h(a^2 b^2) = a^2 b^4.$$  

We therefore present a bit weaker version, which fits the purpose of this paper.

**Lemma 29.** Let $g, h : A^* \to A^*$ be two marked morphisms. Let $u$ and $v \in A^*$ be words, and $s, r, q$ positive integers, such that

$$g(a^s bu) = h(a^s bu), \quad g(a^r bv) = h(a^q bv).$$

Then $s = r = q$.

**Proof.** Recall that we suppose $g \neq h$. (For $g = h$ only $r = q$ holds, as it is easy to see.) Let $g$ and $h$ be morphisms satisfying assumptions, and suppose that $s = r = q$ does not hold. Assume, moreover, that the length of $a^s bu$ is smallest possible. We show that $a^s bu$ can be shortened, and hence obtain a contradiction.

We first prove that $g(a)$ and $h(a)$ do not commute. Suppose for a while that $|g(a)| > |h(a)|$, and that $t$ is the common primitive root of $g(a)$ and $h(a)$. From (6) we deduce that $h(b)$ is comparable with $h(a^s)^{-1} g(a^s)$, which is an element of $t^+$. That is a contradiction with $h$ being marked. Similarly if $|g(a)| < |h(a)|$.

(Clearly, $g(a) = h(a)$ implies $g = h$.)

Let us continue the proof of the lemma. By Corollary 16,

$$g(a^s bu \wedge a^r bv) = h(a^s bu \wedge a^q bv).$$

18
1. If \( s \neq r \) and \( s \neq q \), then (8) yields 
\[
g(a^i) = h(a^j),
\]
with \( i = \min(s, r) \), \( j = \min(s, q) \). Therefore the words \( g(a) \) and \( h(a) \) commute, a contradiction.

2. Suppose next, by symmetry, \( s = r \) and \( s \neq q \). Put \( m = \min(s, q) \). Equality (8) implies 
\[
g(a^s bw) = h(a^m),
\]
where \( w = u \land v \).

The set \( \mathbb{C}(g, h) \) contains elements \( (a^s bu, a^s bu) \) and \( (a^s bw, a^m) \), whence it is not difficult to see that the rank of \( \mathbb{C}(g, h) \) is two. Let \( (e, f) \) and \( (e', f') \) be the blocks of \( g \) and \( h \), and let \( g_1, h_1 \) be their successor morphisms defined by (5).

By symmetry, suppose that \( \text{pref}_1(f) = a \). Equality (9) implies that there is a positive integer \( p \), such that \( f = a^p \). Since \( g(a) \) and \( h(a) \) do not commute, we deduce that \( e \not\in a^+ \) and thus \( |e| > s \). Since \( a^s bu \) and \( a^q bv \) are elements of \( \{f, f'\}^* \), both \( s \) and \( q \) are multiples of \( p \). Put 
\[
s_1 = \frac{s}{p}, \quad q_1 = \frac{q}{p},
\]
and define words \( u_1 \) and \( v_1 \) by 
\[
g_1(u_1) = a^s bu, \quad h_1(u_1) = a^s bu, \\
g_1(v_1) = a^q bv, \quad h_1(v_1) = a^q bv.
\]

Since \( f = a^p \), the words \( u_1 \) and \( v_1 \) can be factorized as 
\[
u_1 = a^{s_1} bu_2, \quad v_1 = a^{q_1} bv_2,
\]
with \( u_2, v_2 \in A^+ \). Therefore 
\[
g_1(a^{s_1} bu_2) = h_1(a^{s_1} bu_2) = a^s bu, \\
g_1(a^{q_1} bv_2) = h_1(a^{q_1} bv_2) = a^q bv.
\]

Inequality \( s \neq q \) implies \( s_1 \neq q_1 \), and \( |e| > s \) yields \( |a^{s_1} bu_2| < |a^s bu| \). This completes the proof.

The following two claims exploit the previous lemma. The words \( \sigma, \nu_a \) and \( \nu_b \) are as in Lemma 26.

Claim 1. There is no counterexample such that \( z_h \) commutes with \( g(b) \) and \( \text{pref}_1(\sigma) = b \).
Proof. Suppose that \((g, h)\) is a counterexample. Let \(b^l\) be the maximal \(b\)-prefix of \(\sigma\) and \(b^k\) be the maximal \(b\)-prefix of \(\nu_0\sigma\). We have

\[
z_h = t^{m_1}, \quad g(b) = t^{m_2},
\]

with some primitive word \(t\) and some positive integers \(m_1, m_2\).

Then (**b) yields that \(t^{m_1+k}m_2\) is the maximal \(t\)-prefix of \(z_h\nu_0\sigma\). Similarly, from (*) it follows that \(t^{\ell}m_2\) is the maximal \(t\)-prefix of \(h(\sigma\nu_0)\).

1. Suppose that \(h(b) = t^{m_3}\) for some \(m_3 \in \mathbb{N}_+\). Since \(|h(b)| > |g(b)|\), the equality (*) implies that \(g(a)\) is comparable with \(t^{\ell}(m_3-m_2)\), a contradiction with \(g\) being marked.

2. This implies, by Periodicity Lemma, that the maximal \(t\)-prefix of \(h(b)z_h\) is shorter than \(|h(b)t|\). Hence \(t^{\ell}m_2\) is the maximal \(t\)-prefix of any word \(h(bu)z_h\), \(u \in A^*\).

The equality (**b) now implies

\[
m_1 + k \cdot m_2 = \ell \cdot m_2.
\]

Thus

\[
m_1 = (\ell - k) \cdot m_2
\]

and \(z_h = g(b)^{\ell-k}\).

Put \(\sigma' = b^{-s}\sigma\). Then

\[
z_hg(\sigma') = h(b^s\sigma')z_h, \quad z_h\nu_0\sigma = h(\nu_0\sigma)z_h,
\]

and Lemma 29, applied to morphisms \(h_m \circ \pi\) and \(g \circ \pi\), yields a contradiction.

\[
\Box
\]

Claim 2. There is no counterexample such that \(z_h\) commutes with \(h(a)\), \(\text{pref}_1(\sigma) = a\), and the common primitive root of \(z_h\) and \(h(a)\) is a suffix of \(g(a)\).

Proof. Suppose that \((g, h)\) is a counterexample. Let

\[
z_h = t^{m_1}, \quad h(a) = t^{m_2}
\]

for a primitive word \(t\) and some \(m_1, m_2 \in \mathbb{N}_+\). Let \(a^l\) be the maximal \(a\)-prefix of \(\sigma\nu_0\) and \(a^k\) be the maximal \(a\)-prefix of \(\nu_0\sigma\). By (1), the word \(z_h\) is the maximal \(t\)-prefix of every \(h(bu)z_h\). Whence the word \(t^{\ell}m_2+m_1\) is the maximal \(t\)-prefix of \(g(\sigma\nu_0)\). The maximal \(t\)-prefix of \(h(\nu_0\sigma)\) is \(t^{k}m_2+m_1\).

1. First suppose that \(g(a) = t^{m_3}\) for some \(m_3 \in \mathbb{N}_+\). Since \(g\) is marked, the word \(t^{k}m_2\) is the maximal \(t\)-prefix of \(g(\nu_0\sigma)\). From (**a) we have

\[
k \cdot m_3 + m_1 = k \cdot m_2 + m_1, \quad (10)
\]

and \(m_2 = m_3\), a contradiction with \(|g(a)| > |h(a)|\).
2. Since \( g(a) \notin t^+ \), and \( t \) is a suffix of \( g(a) \), the maximal \( t \)-prefix of \( g(\sigma \nu_h) \), namely \( t^\ell \cdot m_2 + m_1 \), is also the maximal \( t \)-prefix of \( g(a) \). The equality (**a) now yields
\[
k \cdot m_2 + m_1 = \ell \cdot m_2 + 2 \cdot m_1
\]
and \( z_h = h(a)^{k-\ell} \).

From (*) and (**a) we obtain
\[
z_h g(\sigma) = h(a^* \sigma) z_h, \quad z_h g(\nu_a \sigma) = h(\nu_a \sigma) z_h.
\]

Verify that morphisms \( h_m, g \) satisfy the assumptions of Lemma 29, a contradiction.

\[\Box\]

8 Case: \( \overline{g} \) is not marked

In this section we deal with the situation when \( \overline{g} \) is not marked. Note that then \( \overline{h} \) is marked, by Lemma 14. By symmetry of \( g \) and \( h \), and by the mirror symmetry, we can also suppose
\[
|z_g| \geq |z_h|.
\]
(11)

More precisely, if \( |z_g| < |z_h| \), then we consider \( (\overline{h} \circ \pi, \overline{g} \circ \pi) \), which is also a counterexample, instead of \( (g, h) \). Recall that \( \pi \) exchanges letters \( a \) and \( b \), and it is applied in order to satisfy the condition (c) of Definition 25 of the counterexample.

The mirror variant of (1) implies that \( z_g \) is a suffix of any \( g(u) \) enough long. Especially,
\[
z_g \in \text{suff}(g(a)^+), \quad z_g \in \text{suff}(g(b)^+).
\]
(12)

Thus also (see the picture)
\[
z_h \in \text{suff}(z_g).
\]
(13)

The following claim excludes the situation of this section.

Claim 3. There is no counterexample with \( \overline{g} \) not marked.

Proof. Suppose that \((g, h)\) is a counterexample.

21
1. Suppose first $\text{pref}_1(\sigma) = a$. The equality (*) yields $h(a) \in \text{pref}(g(a))$, and (**a) implies that $h(a)z_h$ is a prefix of $z_hg(a)$. Thus $z_hh(a) = h(a)z_h$.

Let $t$ be the common primitive root of $h(a)$ and $z_h$. From (13) we deduce that $t$ is a suffix of $z_h$, and the first line of (12) together with $|g(a)| > |h(a)| \geq |t|$ yields that $t$ is a suffix of $g(a)$. This is a contradiction with Claim 2.

2. Suppose then that $\text{pref}_1(\sigma) = b$. From (13) and (12) we deduce that $z_hg(b)$ is a suffix of $g(b)^+$. Equalities (*) and (**b) imply that $g(b)$ is a prefix of $z_hg(b)$. Therefore Lemma 7(D) yields that $g(b)$ and $z_h$ commute, a contradiction with Claim 1.

\[ \square \]

9 Case: $\overline{h}$ is not marked

In this subsection we consider the situation when $\overline{g}$ is marked and $\overline{h}$ is not. We shall not exclude this case directly. Instead we reduce it to the case when both $\overline{g}$ and $\overline{h}$ are marked.

To accomplish this plan we first we need a description of the possible counterexample structure, which is more precise than Lemma 26.

Lemma 30. Let $(g, h)$ be a counterexample. Then one of the following possibilities takes place.

(A) There exist words $\sigma, \mu_a, \mu_b \in A^+$, and $\tau \in A^*$ such that

$$\text{eq}(g, h) = \{\sigma \mu \tau, \sigma \mu_h \tau\},$$

where

$$z_hg(\mu_a)z_h = h(\mu_a), \quad g(\sigma) = h(\sigma)z_h,$$

$$z_hg(\mu_b)z_h = h(\mu_b), \quad g(\tau) = z_hh(\tau),$$

and

$$\text{pref}_1(\mu_a) = a, \quad \text{pref}_1(\mu_b) = b, \quad \text{suff}_1(\mu_a) \neq \text{suff}_1(\mu_b).$$

(B) There exist words $\zeta, \mu, \rho, \tau \in A^+$ such that

$$\text{eq}(g, h) = \zeta(h(\mu)^+ \rho \tau = \zeta \rho(\mu \rho)^* \tau,$$
Let \( g(z) = h(z) \), \( z_h g(\mu)z_h = h(\mu) \), \( \text{pref}_1(\mu) \neq \text{pref}_1(\tau) \).
\[
g(\rho) = z_h^\infty h(\rho)z_h, \quad z_h g(\tau) = h(\tau), \quad \text{suff}_1(\mu) \neq \text{suff}_1(\tau) .
\]

**Proof.** Let \( \alpha \) and \( \beta \) be two shortest elements of \( \text{eq}(g, h) \). Put \( \sigma = \alpha \land \beta \), and similarly let \( \tau \) be the longest common suffix of \( \alpha \) and \( \beta \). By Corollary 21, applied first to \( g \) and \( h \), and then to \( \overline{g} \) and \( \overline{h} \), we have
\[
g(\sigma) = h(\sigma)z_h, \quad (14)
g(\tau) = z_h^\infty h(\tau). \quad (15)
\]
Denote by \( v_0 \) and \( v_1 \) the words \( \sigma^{-1}\alpha \) and \( \sigma^{-1}\beta \). Clearly, \( \text{pref}_1(v_0) \neq \text{pref}_1(v_1) \).

1. First suppose that \( v_0 \) and \( v_1 \) are not suffix-comparable. Then with a suitable choice of \( i, j \in \{0, 1\} \) we have \( v_i = \mu_i \tau, v_j = \mu_j \tau, \) and \( \text{pref}_1(\mu_\ell) = \ell \) for both \( \ell \in A \).

Therefore \( \{\sigma \mu_0 \tau, \sigma \mu_1 \tau\} = \{\alpha, \beta\} \). We show that \( \sigma \) is the unique prefix of \( \alpha \) (\( \beta \) resp.) satisfying (14).

Suppose first that \( \sigma \alpha_2 = \sigma \) and \( g(\sigma_1) = h(\sigma_1)z_h \). Then it is easy to see that also \( \sigma v_i \in \text{Eq}(g, h), i = 1, 2 \), a contradiction with \( \alpha \) and \( \beta \) being the shortest elements of \( \text{eq}(g, h) \).

Let then \( v_i = w_i w_2 \), for some \( i \in \{0, 1\} \), and \( g(\sigma w_1) = h(\sigma w_1)z_h \). Then \( \sigma w_2 \) is an element of \( \text{Eq}(g, h) \), which is shorter than \( \sigma v_i \). Since \( \alpha \) and \( \beta \) are shortest elements of \( \text{eq}(g, h) \), it remains that \( \sigma w_2 = \sigma v_{1-i} \). But then \( v_0 \) and \( v_1 \) are suffix-comparable, a contradiction.

We still have to show that the set \( \{\alpha, \beta\} \) generates whole \( \text{Eq}(g, h) \). Suppose that \( w \) is an element of \( \text{Eq}(g, h) \) such that neither \( \alpha \), nor \( \beta \) are prefixes of \( w \), and consider words \( w_\alpha = w \land \alpha \) and \( w_\beta = w \land \beta \). It is easy to deduce that either \( w_\alpha \) is a prefix of \( \alpha \) distinct from \( \sigma \), or \( w_\beta \) is a prefix of \( \beta \) distinct from \( \sigma \). Take the first possibility (the second being similar). Corollary 21 implies that \( g(w_\alpha) = h(w_\alpha)z_h \), a contradiction with the previous paragraph.

Consequently, we have the case (A).

2. Suppose now, by symmetry, that \( v_1 = uv_2 \). Then \( z_h g(u) = h(u)z_h \) and \( \sigma u^* v_2 \) is a subset of \( \text{Eq}(g, h) \). Moreover, \( \sigma \) and \( \sigma u \) are the only prefixes of \( \sigma u v_2 \) satisfying (14). The proof is similar as above: any other prefix satisfying (14) allows to drop a part of the word, which contradicts the minimality of \( \alpha \) and \( \beta \). We omit details. This, in particular, implies that \( u \) and \( \sigma \) are not suffix-comparable.

23
We show that $\sigma u^* v_2$ generates the whole equality set. Suppose the contrary, and let $w$ be the shortest element of $\text{Eq}(g, h)$, not generated by $\sigma u^* v_2$. Then the words $w_1 = w \land \sigma v_2$ and $w_2 = w \land \sigma u^* v_2$ satisfy $g(w_i) = h(w_i) z_i$, $i = 1, 2$. Therefore $w_1 = \sigma$, by the previous paragraph. From $\text{pref}_1(u) \neq \text{pref}_1(v_2)$, one obtains that $w_2$ is strictly longer than $\sigma$, which implies $w_2 = \sigma u$. Therefore $w = \sigma u v'$, whence $\sigma u v'$ is an element of $\text{Eq}(g, h)$, shorter than $w$, and thus generated by $\sigma u^* v_2$. It is now easy to see that also $w$ is generated by $\sigma u^* v_2$, a contradiction.

Since $u$ and $\sigma$ are not suffix-comparable, we can define $\rho$ as the longest common suffix of $u$ and $\sigma$, and denote, $\tau = v_2$, $\zeta = \sigma \rho^{-1}$ and $\mu = u \rho^{-1}$.

Note that the word $\rho \tau$ is the longest common suffix of $\alpha$ and $\beta$. Corollary 21 applied to $(g, h)$ yields $g(\rho \tau) = z h(h(\rho \tau))$. The verification of all claims in case (B) is now straightforward.

\[\Box\]

Note that the previous lemma proves, in particular, Theorem 1(C). The following lemma allows to suppose that both $\overline{g}$ and $\overline{h}$ are marked, which was the task of this section.

**Claim 4.** Let $(g, h)$ be a counterexample. Then there exists also a counterexample $(g_1, h_1)$ such that both $\overline{g_1}$ and $\overline{h_1}$ are marked.

**Proof.** Suppose that $(g, h)$ is a counterexample. Suppose that $\rho \tau \neq \varepsilon$ and define $g_1$ and $h_1$ by

$$g_1(u) = g(u), \quad h_1(u) = \overline{\rho} \cdot h(u)(\overline{\rho})^{-1}.$$ 

It is not difficult to see that morphism $h_1$ is well defined. The claim is now a consequence of the characterization presented in Lemma 30. Let words $\zeta$, $\sigma$, $\tau$, $\rho$, $\mu_a$, $\mu_b$, and $\mu$ be as in that lemma.

1. If the case (A) of Lemma 30 takes place, then

$$\text{eq}(g, h) = \{\tau \sigma \mu_a, \tau \sigma \mu_b\}.$$ 

2. If, on the other hand, we have the case (B) of the Lemma 30, then

$$\text{eq}(g, h) = \{\rho \mu, \rho \tau \zeta\}.$$ 

The words $\tau \sigma$ and $\rho$ are non-empty, $g_1$ is marked, and $h_1$ is not. Thus $(g_1, h_1)$ is a counterexample with $\overline{g_1}$ and $\overline{h_1}$ marked. \[\Box\]
10 The case $\overline{g}$ and $\overline{h}$ marked.

From now on we shall suppose that both $\overline{g}$ and $\overline{h}$ are marked. Consider Lemma 30. It is easy to note that the case (A) of the lemma has to take place, and moreover, the word $\tau$ is empty. Therefore

$$eq(g, h) = \{\sigma \mu_a, \sigma \mu_b\},$$

with $pref_1(\mu_a) = a$, $pref_1(\mu_b) = b$, and $suff_1(\mu_a) \neq suff_1(\mu_b)$.

Note the following useful fact.

**Lemma 31.** Let $(g, h)$ be a counterexample such that $\overline{g}$ and $\overline{h}$ marked. Put $g_1 = g$ and $h_1 = h_m$. Then the pair $(g_1, h_1)$ is again a counterexample, such that $g_1$ and $h_1$ is marked, and

$$eq(g_1, h_1) = \{\overline{\sigma \mu_a}, \overline{\sigma \mu_b}\}.$$

**Proof.** The verification is straightforward. \[\square\]

10.1 The case: $pref_1(\sigma) = a$ or $suff_1(\sigma) = a$

In this subsection we show that the word $\sigma$ of a counterexample cannot start nor end by the letter $a$.

Since $|g(a)| > |h(a)|$ and $suff_1(\mu_c) = a$ for some $c \in A$, we have

$$h(a) \in suff(g(a)). \quad (16)$$

**Claim 5.** There is no counterexample such that both $\overline{g}$ and $\overline{h}$ are marked and $pref_1(\sigma) = a$ or $suff(\sigma) = a$.

**Proof.** Let first $pref_1(\sigma) = a$. As in the proof of Claim 3 we obtain that $z_h$ and $h(a)$ have a common primitive root, say $t$. From (16) we have that $t$ is a suffix of $g(a)$, which yields a contradiction with Claim 2.

The case $suff_1(\sigma) = a$ follows from the same considerations for morphisms $\overline{g}$ and $\overline{h}_m$, by Lemma 31. \[\square\]

10.2 The case: $pref_1(\sigma) = b$ and $suff_1(\sigma) = b$

This is the final, most complicated part of the proof of Theorem 2.

In the rest of the section we shall implicitly suppose that $(g, h)$ is a counterexample such that $\overline{g}$ and $\overline{h}$ are marked, and $pref_1(\sigma) = suff_1(\sigma) = b$. The subsection consists of four lemmas and four claims. We first fix some notation.

**Convention 32.**

- Denote by $\xi$ the word $\mu_a$ or $\mu_b$ such that $suff(\xi) = b$.
- Denote by $\ell$ the maximal integer such that $b^\ell$ is a prefix of $\sigma$.
- Denote by $k$ the maximal integer such that $b^k$ is a prefix of $\mu_b$.
- Denote by $\ell'$ the maximal integer such that $b^{\ell'}$ is a suffix of $\xi$. 

25
• Denote by \( k' \) the maximal integer such that \( b^{k'} \) is a suffix of \( \sigma \).

From Definition 25(d) and from (*) we obtain, by a length argument, that \( \sigma \) contains at least one \( a \).

Now we present four lemmas.

**Lemma 33.** The words \( g(b) \) and \( h(b) \) do not commute.

*Proof.* Suppose, for a contradiction, that \( t \) is the common primitive root of \( g(b) \) and \( h(b) \). Since \( |g(b)| < |h(b)| \), we deduce, by (*), that the first occurrence of \( g(a) \) in \( g(\sigma) \) is comparable with \( t \), a contradiction with \( g \) being marked. \( \square \)

**Lemma 34.**

\[ |h(b)| > (\ell + \ell' - 1)|g(b)|. \]

*Proof.* The word \( h(b) \) is comparable with \( g(b)^\ell \) and suffix-comparable with \( g(b)^{\ell'} \). If \( |h(b)| \leq (\ell + \ell' - 1)|g(b)| \), then \( g(b) \) and \( h(b) \) commute, by Lemma 7, a contradiction with Lemma 33.

**Lemma 35.**

\[ |z_h| > (\ell + k' - 1)|g(b)|. \]

*Proof.* The word \( z_h \) is comparable with \( g(b)^\ell \), since \( z_h \) is comparable with \( h(b) \), and \( g(b)^\ell \) is a prefix of \( h(b) \). Also \( z_h \) is suffix-comparable with \( g(b)^{k'} \), by (**b). First suppose that \( |z_h| \geq |g(b)| \). Now, if \( |z_h| \leq (\ell + k' - 1)|g(b)| \), then \( z_h \) and \( g(b) \) commute, by Lemma 7, a contradiction with Claim 1.

Suppose now that \( z_h \) is shorter than \( g(b) \). Recall that \( g(b) \) is a prefix of \( g(\mu b) \), prefix of \( h(b) \), and a suffix of \( g(\sigma) \). From (**b) we deduce that \( g(b) = sz_h \) and at the same time \( g(b) = z_h s \). Again, the words \( g(b) \) and \( z_h \) commute, a contradiction.

**Lemma 36.** Let \( (g, h) \) be a counterexample such that \( h(b) \) is a prefix of \( g(b' a) \), and let \( k \geq \ell \). Then \( h(b) \) commutes with \( z_h g(b)^{k - \ell} \).

---

26
Proof. From (*) and Lemma 34 we deduce that \( h(b) = g(b)^\ell u \) for some prefix \( u \) of \( g(a) \). Since \( |h(b)| > |g(b)| \) and \( \ell \geq 1 \), we have
\[
|h(b)^k z_h| > |z_h g(b)^{k-\ell} h(b)|.
\]
The equality (**b) now implies that the word \( z_h g(b)^{k-\ell} g(b)^\ell u = z_h g(b)^{k-\ell} h(b) \) is a prefix of \( h(b)^* \) and thus \( z_h g(b)^{k-\ell} \) commutes with \( h(b) \), by Lemma 4. \( \square \)

We can now conclude the proof. The remaining cases are divided into four claims.

Claim 6. There is no counterexample such that \( g(b^i a) \) is a prefix of \( h(b) \). Similarly, there is no counterexample such that \( g(ab^j) \) is a suffix of \( h(b) \).

Proof. In this proof we shall consider occurrences of \( g(b)s \) and \( h(b)s \) in \( g(\sigma) \) and \( h(\sigma) \), and their relative position. The idea is quite intuitive, but we give a more formal definition. Let \( i, j \leq |\sigma|_b \) be positive integers. Denote by \( u_i \) the prefix of \( \sigma \) such that also \( u_i b \) is a prefix of \( \sigma \), and \( |u_i b|_b = i \).

We say that the \( i \)th occurrence of \( g(b) \) in \( g(\sigma) \) starts within the \( j \)th occurrence of \( h(b) \) in \( h(\sigma) \), if
\[
|h(u_j)| \leq |g(u_i)| < |h(u_i b)|.
\]
Similarly, we say that the \( i \)th occurrence of \( g(b) \) in \( g(\sigma) \) ends within the \( j \)th occurrence of \( h(b) \) in \( h(\sigma) \), if
\[
|h(u_j)| < |g(u_i b)| \leq |h(u_i b)|.
\]

From Lemma 35 it follows that the last occurrence of \( g(b) \) in \( g(\sigma) \) both starts and ends outside \( h(\sigma) \). Therefore, by the pigeon hole principle, there is an occurrence of \( h(b) \) in \( h(\sigma) \) such that no occurrence of \( g(b) \) in \( g(\sigma) \) starts within it. Similarly, there is an occurrence of \( h(b) \) in \( h(\sigma) \) within which no \( g(b) \) ends.

From this it is easy to deduce that \( h(b) \) is either a factor of \( g(a)^+ \), or it is both prefix of \( sg(a)^+ \) and a suffix of \( g(a)^+ p \), where \( s \) is a proper suffix, and \( p \) a proper prefix of \( g(b) \). Consider the second possibility. From the fact that \( g(b^i) g(a) \) is prefix of \( sg(a)^+ \) we deduce that \( \overline{g} \) is not marked, by Lemma 7, a contradiction.

Similarly, we obtain a contradiction with the markedness of \( g \) or \( \overline{g} \) in the remaining cases. \( \square \)

Claim 7. There is no counterexample such that \( k > \ell \).

Proof. By Claim 6, we can suppose that \( h(b) \) is a prefix of \( g(b^i a) \), and Lemma 36 implies that the words \( h(b) \) and \( z_h g(b)^{k-\ell} \) commute.

Lemma 35 implies that the maximal \( g(b) \)-suffix of \( z_h g(b)^{k-\ell} \) is \( g(b)^{k-\ell+k'} \). The maximal \( g(b) \)-suffix of \( h(b) \) is \( g(b)^{\ell'} \). Since \( h(b) \) and \( z_h g(b)^{k-\ell} \) commute, we have \( k - \ell + k' = \ell' \), and thus \( \ell' > k' \).

By Lemma 36 applied to \( (\overline{g}, h_m) \), the word \( h(b) \) commutes also with \( g(b)^{k' - \ell'} z_h \). Therefore \( z_h g(b)^{k-\ell} = g(b)^{k' - \ell'} z_h \), and the words \( z_h \) and \( g(b) \) commute. The rest is Claim 1. \( \square \)
Claim 8. There is no counterexample such that \( k < \ell \).

Proof. Again, we can suppose that \( h(b) \) is a prefix of \( g(b'a) \), by Claim 6. Let \( u \) be a prefix of \( g(a) \) such that \( g(b'u) = h(b) \). Thus

\[
|g(b')u g(b')^{\ell - k}| < |g(b'a)|
\]

and, by (*), \( u g(b')^{\ell - k} \) is a prefix of \( g(a) \). From (**b) we deduce

\[
h(b) z_h = z_h g(b)^k u g(b)^{\ell - k}.
\]

Since \( |z_h| \geq |g(b')^{\ell - k}| \), by Lemma 35, the rear of the equality (17) yields \( z_h = sg(b)^{\ell - k} \) for some \( s \in A^* \), and it can be written as

\[
h(b) g(b)^{\ell - k} = g(b)^{\ell - k} g(b)^{k} u g(b)^{\ell - k} = sh(b) g(b)^{\ell - k}.
\]

Thus the words \( h(b) \) and \( s \) commute.

Consider the counterexample \((h_m, \mathcal{G})\). By Claim 7, we can suppose that \( k' \geq \ell' \), and as above we obtain that \( z_h = g(b)^{k' - \ell'} s' \), where \( s' \) commutes with \( h(b) \). Let \( t \) be the primitive root of \( h(b) \). We have

\[
z_h = t^i g(b)^{\ell - k} = g(b)^{k' - \ell'} t^j,
\]

for some positive integers \( i \) and \( j \). This implies that \( z_h \) commutes with \( g(b) \), by Lemma 4, and we are through, by Claim 1.

It remains to consider the situation when both \( k = \ell \).

Claim 9. There is no counterexample such that \( k = \ell \).

Proof. Let \((g, h)\) be a counterexample. The ground of this proof is an induction on the length of \( \sigma \mu_a \) and \( \sigma \mu_b \). Suppose therefore that those words are the shortest possible equality words of any counterexample \((g', h')\) satisfying that \( \mathcal{G} \) and \( \mathcal{H} \) are marked. We show that we can always find shorter words, which will prove the claim.

By Claim 6, we have that \( h(b) \) is a prefix of \( g(b'a) \). Lemma 36 and \( k = \ell \) now imply that \( z_h \) commutes with \( h(b) \); let \( t \) be their common primitive root. The maximal \( t \)-prefix of \( g(\mu_b) \) is \( z_h^{-1} h(b)^k z_h \), which equals \( h(b)^k \). Maximal \( t \)-prefix of \( g(\sigma) \) is \( h(b)^k z_h \). Consequently, by Lemma 8, there is a prefix \( w \) of both \( \sigma \) and \( \mu_b \) such that \( h(b)^k = g(w) \).
Since morphisms $\varphi$ and $\overline{h}$ are marked, it is convenient to rewrite the above equality as
$$\varphi (\overline{u}) = \overline{h} (b^k).$$
(18)
Whence
$$c(\varphi, \overline{h}) = \{(e, f), (e', f')\},$$
where $f' \in b^+$ and $w \in (e')^+$. Define morphisms $g_1, h_1$ by
$$\left\{\begin{array}{ll}
g_1(a) = e, \\
g_1(b) = e',
\end{array}\right. \quad \left\{\begin{array}{ll}
h_1(a) = f, \\
h_1(b) = f'.
\end{array}\right.$$
Note that $(g_1, h_1)$ are successor morphisms of $(\varphi, \overline{h})$. The equalities
$$\overline{g} (\overline{mu} \overline{u}) = \overline{h} (\overline{mu} \overline{u}), \quad \overline{g} (\overline{mu} \overline{v}) = \overline{h} (\overline{mu} \overline{v})$$
imply that there are words $u, v$ such that
$$g_1(u) = h_1(u) = \overline{mu} \overline{u},$$
$$g_1(v) = h_1(v) = \overline{mu} \overline{v}.$$  
The equality (18) yields that $\text{suff}_1(u) = \text{suff}_1(v) = b$, since $w$ and $b^k$ are prefixes of $\sigma$.

This can be again rewritten as
$$\overline{g_1} (\overline{u}) = \overline{h_1} (\overline{u}) = \sigma \mu_u,$$
$$\overline{g_1} (\overline{v}) = \overline{h_1} (\overline{v}) = \sigma \mu_v,$$
with $\text{pref}_1(\overline{u}) = \text{pref}_1(\overline{v}) = b$. Obviously, $\overline{u}$ and $\overline{v}$ are shorter than $\sigma \mu_u$ and $\sigma \mu_v$. Moreover, the morphisms $g_1$ and $h_1$ are marked, by Lemma 19, since $\varphi$ and $\overline{h}$ are marked.

This completes the proof of Theorem 2. \qed

11 Test set

In this section we show that each binary language has a test set of cardinality at most two. The result is a consequence of Theorem 2.

Test set of a language $L \subset \Sigma^*$ is defined as a subset $T$ of $L$ such that the agreement of two morphisms on the language $T$ guarantees their agreement on $L$. Formally, for any two morphisms $g$ and $h$ defined on $\Sigma^*$
$$(\forall u \in T) \ (g(u) = h(u)) \Rightarrow (\forall v \in L) \ (g(v) = h(v)).$$

Let $L \subset A^*$ be a binary language. The ratio of a non-empty word $u \in L$ is denoted by $r(u)$ and defined by
$$r(u) = \frac{|u|_a}{|u|_b}.$$
If \( |u|_b = 0 \), then \( r(u) = \infty \). A word \( u \) is said to be ratio-primitive if no proper prefix of \( u \) has the same ratio as \( u \).

It is not difficult to see that each non-empty word \( u \) has a unique factorization

\[
u = u_1 \ldots u_k,
\]

where each \( u_i \) is a non-empty ratio-primitive word, such that \( r(u_i) = r(u) \). We call it the ratio-primitive factorization of \( u \).

**Theorem 37.** Let \( L \subset A^* \) be a language. Then \( L \) possesses a test set of cardinality at most two.

**Proof.** Consider morphisms \( g \) and \( h \) such that at least one of the inequalities \( |g(a)| \neq |h(a)| \) or \( |g(b)| \neq |h(b)| \) holds. It is then easy to see that

\[
|g(u)| = |h(u)| \iff r(u) = \frac{|h(b)| - |g(b)|}{|g(a)| - |h(a)|}.
\]  

(19)

This also implies that if \( u = u_1 u_2 \ldots u_n \) is the ratio-primitive factorization of \( u \), then \( g(u) = h(u) \) if and only if \( g(u_i) = h(u_i) \) for each \( i = 1, \ldots, n \).

Let \( R(L) \) denote the set of all ratio-primitive words \( u \), such that \( u \) occurs in the ratio-primitive factorization of at least one word in \( L \). It is obvious, from the previous paragraph, that \( g \) and \( h \) agree on \( L \) if and only if they agree on the language \( R(L) \). Moreover, any test set \( T \) of \( R(L) \) can be transformed into a test set \( T' \) of \( L \) of the same or smaller cardinality: it is enough to choose, for each word \( u \in R(L) \), a word \( v \in L \) such that \( u \) is contained in the ratio-primitive factorization of \( v \).

The above considerations allow to limit our investigation to languages consisting of ratio-primitive words. Let therefore \( L \) be such a language, and suppose that the cardinality of \( L \) is at least three. The test set \( T \) is constructed as follows.

(a) If \( L \) contains words \( u, v \) with \( r(u) \neq r(v) \), then \( T = \{u, v\} \).

(b) If all words in \( L \) have the same ratio, then \( T = \{u, v\} \) for some words \( u, v \in L \) such that \( \text{pref}_1(u) = \text{pref}_1(v) \).

We show that \( T \) is a test set of \( L \). Suppose that \( g \) and \( h \) agree on \( T \). Let also \( g \neq h \), the other possibility being trivial.

Note that \( uv \) contains both letters \( a \) and \( b \), since \( u \) and \( v \) are ratio-primitive. Therefore \( g(uv) = h(uv) \) and \( g \neq h \) imply that \( |g(a)| \neq |h(a)| \) and \( |g(b)| \neq |h(b)| \). By (19), the case (a) is excluded, and all words in \( \text{Eq}(g, h) \) have the same ratio. This implies that \( T \subset \text{eq}(g, h) \), since \( L \) contains only ratio primitive words.

By Theorem 1 and Theorem 2, the set \( \text{eq}(g, h) \) can contain two words with the same first letter, only if both morphisms are periodic. Therefore \( g \) and \( h \) agree on all words with the given ratio, thus, in particular, on whole \( L \). This completes the proof.

30
References


31
Appendix: Successors of marked morphisms

Lemma 38. Let $g_0, h_0 : A^* \rightarrow A^*$ be marked morphisms such that the rank of $\text{Eq}(g_0, h_0) = \{v_0, w_0\}^*$, is two. Then following statements hold.

(A) There exist a sequence of non-erasing marked morphisms $(g_i, h_i)_{i \in \mathbb{N}}$ such that for each $i \in \mathbb{N}$

$$C(g_i, h_i) = \{(e_i, f_i), (e'_i, f'_i)\}^*,$$

with

\[
\begin{align*}
& e_i = g_{i+1}(a), & f_i = h_{i+1}(a), \\
& e'_i = g_{i+1}(b), & f'_i = h_{i+1}(b),
\end{align*}
\]

and

\[
\begin{align*}
& \text{pref}_1(g_i(a)) = \text{pref}_1(h_i(a)) = a, \\
& \text{pref}_1(g_i(b)) = \text{pref}_1(h_i(b)) = b.
\end{align*}
\]

(B) For any $i < j$

$$E(g_i, h_i) = g_{i+1} \circ g_{i+2} \circ \cdots \circ g_j(E(g_j, h_j)).$$

(C) There exists a number $m$ such that $e_m = f_m$, $e'_m = f'_m$ and $e_i = f_i = a$, $e'_i = f'_i = b$ for all $i > m$.

Proof. The items (A) and (B) follow from Lemma 24 by induction. For item (C) it is enough to note that unless $|e_i| = |f_i| = |e_i| = |f_i| = 1$ the length of the word $v_i w_i$ is strictly decreasing. 

The construction of the sequence $(g_i, h_i)_{i \in \mathbb{N}}$ is similar to an idea used in the proof that Post Correspondence Problem is decidable in the binary case (see [4] and [9], where the idea is more explicit). The sequence has also the following interesting property.

Lemma 39. Let $i, j \geq 0$ and let

$$g_{i+j}(u) = h_{i+j}(v),$$

with $u \neq v$. Then $i + j < m$ and

$$g_i \circ g_{i+1} \circ \cdots \circ g_{i+j}(u) = h_i \circ h_{i+1} \circ \cdots \circ h_{i+j}(v)$$
if and only if $j$ is even.
Proof. By induction, it is enough to show

\[ g_i \circ g_{i+1}(u) \neq h_i \circ h_{i+1}(v) \]

and

\[ g_i \circ g_{i+1} \circ g_{i+2}(u) = h_i \circ h_{i+1} \circ h_{i+2}(v). \]

By definition, \( g_i(u') = h_i(v') \) if and only if \((u', v') \in \{(e_i, f_i), (e'_i, f'_i)\}^*\), i.e. if and only if there exist a word \( w \) such that \( u' = g_{i+1}(w), v' = h_{i+1}(w) \). But we suppose \( u \neq v \). On the other hand, if \( j = 2 \), put \( w = g_{i+2}(u) = h_{i+2}(v) \).

For \( k \geq m, e_k = f_k, e'_k = f'_k \) and thus \( g_k(u) = h_k(v) \) if and only if \( u = v \). Therefore \( i + j \) must be less than \( m \). \( \square \)