Decidability of the binary infinite Post Correspondence Problem

Vesa Halava*, Tero Harju, Juhani Karhumäki

Department of Mathematics, TUCS—Turku Centre for Computer Science, University of Turku, Turku FIN-20014, Finland

Received 5 December 2002; accepted 7 February 2003

Abstract

We shall show that it is decidable for binary instances of the Post Correspondence Problem whether the instance has an infinite solution. In this context, a binary instance \((h, g)\) consists of two morphisms \(h\) and \(g\) with a common two element domain alphabet. An infinite solution \(\omega\) is an infinite word \(\omega = a_1a_2\ldots\) such that \(h(\omega) = g(\omega)\). This problem is known to be undecidable for the unrestricted instances of the Post Correspondence Problem.

© 2003 Elsevier B.V. All rights reserved.

Keywords: Post Correspondence Problem; Infinite words; Decidability; Binary PCP

1. Introduction

Let \(A\) and \(B\) be two finite alphabets. In the Post Correspondence Problem, PCP for short, we are given two morphisms \(h, g: A^* \rightarrow B^*\) and we are asked whether or not there exists a nonempty word \(w \in A^*\) such that \(h(w) = g(w)\). The pair \((h, g)\) is called an instance of the PCP and a word \(w \in A^+\) is a solution of the instance \((h, g)\) if \(h(w) = g(w)\). The set of all solutions, \(E(h, g) = \{w \in A^+ \mid h(w) = g(w)\}\) is called the equality set of the instance \((h, g)\).

* Corresponding author. Turku Centre for Computer Science, Academy of Finland, Lemminkäinenkatu 14A, Turku 20520, Finland. Tel.: +358-2-333-6675; fax: +358-2-333-6595.

E-mail addresses: vesahalava@utu.fi, vehalava@utu.fi (V. Halava), harju@utu.fi (T. Harju), karhumak@cs.utu.fi (J. Karhumäki).

1 Supported by the Academy of Finland under grant 44087.
The PCP is undecidable in this general form (see [9]). The borderline between decidable and undecidable set of instances has been investigated in several occasions, e.g., it is an easy exercise to show that the unary PCP, with unary domain alphabets, is decidable. An instance \((h, g)\) with \(h, g: A^* \to B^*\) is binary, if the domain alphabet \(A\) has two letters. Without restriction we can always choose \(A = \{0, 1\}\) in this case. It was proved in [1] that the PCP is decidable for binary instances. In [4], a somewhat simpler proof was presented. On the other hand, the PCP is undecidable for instances with domain alphabets \(A\) satisfying \(|A| \geq 7\) (see [8]).

In this paper, we shall consider infinite solutions of the instances \((h, g)\). Let \(\omega = a_1a_2\ldots\) be an infinite word over \(A\) where \(a_i \in A\) for each index \(i\). Two (finite) words \(u\) and \(v\) are comparable, denoted by \(u \bowtie v\), if one is a prefix of the other. We write \(h(\omega) = g(\omega)\), if the morphisms \(h\) and \(g\) agree on \(\omega\), that is, if \(g(u) \bowtie h(u)\) for all finite prefixes \(u\) of \(\omega\). We also say that such an infinite word \(\omega\) is an infinite solution of the instance \((h, g)\). It was shown in [10] that there is no algorithm to determine whether a general instance of the PCP has an infinite solution.

**Theorem 1.** It is undecidable for instances \(I = (h, g)\) of the PCP whether \(I\) has an infinite solution.

A morphisms \(h: A^* \to B^*\) is said to be marked if the images \(h(a)\) and \(h(b)\) of any two different letters \(a, b \in A\) begin with different letters. We call the problem where the instances are pairs of marked morphisms the marked PCP. Note that a marked morphism is injective. Indeed, it is a prefix coding, that is, a morphism in which no image of a letter is a prefix of an image of another letter. Actually, by [10], it can be assumed in Theorem 1 that the morphisms in the instances are prefix codings.

The following result was proved in [3] (see also [2]).

**Theorem 2.** It is decidable for instance \(I\) of the marked PCP whether \(I\) has an infinite solution. Indeed, it is decidable whether \(I\) has an infinite solution beginning with a given letter.

The proof of Theorem 2 in [3] used the decidability of the marked PCP for finite words which was proven in [5]. The second part of Theorem 2 is implicit in the proof of the first part in [3].

We shall prove that the existence of an infinite solution is decidable for the binary instances. In the proof, we shall use Theorem 2 and a reduction defined in [1], where a given binary instance \(I\) was transformed to an equivalent instance of the binary marked generalized PCP. Recall that an instance of the generalized PCP consists of four words \(p_1, p_2, s_1, s_2 \in B^*\) and two morphisms \(h, g: A^* \to B^*\). In the problem, we are asked whether or not there exists a word \(w \in A^*\) such that

\[ p_1h(w)s_1 = p_2g(w)s_2. \]

While considering the existence of infinite solutions the end words \(s_1\) and \(s_2\) of the instances can be omitted. In fact, it is sufficient to study the infinite solutions of the instances of the marked (ungeneralized) PCP.
Note that if $E(h,g)$ contains a nonempty element $w$, then $ww\ldots$ is an infinite solution of the instance $(h,g)$. However, the existence of an infinite solution of $(h,g)$ does not imply that there is a finite solution of the instance.

Next example shows that the problem is not trivial. Consider the instance where $h$ and $g$ are defined by

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>$h$</td>
<td>aab</td>
<td>ba</td>
</tr>
<tr>
<td>$g$</td>
<td>aab</td>
<td>aa</td>
</tr>
</tbody>
</table>

The equality set $E(h,g) = \{\varepsilon\}$, but $\omega = a^2b^2a^4b^4a^8b^8\ldots$ is the unique infinite solution of the instance (that counts the powers of 2). Note that from this example it also follows that an infinite solution need not be regular, that is, accepted by a finite automaton. Note also that if $E(h,g)$ is generated by two words—which is possible—then the instance has uncountable number of infinite solutions. The form of the equality set for binary instances has been recently studied in [6,7].

We shall now fix some notations. The empty word is denoted by $\varepsilon$. The length of a word $u$ is denoted by $|u|$. A word $u \in A^*$ is said to be a prefix of $v \in A^*$, if there exists $w \in A^*$ such that $v = uw$. This will be denoted by $u \preceq v$. Also, if $u \neq \varepsilon$ and $w \neq \varepsilon$ in $v = uw$, then $u$ is a proper prefix of $v$, and, this is denoted by $u < v$. Recall that $u$ and $v$ are comparable, $u \bowtie v$, if $u \preceq v$ or $v \preceq u$. The longest common prefix of the words $u$ and $v$ is denoted by $u \wedge v$. If $v = uw$ then we also denote $u = vw^{-1}$ and $w = u^{-1}v$.

2. Reduction to marked binary generalized PCP

The PCP for binary instances was shown to be decidable in [1]. There the basic idea of the proof was that each binary instance $(h,g)$, for $h,g: A^* \to B^*$, is either

1. periodic, i.e., $h(A^*) \subseteq u^*$ for a word $u \in B^*$, or
2. it can be reduced to an equivalent instance of the binary generalized PCP with marked morphisms.

Then it was proved in [1] that both of these two cases are decidable.

In this section, we present the reduction from the binary instances of the PCP to instances of the marked generalized PCP. In the next section, we show that in both of the above cases (1) and (2) the existence of an infinite solution can be decided.

Note that in the (generalized) PCP we can always assume that the image alphabet $B$ is binary, since any $B$ can be embedded into $\{0,1\}^*$. For example, if $B = \{b_1,b_2,\ldots,b_m\}$, then $\varphi: B^* \to \{0,1\}^*$, where $\varphi(b_i) = 01^i$ for all $1 \leq i \leq m$, is such an embedding. Therefore, in the binary case we shall assume that

$$A = \{0,1\} = B.$$
Let $h$: $\{0,1\}^* \rightarrow \{0,1\}^*$ be a nonperiodic morphism. Clearly, $h$ is then nonerasing. Let $h^{(0)}=h$. For a word $w$, denote by $w_i$ the prefix of $w$ of length $i$. Define a morphism $h^{(1)}$ by

$$h^{(1)}(x) = (h(x))^{-1}(h(x)h(x)_{1}) \quad \text{for} \quad x \in A.$$  

In other words, the images of $h^{(1)}$ are the cyclic shifts of the images of $h$. Now define recursively $h^{(i+1)} = (h^{(i)})^{(1)}$ for $i \geq 1$. Now, for each $i$, let $j$ be such that $j \equiv i \pmod{|h(x)|}$ with $0 \leq j < |h(x)|$. Then

$$h^{(i)}(x) = (h(x)_j)^{-1}(h(x)h(x)_j).$$

For any two words $u,v \in A^*$, it is well known that $uw = vu$ if and only if $u$ and $v$ are powers of a common word. It follows from this that the maximum common prefix of $h(01)$ and $h(10)$ has a length at most $|h(01)| - 1$, since $h$ is nonperiodic.

The following lemma was proved in [1] (see also [4,2]).

**Lemma 1.** Let $z_h=h(01)\wedge h(10)$ and denote $m = |z_h|$. Then $h^{(m)}$ is a marked morphism and $h^{(m)}(w) = z_h^{-1}(h(w)z_h)$, for all $w \in \{0,1\}^*$. Moreover, for any $w$, if $|h(w)| \geq m$, then $z_h \leq h(w)$.

Let $(h,g)$ be a binary instance of the PCP. Assume further that $h$ and $g$ are nonperiodic. Let $z_h$ be as above, $m = |z_h|$ and $n = |z_g|$. We may assume, by symmetry, that $m \geq n$.

The following lemma is again originally from [1] (see also [4,2]).

**Lemma 2.** A binary instance $(h,g)$ of the PCP has a solution if and only if the instance $((z_g^{-1}z_h,v),h^{(m)}(v),g^{(n)},(v,z_g^{-1}z_h))$ of the generalized PCP has a solution.

In the next section we shall prove a similar theorem for infinite solutions.

### 3. Infinite solutions

In this section, we shall prove our main theorem: the existence of an infinite solution is decidable for the binary instances. In the proof the construction of the marked PCP turns out to be quite useful also in this occasion.

We begin with a simple case of the periodic instances, i.e., instances where at least one of the morphisms is periodic. Recall that a morphism $h$: $A^* \rightarrow B^*$ is periodic, if there exists a word $v \in B^*$ such that $h(a) \in v^*$ for all $a \in A$.

**Lemma 3.** It is decidable for periodic binary instances $I$ of the PCP whether or not $I$ has an infinite solution.

**Proof.** Let $I=(h,g)$ be an instance of the PCP such that $h, g$: $\{0,1\}^* \rightarrow \{0,1\}^*$ where $h(\{0,1\}) \subset v^*$ for a word $v \in \{0,1\}^+$. Let $|v| = k$ and let $v = vv \ldots$ be the infinite word with period $v$. It is clear that $\omega$ is an infinite solution of the instance $I$ if and only if $g(\omega) = v$, since $h(\omega) = v$ for all $\omega$. 
Such a solution \( \omega \) exists if and only if there exists a word \( w \) with \( |w| = k + 1 \) such that \( g(w) \) is a prefix of \( v \). Indeed, suppose that \( g(w) \) is a prefix of \( v \) for \( w \) and denote by \( w_i \) the prefix of \( w \) of length \( i \). Then \( g(w_i) = v^i v_i \) for some \( i \geq 0 \) and \( v_i \leq v \). Since the word \( v \) has \( k \) prefixes different from \( v \), there are indices \( i < j \) such that \( v_i = v_j \). Let \( w = w_i^{-1} w_j \). Then \( g(w_{i-1} w_k) \in v^i v_i \) for all \( k \geq 0 \), and \( \omega = w_{i-1} w u u \ldots \) is an infinite solution of the instance.

On the other hand, if the instance has a solution, then the existence of such a word \( w \) is trivial. \( \square \)

Let \( I = (h, g) \) be a binary instance of the PCP with nonperiodic morphisms and let \(((z^{-1}z_h, v), h^{(m)}, g^{(n)}, (v, z^{-1}z_h))\) be the equivalent instance of the binary marked generalized PCP provided by Lemma 2. Let \( \# \) be a new marker symbol. We define a new instance \((h', g')\) of the marked PCP, for \( h', g' \): \( \{0, 1, \#\} \to \{0, 1\}^* \), as follows:

\[
\begin{align*}
    h'(\#) &= \#z^{-1}_h z_h, & h'(a) &= h^{(m)}(a) \quad \text{for } a \in \{0, 1\}, \\
    g'(\#) &= \#, & g'(a) &= g^{(n)}(a) \quad \text{for } a \in \{0, 1\}.
\end{align*}
\]

It is obvious that the instance \((h', g')\) is marked, but it is not binary anymore.

**Lemma 4.** A binary instance \((h, g)\) of the PCP has an infinite solution if and only if the instance \((h', g')\) of the marked PCP has an infinite solution beginning with \( \# \).

**Proof.** Assume first that \( h(\omega) = g(\omega) \) for an infinite word \( \omega = a_1 a_2 a_3 \ldots \). Let \( w \) be a prefix of \( \omega \). Then \( h(w) \) and \( g(w) \) are comparable. Denote

\[
x = a_{|w|+1} a_{|w|+2} \ldots a_{|w|+m},
\]

where \( m = |z_h| \). Then, trivially, we have

\[

g(w x) = (z_h z_h^{-1} (h(w x) z_h)) z_h^{-1} = (z_h h^{(m)}(w x)) z_h^{-1},
\]

\[
g(w x) = (z_h z_h^{-1} (g(w x) z_h)) z_h^{-1} = (z_h g^{(n)}(w x)) z_h^{-1}
\]

and therefore \((z_h h^{(m)}(w x)) z_h^{-1} \gg (z_h g^{(n)}(w x)) z_h^{-1}\), and so

\[
(\#z_h^{-1} z_h h^{(m)}(w x)) z_h^{-1} \gg \#g^{(n)}(w x) z_h^{-1}.
\]

Since \( |h^{(m)}(x)| \gg |z_h| \) and \( |g^{(n)}(x)| \gg |z_g| \), we obtain

\[
(\#z_h^{-1} z_h h^{(m)}(w) = h'(\#w) \gg \#g^{(n)}(w) = g'(\#w).
\]

Therefore, \( \omega' = \# \omega \) is an infinite solution of \((h', g')\).

In the other direction, let \( \# \omega \) be an infinite solution of \((h', g')\). Then, for all prefixes \( w \) of \( \omega \),

\[
(\#z_h^{-1} z_h h^{(m)}(w) = h'(\#w) \gg g'(\#w) = \#g^{(n)}(w)
\]

and hence

\[
(\#z_h^{-1} z_h (h(w) z_h)) z_h^{-1} \gg \#g^{(n)}(g(w) z_g).
\]
It follows that \( h(w)z_h \gg g(w)z_g \) and also that \( h(w) \gg g(w) \). Therefore, \( \omega \) is an infinite solution of the instance \((h,g)\) \( \square \)

**Theorem 3.** It is decidable for binary instances \( I \) of the PCP whether or not \( I \) has an infinite solution.

**Proof.** For periodic instances the claim follows from Lemma 3. If \( I \) is a nonperiodic instance, then, by Lemma 4, the problem is equivalent to checking whether an instance of the marked PCP has an infinite solution beginning with a specific letter. This decidable by Theorem 2. \( \square \)

It seems that the form of the infinite solutions, or even the possible characterization of these solutions, can be reached by considering the algorithm for the marked case. However, for this we would need to study the properties of the actual algorithm which is quite involved. Therefore, this is left for further research.

**References**


