Keijo Ruohonen

A Note on Permutational Variants of Post’s Correspondence Problem

Tampere 1984
Keijo Ruohonen *

A NOTE ON PERMUTATIONAL VARIANTS OF
POST'S CORRESPONDENCE
PROBLEM

TAMPERE 1984

* Tampere University of Technology
P.O.Box 527
SF-33101 Tampere 10
Finland

ISSN 0357-7848
1. **Introduction**

Define the binary relation \( \triangleright_n \) on the finitely generated free monoid \( \Sigma^* \) as follows:

\[
P \triangleright_n Q \iff \text{there exist words } A_1, \ldots, A_n \in \Sigma^* \text{ and an n-permutation } \\
\sigma \text{ such that } P = A_1 \cdots A_n \text{ and } Q = A_{\sigma(1)} \cdots A_{\sigma(n)}.
\]

Using this we can define the \((m,n)\)-Permutation Post’s Correspondence Problem \(((m,n)\text{-PPCP})\) as follows: Are there words \( P, Q \in \Sigma_1^+ \) such that

\[
P \triangleright_m Q \text{ and } f(P) \triangleright_n g(Q)
\]

where \( f, g : \Sigma_1^* \rightarrow \Sigma_2^* \) are given word morphisms. The \((n,1)\text{-PPCP}\) is also called the \(n\text{-PPCP}\). \((1,1)\text{-PPCP}\) is, of course, the "ordinary" Post’s Correspondence Problem, see e.g. [1,4].

It was shown in [2] that the \((1,2)\text{-PPCP}\) and the \((2,2)\text{-PPCP}\) are undecidable, and especially that, for any \( n = 1, 2, \ldots \), the \(n\text{-PPCP}\) is undecidable. In fact, a stronger result was shown, though not explicitly stated, namely

**Theorem 1.** It is undecidable, given a nonempty set \( S \) of \( n\)-permutations, of morphisms \( f \) and \( g \), whether or not there are nonempty words \( P \) and \( Q \), and a permutation \( \sigma \in S \), such that \( f(P) = g(Q) \), \( P = A_1 \cdots A_n \) and \( Q = A_{\sigma(1)} \cdots A_{\sigma(n)} \). \( \Box \)

It was conjectured in [2] that the \((m,n)\text{-PPCP}\) is undecidable for each \((m,n)\). We shall prove this conjecture here in Section 2. (Actually we prove a stronger result à la Theorem 1.) No new "machinery" is needed, only a combination and a refinement of certain ideas in [2]. We assume that the reader has [2] available so that the definitions there need not be repeated.

Inspecting the proof in [2, Sect. 4] one sees that the main difficulties in establishing the undecidability of the \(n\text{-PPCP}\) for \( n \geq 2 \) are present already in the case \( n = 2 \). This raises an interesting question: Could it be that the undecidability of the \(n\text{-PPCP}\) has a simpler proof for \( n \geq 3 \) ? That is, does the greater value of \( n \) allow enough "leeway" for,
say, an easy reduction of the ordinary PCP? In Section we show that this
is indeed the case. It seems, however, that the stronger Theorem 1 cannot
be proved in this fashion. We do not know either whether a similar proof
exists for the undecidability of the \((m,n)\)-PPCP with sufficiently large
\(m\) and \(n\).

There is another aspect in the result of Section 3. In [2] and in
Section 2 our method of proof uses a kind of fault-tolerant computing.
(For other approaches in fault-tolerance see e.g. [5].) Section 3 shows
however that, somewhat surprisingly, a proof of the undecidability of the
\(n\)-PPCP for \(n \geq 3\) need not involve any fault-tolerance "mechanisms".
Whether or not such "fault-tolerance-free" proofs exist for the undecid-
ability of the \((m,n)\)-PPCP in general, or for Theorem 1, remains an open
question.

2. The result

We need two simple lemmata, in addition to those in [2].

**Lemma 1.** If \(P_2 = g_3(P_1)\) and \(P_2 = P_3 P_4 P_5\), where \(P_4\)
is the image
of a segment \(P_6\) under \(g_3\), then \(P_1 = P_7 P_6 P_8\) where \(P_3 = g_3(P_7)\) and
\(P_5 = g_3(P_8)\).

**Proof.** This follows from the definition of \(g_3\). Note especially the
use of double endmarkers. □

**Lemma 2.** \(g_3\) is injective.

**Proof.** This is immediate. (\(g_3\) is, in fact, a so-called bounded
delay morphism, cf. [4].) □

Take then \(r\) distinct copies of \(\Sigma_{1\ell}\), denoted by \(\Sigma^{<1>}_{1\ell}, \ldots, \Sigma^{<r>}_{1\ell}\),
and denote by \(P^{<i>}_{\ell}\) the isomorphic copy of a word \(P\) over \(\Sigma^{<i>}_{1\ell}\)
in \((\Sigma^{<i>}_{1\ell})^*\) \((i = 1, \ldots, r)\). We say that \(P^{<i>}_{\ell}\) is colored by the \(i\)th color.

Let then \(\Sigma_{3\ell}\) be the range alphabet of \(f_3\) and \(g_3\), and define \(\Sigma^{<1>}_{3\ell}, \ldots,
\Sigma^{<r>}_{3\ell}\) and the colored words \(P^{<i>}_{\ell} \in (\Sigma^{<i>}_{3\ell})^*\) for \(P \in \Sigma^{<i>}_{3\ell}\) and \(i = 1, \ldots, r\),
as above.

Define next the morphisms \(f_5, g_5 : (\Sigma^{<1>}_{1\ell} \cup \cdots \cup \Sigma^{<r>}_{1\ell})^* \rightarrow (\Sigma^{<1>}_{3\ell} \cup \cdots \cup \Sigma^{<r>}_{3\ell})^*\)
by
\[
f_5(a^{<i>}) = (f_3(a))^{<i>}
\text{ for } a \in \Sigma_{1 \&} \text{ and } i = 1, \ldots, r
\]
and
\[
eg_{5}(a^{<i>}) = (\neg_{3}(a))^{<i+1>}
\text{ for } a \in \Sigma_{1 \&} \text{ and } i = 1, \ldots, r-1;
\]
\[
eg_{5}(a^{<r>}) = (\neg_{3}(a))^{<1>}
\text{ for } a \in \Sigma_{1 \&}.
\]

The values of \( r \) and \( \& \) will be fixed later. We assume that either \( m > 1 \) or \( n > 1 \).

We now proceed to prove our main result. So suppose

\[
f_5(P) \sim_n \neg_5(Q) \text{ and } P \sim_m Q
\]

where \( P \) and \( Q \) are nonempty words over \( \Sigma^{<1>}_{1 \&} \cup \cdots \cup \Sigma^{<r>}_{1 \&} \). We can then write

\[
f_5(P) = B_1 \cdots B_n \quad \text{ and } \quad \neg_5(Q) = B_{\sigma(1)} \cdots B_{\sigma(n)}
\]

for some words \( B_1, \ldots, B_n \) and an \( n \)-permutation \( \sigma \), and

\[
P = A_1 \cdots A_m \quad \text{ and } \quad Q = A_{\tau(1)} \cdots A_{\tau(m)}
\]

for some words \( A_1, \ldots, A_m \) and an \( m \)-permutation \( \tau \). There may be several possible choices for \( B_1, \ldots, B_n, A_1, \ldots, A_m \) and \( \sigma, \tau \). We choose one of them and consider it fixed.

Thus we get the words \( B_1, \ldots, B_n \) by making \( n-1 \) cuts in \( f_5(P) \) and also, possibly in a different order, by making \( n-1 \) cuts in \( \neg_5(Q) \). Similarly, we get \( A_1, \ldots, A_m \) by making \( m-1 \) cuts alternatively in \( P \) or \( Q \). Note that, because some of the words \( B_1, \ldots, B_n, A_1, \ldots, A_m \) may be empty, it is possible that several cuts are "merged" and that there may be (merged) cuts immediately preceding the first symbol or immediately following the last symbol of the words \( f_5(P), \neg_5(Q), P, Q \).

By a color block we mean a unicolored subword of maximal length. Thus there cannot be adjacent color blocks of the same color. If a cut takes place inside a color block of \( f_5(P), \neg_5(Q), P \) or \( Q \), we say that the color block is cut. Thus a cut occurring exactly between two adjacent color blocks is not considered as cut of neither of these two blocks.
Each color block of $f_5(P)$ has an "ancestor color block" of the same color in $P$. Similarly, each color block of $g_5(Q)$ has an ancestor color block in $Q$ of the preceding color in the circular order. Thus all colors must occur in these words.

We then choose the number of colors to be $3n$, i.e., $r = 3n$. It follows that there are three consecutive color blocks in $f_5(P)$ which are not cut. Note that a color block which is not cut in $f_5(P)$ may be part of a cut color block in $g_5(Q)$. Of any three consecutive uncut color blocks in $f_5(P)$, the one in the middle must be uncut in $g_5(Q)$, too. By [2,Lemma 3.4] the middle color block must be of the form $S_1^{<1>}$ where $S \in f^+(R_2) \cap g^+(R_2)$. The ancestors of this middle block in $P$ and $Q$ are then of the form $S_1^{<1>}$ and $S_2^{<i-1>}$ (or $S_2^{<i>}$ if $i = 1$), respectively, where $S_1, S_2 \in R_1^+$ and $f_5(S_1) = g_5(S_2)$. Thus $S_2^{<i-1>}$ contains a sequence of $i$ consecutive segments, colored by the $(i-1)$st color, of course.

We then choose $\lambda$ to be equal to $m^{n-1} m^{m-1}$. By Lemmata 1-2 we can "trace the route" of each of the above mentioned $\lambda$ consecutive segments in $S_2^{<i-1>}$ clockwise in the diagram of Fig. 1 as long as the segment is not cut in $Q$ or $f_5(P)$.

![Diagram](image)

Figure 1.

Now, because of the indexing of the segments, it is obvious that no cut, whether in $Q$ or in $f_5(P)$, can occur more than once along this route. Since there are $m-1$ cuts in $Q$ and $n-1$ cuts in $f_5(P)$ (some of them possibly merged), we deduce, using Dirichlet's box principle as in [2,Sect.4], that for at least one of these segments the route is endless. It follows that there is a nonempty recurrent ID of $M$.

Thus the existence of nonempty words $P$ and $Q$ such that $f_5(P) \xrightarrow{m} g_5(Q)$ and $P \xrightarrow{n} Q$ implies that $M$ has nonempty recurrent ID's. The converse is easily shown, exactly as in [2,Sect.5].

We have thus proved that the ($m,n$)-PPCP is undecidable for any non-
negative integers \( m \) and \( n \). Actually we have shown the following stronger result, as is easily seen:

**Theorem 2.** It is undecidable, given a nonempty set \( U_1 \) of \( m \)-permutations and a nonempty set \( U_2 \) of \( n \)-permutations, of morphisms \( f \) and \( g \), whether or not there exist nonempty words \( P \) and \( Q \), and permutations \( \sigma \in U_2 \) and \( \tau \in U_1 \), such that \( f(P) = B_1 \cdots B_n \), \( g(Q) = B_{\sigma(1)} \cdots B_{\sigma(n)} \), \( P = A_1 \cdots A_m \) and \( Q = A_{\tau(1)} \cdots A_{\tau(m)} \).

Note that for the following pairs \((m,n)\) Theorem 2 is, in fact, a consequence of the undecidability of the \((m,n)\)-PPCP: \((1,1),(1,2),(2,1)\) and \((2,2)\). All these pairs were treated already in \([2]\).

3. A "short" proof of the undecidability of the \( n \)-PPCP for \( n \geq 3 \)

Let \( f,g : \Sigma_1^* \rightarrow \Sigma_2^* \) be nonerasing morphisms. The pair \((f,g)\) may be considered as an instance of the ordinary PCP, which is well-known to be undecidable for nonerasing morphisms. We will, in fact, assume that \((f,g)\) is an instance of the so-called modified PCP (MPCP), also undecidable (cf. \([1]\)). The MPCP is the following problem: Does there exist a word \( P \in \Sigma_1^* \) such that \( f(P) = g(P) \), and \( P \) and \( f(P) \) both begin with a certain prescribed symbol \( \psi \in \Sigma_1 \cap \Sigma_2 \) which does not occur elsewhere in \( P \) or \( f(P) \). To give a detailed reduction of the PCP for nonerasing morphisms, we might as well give a proof of the undecidability of the MPCP by reducing the ordinary PCP for nonerasing morphisms to it.

**Lemma 3.** MPCP is undecidable.

**Proof.** Let \( h,k : \Delta_1^* \rightarrow \Delta_2^* \) be a pair of nonerasing morphisms. Let \( \psi \) and \( \# \) be new symbols and define \( h' \) and \( k' \) on \((\Delta_1 \cup \{\psi,\#\})^*\) by

\[
h'(\psi) = \psi \# , \quad h'(\#) = \# \#^2 , \quad h'(\#) = \# , \quad k'(\#) = \#^2 ,
\]

\[
h'(a) = \# a_1 \#^2 a_2 \# \cdots \#^2 a_n \quad \text{where} \quad h(a) = a_1 \cdots a_n \quad \text{and} \quad a_1, \ldots, a_n \in \Delta_2 ;
\]

\[
k'(a) = a_1 \#^2 a_2 \# \cdots \#^2 a_n \quad \text{where} \quad k(a) = a_1 \cdots a_n \quad \text{and} \quad a_1, \ldots, a_n \in \Delta_2 .
\]
It is then easily seen that \( h(b_1 \cdots b_m) = k(b_1 \cdots b_m) \), where \( b_1, \ldots, b_m \in \Delta_1 \) and \( m \geq 1 \), if and only if \( h'(\#b_1 \# b_2 \# b_3 \cdots \# b_m) = k'(\#b_1 \# b_2 \# b_3 \cdots \# b_m) \), and that this is the only way an equality \( h'(P) = k'(P) \) can hold true for a word \( P \) beginning with \( \phi \) and not containing other occurrences of \( \phi \).

We will only indicate why it is not possible for \( P \) to contain several consecutive occurrences of \( \# \). Suppose, to the contrary, that \( P \) contains \( v \geq 2 \) consecutive occurrences of \( \# \). Obviously these cannot immediately follow the prefix symbol \( \phi \), nor can they be the last symbols of \( P \).

Thus the occurrences are situated between two symbols of \( \Delta_1 \). From the equality \( h'(P) = k'(P) \) it follows that there are

\[
v, 2v-1, 4v-3, \ldots, 2^{n}(v-1)+1, \ldots
\]

consecutive occurrences of \( \# \) in \( P \). Since \( v > 1 \), this is a contradiction.

Let then \( n \geq 3 \) be an integer and \( \phi_1, \ldots, \phi_n \) be new symbols. Extend \( f \) and \( g \) to \((\Sigma_1 \cup \{\phi_1, \ldots, \phi_n\})^*\) by

\[
f(\phi_i) = \phi_i \quad \text{and} \quad g(\phi_i) = \phi_{n-i} \quad \text{for} \quad i = 1, \ldots, n-1;
\]

\[
f(\phi_n) = g(\phi_n) = \phi_n.
\]

The regular language \( \phi_1 \phi_2 \cdots \phi_{n-1} \phi(\Sigma_2 - \{\phi\}) \phi_n \) is recognized by the unique state automaton in Fig. 2. Let \( f' \) and \( g' \) be the corresponding morphisms (see [2, Lemma 3.2]).

\[
\begin{array}{cccccc}
0 & \phi_1 & \phi_2 & \ldots & \phi_{n-2} & \phi_{n-1} \\
\downarrow & \downarrow & \downarrow & \ldots & \downarrow & \downarrow \\
1 & \phi_2 & \ldots & \phi_{n-2} & \phi_{n-1} & \phi_n \\
\downarrow & \downarrow & \downarrow & \ldots & \downarrow & \downarrow \\
n & & & & & n+1 \\
\end{array}
\]

Figure 2.
It is then easily verified that there are nonempty words $P$ and $Q$ such that $P \cdot Q$ and $f^* f(P) = g^* g(Q)$ if and only if $P$ is of the form $1 \cdot 2 \cdot \ldots \cdot n \cdot 1 \cdot \ldots \cdot 1$ and $Q$ is of the form $\ldots \cdot n \cdot n-2 \cdot \ldots \cdot 1 \cdot 1 \cdot \ldots \cdot 1$, where $P_1$ is a nonempty word over $\Sigma_2 - \{\epsilon\}$ such that $f(\epsilon P_1) = g(\epsilon P_1)$.

We have thus reduced the ordinary PCP for nonerasing morphisms to the $n$-PPCP (with $n \geq 3$). Note that the construction does not work for $n=2$. Note also that it does not prove Theorem 1 unless the set $S$ contains the permutation $\begin{bmatrix} 1 & 2 & \ldots & n-1 & n \end{bmatrix}$ or other applicable permutations of order $n$, such as the "mirror image" $\begin{bmatrix} 1 & 2 & 3 & \ldots & n \end{bmatrix}$ or (for $n \geq 5$) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \end{bmatrix}$ or $\begin{bmatrix} 2 & 1 & 3 & \ldots & n-1 & 4 \end{bmatrix}$. Thus the present method appears to be much weaker than the one in [2]. It is perhaps less interesting for another reason, too: While the method in [2] is based on properties of computation, i.e., proceeding sufficiently many copies of computations simultaneously to thwart the effect of permuting subwords, the trick in the present proof seems to be purely an artifact of the morphism simulation.

Remark. It is not difficult to see that if the morphisms $f$ and $g$ above are biprefix morphisms (see e.g. [4]) then so are $f^* f$ and $g^* g$. Since the MPCP is undecidable for biprefix morphisms (see [3]), it follows that the $n$-PPCP for biprefix morphisms is also undecidable for $n \geq 3$. The case is open for $n=2$ as is the validity of Theorem 1 for biprefix morphisms $f$ and $g$ and $n \geq 2$.

References


