Vesa Halava | Tero Harju | Mari Huova

On n-permutation Post Correspondence Problem

Turku Centre *for* Computer Science

TUCS Technical Report
No 1084, December 2013

On n-permutation Post Correspondence Problem

Vesa Halava
Department of Mathematics and Statistics
University of Turku
FI-20014 Turku, Finland
vehalava@utu.fi

Tero Harju
Department of Mathematics and Statistics
University of Turku
FI-20014 Turku, Finland
harju@utu.fi

Mari Huova
Department of Mathematics and Statistics
and TUCS - Turku Centre for Computer Science
University of Turku
FI-20014 Turku, Finland
mari.huova@utu.fi

TUCS Technical Report
No 1084, December 2013

Abstract

We give new and simpler proof for the undecidability of the n-permutation Post Correspondence Problem that was originally proved by K. Ruohonen (Acta Informatica 19 (1983), 357 – 367). Our proof uses a recent undecidability result on deterministic semi-Thue systems that says that it is undecidable, for a given deterministic semi-Thue system T and a word u, whether or not there exists a nonempty cyclic derivation $u \rightarrow_T^* u$ in T.

Keywords: Permutation Post Correspondence Problem, semi-Thue system, word problem, deterministic, cyclic derivation

TUCS Laboratory
FUNDIM, Fundamentals of Computing and Discrete Mathematics

1 Introduction

In the history of computation, the Post Correspondence Problem and it variants have played a major role as a simply defined algorithmically undecidable problem that can be used to prove other undecidability results. For example, several problems in formal language theory and theory of integer matrices are shown to be undecidable by reducing the Post Correspondence Problem to them.

The original formulation of the Post Correspondence Problem, or PCP for short, by Emil Post [8] is the following:

Problem 1 (PCP)**.** *Let B be an alphabet, and let B^* be the set of all finite words over B, including the empty word ε. Given an integer n and two finite ordered lists of words*

$$(u_1, u_2, \ldots, u_n) \quad \textit{and} \quad (v_1, v_2, \ldots, v_n) \tag{1}$$

where $u_i, v_i \in B^*$ for all $i = 1, 2, \ldots, n$, does there exist a finite nonempty sequence $i_1, i_2, \ldots, i_k$ of indices such that

$$u_{i_1} u_{i_2} \cdots u_{i_k} = v_{i_1} v_{i_2} \cdots v_{i_k}? \tag{2}$$

An *instance of the PCP* consists of two sequences (1) of words where the integer $n \geq 1$ is called the *size* of the instance. A sequence $i_1, i_2, \ldots, i_k$ satisfying (2) is called a *solution* of the instance. The PCP was proven to be undecidable by its inventor Emil Post in 1946 in [8].

The PCP is given an equivalent form in Problem 2. Let A and B be two alphabets. A mapping $h\colon A^* \to B^*$ is a *morphism*, if $h(uv) = h(u)h(v)$ holds for all $u, v \in A^*$. For an instance I in (1) with $u_i, v_i \in B^*$, let $A = \{a_1, a_2, \ldots, a_n\}$ be an alphabet and define two morphisms $h, g\colon A^* \to B^*$ by

$$g(a_i) = u_i \quad \text{and} \quad h(a_i) = v_i$$

for all $i = 1, 2, \ldots, n$. Then the original form of the PCP is equivalent to the following problem.

Problem 2 (PCP)**.** *Given two morphisms $g, h\colon A^* \to B^*$, does there exist a nonempty word $w \in A^+$ such that*

$$g(w) = h(w)\,?$$

Now, a pair $I = (g, h)$ of morphisms is said to be an *instance* of the PCP, and a word w satisfying $h(w) = g(w)$ is called a *solution* of the instance I. The *size* of the instance (g, h) is the cardinality of the domain alphabet A. Notice that the size of an instance refers to the same value in both formulations of the PCP.

Several variants of the PCP are known to be undecidable. By a variant we mean a restriction of the PCP to a specific type of instances. For example, it is known that the PCP is undecidable for instances of size 7; see [7]. It is also known that the PCP is undecidable for instances of injective morphisms; see [5, 11] and [4] for a more recent proof to this end.

In [10], K. Ruohonen proved that the following two variants of the PCP are undecidable.

Problem 3 (n-permutation PCP (nPPCP)). *Given two morphisms $h, g\colon A^* \to B^*$, does there exist a word $w = w_1 w_2 \cdots w_n$ and a permutation σ of the set $\{1, 2, \ldots, n\}$ such that*

$$g(w_1 \cdots w_n) = h(w_{\sigma(1)} \cdots w_{\sigma(n)}).$$

Problem 4 (Circular PCP). *Given two morphisms $h, g\colon A^* \to B^*$, does there exist words $u, v \in A^*$ with $uv \neq \varepsilon$ such that*

$$g(uv) = h(vu).$$

Here the words $w_1 = uv$ and $w_2 = vu$ are called *conjugates* of each other. Hence, the circular PCP could be stated by asking whether there exist conjugate words w_1 and w_2 such that $g(w_1) = h(w_2)$. The phrase 'circular PCP' refers to the problem setting where the words are considered to be cyclic, i.e., the last letter is followed by the first letter.

Note that the circular PCP is the same as the 2-permutation PCP, and trivially the 1-permutation PCP is just the PCP.

The undecidability proofs by Ruohonen in [10] employ an undecidable property of linearly bounded automata. The proofs by Ruohonen are rather long and technical, and therefore, there is a request for simpler proofs for these problems. In [3], instead of linearly bounded automata, the authors employed a special variant of the word problem for semi-Thue systems while proving the undecidability of the circular PCP. Here we shall use the same techniques for the nPPCP.

Let us briefly discuss this special form of the word problem. A *semi-Thue system* T is a pair (Σ, R) where $\Sigma = \{a_1, a_2, \ldots, a_n\}$ is a finite alphabet, the elements of which are called *generators* of T, and $R \subseteq \Sigma^* \times \Sigma^*$ is a relation. The elements of R are called the *rules* of T. We shall also write $x \to_T y$ for a rule $(x, y) \in R$. We write $u \to_T v$, if there exists a rule $(x, y) \in R$ such that $u = u_1 x u_2$ and $v = u_1 y u_2$ for some words u_1 and u_2. We denote by $\to_T^*$ the reflexive and transitive closure of $\to_T$, and by $\to_T^+$ the transitive closure of $\to_T$.

If the relation R is symmetric, then T is a *Thue system* and then T corresponds to a semigroup with generators Σ and relations R.

In the *word problem* for a semi-Thue system $T = (\Sigma, R)$ we are given two words $u, v \in \Sigma^*$ and the task is to determine whether or not there exists a

derivation from u to v using the rules in R i.e., $u \to_T^* y$. The first proofs for undecidability of the word problem of semi-Thue systems were given independently by Post [9] and Markov [6].

Let $T = (\Sigma, R)$ be a semi-Thue system such that $\Sigma = A \cup B$ and $A \cap B = \emptyset$. Then T is called B-*deterministic*, if

1. $R \subseteq A^*BA^* \times A^*BA^*$, namely, if the rules contain a unique letter from B on both sides,

2. for all words $w \in A^*BA^*$, there is a unique derivation in T

In [3] it was proved that the word problem is undecidable for B-deterministic semi-Thue systems, and even in the following special form:

Theorem 1. *Let $T = (\Sigma, R)$ be a B-deterministic semi-Thue system such that $\Sigma = A \cup B$ and $A \cap B = \emptyset$, and $a, c \in A$ and $S \in B$. It is undecidable whether or not there exists a nonempty (cyclic) derivation $aSc \to_T^+ aSc$.*

Note that in the above the derivation for the word aSc is unique in T. The proof of Theorem 1 uses the construction presented in [2] where the halting problem of the Turing machines is reduced to the word problem of this special type. This technique is based on the construction of Karhumäki and Saarela [4] for proving the undecidability of injective PCP.

To reduce an undecidability result of the semi-Thue system to instances of the PCP, we apply the standard construction introduced by Claus [1]. The idea is to simulate a derivation of the semi-Thue system T on a word u with two morphisms g, h such that there exist a word w with $g(w) = h(w)$ if and only if there is a derivation in T starting from u and ending in the given word v. Here the word w corresponds to a required derivation according to T. Hence we may say that the morphisms g and h *simulate* derivations of T starting from a given word u.

2 Construction

We shall shortly describe the required details and properties of the construction of the proof of Theorem 1 in [3].

Let $C_{\mathcal{M}} = (\Sigma, R)$ be a B-deterministic semi-Thue system with $\Sigma = A \cup B$ and $A \cap B = \emptyset$ as constructed in [3]. For all $t \in R$, $t \in A^*BA^* \times A^*BA^*$. Moreover, there are two special symbols $a, c \in A$, and two special rules

$$t_I = (aSc,\ u_I b_I v_I) \quad \text{and} \quad t_C = (u_C b_C v_C, aSc) \tag{3}$$

in R such that $S, b_I, b_C \in B$ are fixed by the determinism of $C_{\mathcal{M}}$. These rules are the initial rule (t_I) and the final rule (t_C). Now, by [3] it is undecidable whether or not

$$aSc \to_{C_{\mathcal{M}}}^+ aSc. \tag{4}$$

By the determinism of $C_{\mathcal{M}}$, the above derivation is unique if it exists. Also, by the construction in [2], the special letters a and c has the following property: For all w,

$$aSc \to^*_{C_{\mathcal{M}}} w \text{ implies } w \in D^*aD^*bD^*c,$$

where $D = A \setminus \{a, c\}$ and $b \in B$. In other words, the letter c is the right marker symbol of the derivation.

Denote the set of rules R by $R = \{t_I, t_1, \ldots, t_k, t_C\}$. Next, we take $n-1$ copies of the alphabets R and Σ. The ith copy of R and Σ are denoted by

$$R^{(i)} = \{t^{(i)} \mid t \in R\} \quad \text{and} \quad \Sigma^{(i)} = \{y^{(i)} \mid y \in \Sigma\},$$

for $i = 1, 2, \ldots, n-1$. We let $A^{(i)} = \{x^{(i)} \mid x \in A\}$. Define $\Gamma = R \cup A$, $\Gamma^{(i)} = R^{(i)} \cup A^{(i)}$, and

$$\Gamma_n = \cup_{i=1}^{n-1} \Gamma^{(i)} \quad \text{and} \quad \Sigma_n = \cup_{i=1}^{n-1} \Sigma^{(i)}.$$

For all words $w \in (\Sigma \cup R)^*$, denote by $w^{(i)}$ the results when all letters in w are replaced by their ith copies.

Next let $\Delta = \Sigma_n \cup \{d\}$ where d is a new symbol not in $\Sigma \cup R$, and let ℓ_d and r_d be the *desynchronizing morphisms* defined by $\ell_d(x) = dx$ and $r_d(x) = xd$ for each letter $x \in \Sigma_n$.

Now let τ be a permutation of the set $\{1, \ldots, n-1\}$. We define two morphisms, $g, h \colon \Gamma_n^* \to \Delta^*$ as follows. For any letter $a \in A$ and $i = 1, 2, \ldots, n-1$, set

$$g(a^{(i)}) = \ell_d(a^{(i)}) = da^{(i)} \quad \text{and} \quad h(a^{(i)}) = r_d(a^{(\tau(i))}) = a^{(\tau(i))}d,$$

and for $t \in R$ with $t \neq t_C$, say $t = u_1 b_1 v_1 \to u_2 b_2 v_2$, we set

$$g(t^{(i)}) = \ell_d((u_1 b_1 v_1)^{(i)}) \quad \text{and} \quad h(t^{(i)}) = r_d((u_2 b_2 v_2)^{(\tau(i))}),$$

where $u_1, u_2, v_1, v_2 \in \Sigma^*$ and $b_1, b_2 \in B$, and $i = 1, 2, \ldots, n-1$.

For the copies of $t_C = (ub_C v, aSc)$, let

$$g(t_C^{(i)}) = \ell_d((ub_C v)^{(i)}) \quad \text{and} \quad h(t_C^{(i)}) = r_d((aSc)^{(\tau(i)+1)}),$$

for $i = 1, \ldots, n-2$ and for $i = n-1$, set

$$g(t_C^{(i)}) = \ell_d((ub_C v)^{(i)})d \quad \text{and} \quad h(t_C^{(i)}) = dr_d((aSc)^{(1)}).$$

Assume now that there exists a cyclic nonempty computation

$$aSc = \beta_0 \to \beta_1 \to \beta_2 \to \cdots \to \beta_k = aSc,$$

in $C_{\mathcal{M}}$ where $\beta_j = x_j(u_j b_j v_j)y_j$, and $t_j = (u_j b_j v_j, u'_j b_{j+1} v'_j) \in R$, $b_j, b_{j+1} \in B$, for $j = 0, \ldots, k-1$. Note that necessarily $t_0 = t_I$ and $t_{k-1} = t_C$, and by

construction in [3], we have $x_0 = y_0 = x_{k-1} = y_{k-1} = \varepsilon$, in other words, $t_I = (\beta_0, \beta_1)$ and $t_C = (\beta_{k-1}, \beta_k) = (\beta_{k-1}, \beta_0)$. Define now a word

$$w = x_0 t_0 y_0 x_1 t_1 y_1 \cdots x_{k-1} t_{k-1} y_{k-1} = t_I x_1 t_1 y_1 \cdots x_{k-2} t_{k-2} y_{k-2} t_C.$$

For $i = 1, \ldots, n-2$, our construction gives

$$\begin{aligned} g(w^{(i)}) &= \ell_d((\beta_0 \cdots \beta_{k-1})^{(i)}) = \ell_d((aSc\beta_1 \cdots \beta_{k-1})^{(i)}) \\ h(w^{(i)}) &= r_d((\beta_1 \cdots \beta_{k-1})^{(\tau(i))}(\beta_k)^{(\tau(i)+1)}) \\ &= r_d((\beta_1 \cdots \beta_{k-1})^{(\tau(i))}(aSc)^{(\tau(i)+1)}). \end{aligned}$$

For $i = n-1$, we have

$$\begin{aligned} g(w^{(i)}) &= \ell_d((\beta_0 \cdots \beta_{k-1})^{(i)})d = \ell_d((aSc\beta_1 \cdots \beta_{k-1})^{(i)})d \\ h(w^{(i)}) &= r_d((\beta_1 \cdots \beta_{k-1})^{(\tau(i))})dr_d((\beta_k)^{(1)}) \\ &= r_d((\beta_1 \cdots \beta_{k-1})^{(\tau(i))})dr_d((aSc)^{(1)}). \end{aligned}$$

Define a word $\omega = w^{(1)}w^{(2)} \cdots w^{(n-1)}$, then clearly

$$g(\omega) = \ell_d((\beta_0\beta_1 \cdots \beta_{k-1})^{(1)} \cdots (\beta_0\beta_1 \cdots \beta_{k-1})^{(n-1)})d$$

and, since $\beta_0 = \beta_k$,

$$\begin{aligned} h(\omega) =& r_d[(\beta_1 \cdots \beta_{k-1})^{(\tau(1))}(\beta_0)^{(\tau(1)+1)} \\ & (\beta_1 \cdots \beta_{k-1})^{\tau(2)}(\beta_0)^{(\tau(2)+1)} \cdots \\ & (\beta_0)^{(\tau(n-2)+1)}(\beta_1 \cdots \beta_{k-1})^{(\tau(n-1))}]dr_d((\beta_0)^{(1)}). \end{aligned}$$

Define next the permutation σ by setting $\sigma(1) = n$ and $\sigma(i) = \tau^{(-1)}(i-1)$ for $i = 2, \ldots, n$. Next, let the words w'_i be such that

$$\omega = w'_1 t_C^{(1)} w'_2 t_C^{(2)} \cdots w'_{n-1} t_C^{(n-1)},$$

and, furthermore, set $w_i = w'_i t_C^{(i)}$ for $i = 1, \ldots, n-2$, $w_{n-1} = w'_{n-1}$ and $w_n = t_C^{(n-1)}$. Finally, we have

$$\begin{aligned} h(w_{\sigma(1)}w_{\sigma(2)} \cdots w_{\sigma(n)}) &= h(w_n w_{(\tau^{(-1)}(1))} \cdots w_{(\tau^{(-1)}(n-1))}) \\ &= dr_d((\beta_0)^{(1)})r_d[(\beta_1 \cdots \beta_{k-1})^{(1)}(\beta_0)^{(1+1)} \\ &\quad (\beta_1 \cdots \beta_{k-1})^{(2)}(\beta_0)^{(2+1)} \cdots \\ &\quad (\beta_0)^{(n-1)}(\beta_1 \cdots \beta_{k-1})^{(n-1)}] \\ &= g(w_1 \cdots w_n). \end{aligned}$$

Therefore, we have shown

Lemma 1. *If there exists a cyclic computation $aSc \to^+ aSc$ in $C_{\mathcal{M}}$, then there exists a solution for the nPPCP for instance (g, h) defined above.*

For the other direction, we prove

Lemma 2. *Let (g, h) be an instance of the nPPCP as defined above. If there exists a solution for the nPPCP, then there exists a nonempty cyclic computation $aSc \to^+ aSc$ in semi-Thue system $C_{\mathcal{M}}$.*

Proof. Assume that the instance (g, h) of the nPPCP has a solution, say $\omega = w_1 \cdots w_n$ and $g(\omega) = w = h(w_{\sigma(1)} \cdots w_{\sigma(n)})$. First note a key feature of the construction: the letters from the set B appear only in the images of rule symbols $t^{(i)}$ of some $R^{(i)}$.

Now, the desynchronizing forces that $w \in d(\Sigma d)^+$. Therefore, ω must contain (indeed, $w_{\sigma(1)}$ must begin with) the symbol $t_C^{(n-1)}$, since that is the only symbol having d as the first symbol in the image of the morphism h. Since $h(t_C^{(n-1)}) = dr_d((aSc)^{(1)})$, and since $(aSc)^{(1)}$ can be generated as an image of g only by $t_I^{(1)}$, the word ω must begin with $t_I^{(1)}$. Next we see that $h(t_I^{(1)}) = r_d((\beta_1)^{(\tau(1))})$, where $t_I = (aSc, \beta_1)$ and

$$aSc \to \beta_1$$

in $C_{\mathcal{M}}$. Continuing, in order to get $\ell_d(\beta_1^{(\tau(1))})$ as an image of g, we necessarily have $\beta_1 = x_1(u_1 b_1 v_1)y_1$, and there must exists a rule $t_1 = (u_1 b_1 v_1, u_1' b_2 v_1') \in R$ with $b_1, b_2 \in B$, and $(x_1 t_1 y_1)^{(\tau(1))}$ is a factor of ω. Therefore, for $\beta_2 = x_1 u_1' b_2 v_1'$, we have

$$aSc \to \beta_1 \to \beta_2$$

in $C_{\mathcal{M}}$. Now,

$$h((x_1 t_1 y_1)^{(\tau(1))}) = r_d((x_1 u_1' b_2 v_1' y_1)^{(\tau(\tau(1)))}) = r_d((\beta_2)^{(\tau(\tau(1)))}).$$

Omitting the copies of the letters, we may continue the reasoning and find that there exists a derivation

$$aSc \to \beta_1 \to \cdots \to \beta_k$$

in $C_{\mathcal{M}}$. On the other hand, since ω is finite, the derivation must be finite. The only possibility for the reasoning to stop and not to force new configuration in the derivation, is that there is no next copy of the configuration in the image word w. This means that the rule that is used last must be $t_C^{(n-1)}$, since its image in h was already placed and forced $\ell_d((aSc)^{(1)})$ in the image of g. Therefore, we have proved that if there exists a solution, there must be a cyclic derivation

$$aSc \to \beta_1 \to \cdots \to \beta_k = aSc$$

□

Theorem 2. *There exists a nonempty computation*

$$aSc \to^+ aSc$$

in $C_{\mathcal{M}}$ *if and only if there exists a nonempty* $\omega \in \Gamma_n$ *such that* $\omega = w_1 w_2 \cdots w_n$ *and* $g(\omega) = h(w_{\sigma(1)} w_{\sigma(2)} \cdots w_{\sigma(n)})$ *for some permutation* σ *on* $\{1, \ldots, n\}$.

Proof. Follows from Lemmata 1 and 2. □

By Theorem 1, we now have a new proof of the following corollary.

Corollary 1. *The n-permutation PCP is undecidable.*

References

[1] V. Claus, Some remarks on PCP(k) and related problems, *Bull. EATCS* **12** (1980), 54 – 61.

[2] V. Halava and T. Harju, Word problem for deterministic and reversible semi-Thue systems, manuscript (submitted), TUCS Technical Report 1044, TUCS, 2012.

[3] V. Halava and T. Harju, New proof for the undecidability of the circular PCP, Acta Informatica, to appear.

[4] J. Karhumäki and A. Saarela, Noneffective Regularity of Equality Languages and Bounded Delay Morphisms, *Discrete Mathematics & Theoretical Computer Science*, 12(4): 9–18, 2010.

[5] M.Y. Lecerf, Récursive insolubilité de l'équation générale de diagonalisation de deux monomorphismes de monoïdes libres $\varphi x = \psi x$, *Comptes Rendus* **257** (1963), 2940 – 2943.

[6] A.A. Markov, On the impossibility of certain algorithms in the theory of associative systems, *Dokl. Akad. Nauk* **55** (1947), 587 – 590; **58** (1947), 353 – 356 (Russian).

[7] Y. Matiyasevich and G. Sénizergues. Decision problems for semi–Thue systems with a few rules. *Theor. Comput. Sci.* 330(1):145-169, 2005

[8] E. Post, A variant of a recursively unsolvable problem, *Bulletin of Amer. Math. Soc.* **52** (1946), 264 – 268.

[9] E. Post, Recursive unsolvability of a problem of Thue, *J. Symb. Logic* **12** (1947), 1 – 11.

[10] K. Ruohonen, On some variants of Post's correspondence problem, *Acta Informatica* **19** (1983), 357 – 367.

[11] K. Ruohonen, Reversible machines and Post's correspondence problem for biprefix morphisms, *J. Inform. Process. Cybernet. EIK* **21** (1985), 579 – 595.

Joukahaisenkatu 3-5 B, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics

Åbo Akademi University
- Department of Information Technologies

Turku School of Economics
- Institute of Information Systems Sciences

ISBN 978-952-12-2921-3
ISSN 1239-1891