HAL
open science

The exact complexity of the infinite Post Correspondence Problem

Olivier Finkel

To cite this version:

Olivier Finkel. The exact complexity of the infinite Post Correspondence Problem. Information Processing Letters, 2015, 115 (6-8), pp.609-611. 10.1016/j.ipl.2015.02.009 . hal-01376975

HAL Id: hal-01376975

https://hal.science/hal-01376975

Submitted on 6 Oct 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The Exact Complexity of the Infinite Post Correspondence Problem

Olivier Finkel
Equipe de Logique Mathématique
Institut de Mathématiques de Jussieu – Paris Rive Gauche
CNRS et Université Paris Diderot Paris 7
UFR de Mathématiques case 7012
75205 Paris Cedex 13, France.
finkel@math.univ-paris-diderot.fr

Abstract

In this short note, we give the exact complexity of the infinite Post Correspondence Problem, showing that it is Π^0_1-complete. Surprisingly, it turns out that the infinite Post Correspondence Problem is not "more complex" than the Post Correspondence Problem, which is known to be Σ^0_1-complete, but has the exact dual complexity. This gives an answer to a question of Simonnet [Sim10].

Keywords. Decision problems; infinite Post Correspondence Problem; exact complexity; Π^0_1-complete.

1 Introduction

The well known Post Correspondence Problem (PCP) is one of the famous undecidable problems in Theoretical Computer Science and in Formal Language Theory, see [HMU01]. The PCP is an abstract problem involving strings, and it has been very useful to prove the undecidability of many other problems by reduction of PCP to those problems. In particular, many problems about context-free languages, those accepted by pushdown automata or generated by context-free grammars, have been shown to be undecidable by this method. For instance it follows from the undecidability of the Post Correspondence Problem that the universality problem, the inclusion and the equivalence problems for context-free languages are also undecidable. Notice that these undecidability results can also be shown from the undecidability of the halting problem for Turing machines, but the proofs obtained from the undecidability of the PCP are simpler. Also, the undecidability of the PCP has been used to prove undecidability results concerning matrices of low order with integer entries, see [Har02].

There is also an extension of the PCP to infinite strings called the infinite Post Correspondence Problem or the ω-PCP which has been shown to be undecidable by Ruohonen in [Ruo85] and by Gire in [Gir86], see also [HH06, HHK06]. This problem has been used to prove the undecidability of other problems in various contexts, for instance in the domains of infinitary rational relations [Pri00, Fin03] or of probabilistic automata [BC03].

The complexity of the PCP is well known; the PCP is Σ_1^0-complete, i.e. it is complete for the class of recursively enumerable problems, i.e. complete at the level Σ_1^0 of the arithmetical hierarchy. On the other hand the complexity of the ω-PCP seems still unknown and the question of its exact complexity was asked by Simonnet [Sim10].

We answer this question in this short note, proving that the infinite Post Correspondence Problem is Π_1^0-complete. This shows that the ω-PCP is not "more complex" than the PCP but has the exact dual complexity.

2 The Infinite Post Correspondence Problem

We assume the reader to be familiar with the theory of formal (ω)-languages [HMU01, Tho90, Sta97]. We recall some usual notation of formal language theory.
When Σ is a finite alphabet, a *non-empty finite word* over Σ is any sequence $x = a_1 a_2 \cdots a_k$, where $a_i \in \Sigma$ for $i = 1, \ldots, k$, and k is an integer ≥ 1. $\Sigma^\star$ is the *set of finite words* (including the empty word) over Σ. The usual concatenation product of two finite words u and v is denoted $u \cdot v$ and sometimes just uv.
The *first infinite ordinal* is ω. An ω-*word* over Σ is an ω -sequence $a_1 a_2 a_3 \cdots$, where for all integers $i \geq 1$, $a_i \in \Sigma$. The *set of* ω-*words* over the alphabet Σ is denoted by Σ^ω. An ω-*language* over an alphabet Σ is a subset of Σ^ω.

We assume the reader to be familiar with the arithmetical hierarchy on subsets of $\mathbb{N}$, and also on subsets of Σ^ω for a finite alphabet Σ, see [Rog67, Sta97].

Recall first the well known result about the undecidability of the Post Correspondence Problem, denoted PCP.

Theorem 2.1 (Post, see [HMU01]) *Let Γ be an alphabet having at least two elements. Then it is undecidable to determine, for arbitrary n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ of non-empty words in $\Gamma^\star$, whether there exists a non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that $x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}$.*

On the other hand, the infinite Post Correspondence Problem, also called ω-PCP, has been shown to be undecidable by Ruohonen in [Ruo85] and by

Gire in [Gir86].

Theorem 2.2 *Let Γ be an alphabet having at least two elements. Then it is undecidable to determine, for arbitrary n-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ of non-empty words in $\Gamma^\star$, whether there exists an infinite sequence of indices $i_1, i_2, \ldots, i_k \ldots$ such that $x_{i_1} x_{i_2} \cdots x_{i_k} \cdots = y_{i_1} y_{i_2} \cdots y_{i_k} \cdots$*

Notice that an instance Ins of the ω-PCP is given by two n-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ of non-empty words in $\Gamma^\star$, and if there exist some solutions of the ω-PCP of instance Ins then these solutions are infinite words over the alphabet $\{1, \ldots, n\}$.

We now recall some known notions, which will be useful in the proof of our main result.

We first recall the variant of the PCP called the modified Post Correspondence Problem.

The MPCP consists, given two n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ of non-empty words in $\Gamma^\star$, in determining whether there exists a non-empty sequence of indices $i_1, i_2, \ldots, i_k$ such that

$$x_1 x_{i_1} x_{i_2} \cdots x_{i_k} = y_1 y_{i_1} y_{i_2} \cdots y_{i_k}.$$

Similarly one can define the ω-MPCP. The ω-MPCP consists, given two n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ of non-empty words in $\Gamma^\star$, in determining whether there exists an infinite sequence of indices $i_1, i_2, \ldots, i_k \ldots$ such that

$$x_1 x_{i_1} x_{i_2} \cdots x_{i_k} \cdots = y_1 y_{i_1} y_{i_2} \cdots y_{i_k} \cdots$$

Recall also that, as usual, a Turing machine is of the form $\mathcal{M} = (Q, \Sigma, \Gamma, \delta, q_0)$, where Q is a finite set of states, Σ is a finite input alphabet, Γ is a finite tape alphabet satisfying $\Sigma \subseteq \Gamma$ and containing a special blank symbol $\Box \in \Gamma \setminus \Sigma$, q_0 is the initial state, and δ is a mapping from $Q \times \Gamma$ to subsets of $Q \times \Gamma \times \{L, R, S\}$.

Recall that Turing machines have also been considered for the reading of infinite words, see [CG78a, CG78b, Sta97]. In particular, a Turing machine $\mathcal{M}$ reading infinite words over a finite alphabet Σ accepts a word $\sigma \in \Sigma^\omega$ for $1'$-acceptance condition iff there is an infinite run of $\mathcal{M}$ on σ visiting only states in a set $F \subseteq Q$ of accepting states.

We now state the following result, giving the exact complexity of the infinite Post Correspondence Problem.

Theorem 2.3 *The infinite Post Correspondence Problem is a Π^0_1-complete problem.*

Proof. We are firstly going to recall a sketch of Gire's proof of the undecidability of the ω-PCP. Next we will determine its exact complexity.

Recall that the proof of Theorem 2.2 in [Gir86] is given in two steps.

Firstly one can see, as in the finitary case (see [HMU01, page 396]) that the ω-MPCP can be reduced to the ω-PCP.

Secondly Gire showed that one can associate in a recursive manner, to each pair $(\mathcal{M}_z, w)$ where $\mathcal{M}_z$ is the Turing machine of index $z \in \mathbb{N}$ and w is an input word for $\mathcal{M}_z$, an instance of the ω-MPCP consisting of two n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ such that there exists an infinite sequence of indices $i_1, i_2, \ldots, i_k \ldots$ such that

$$x_1 x_{i_1} x_{i_2} \cdots x_{i_k} \cdots = y_1 y_{i_1} y_{i_2} \cdots y_{i_k} \cdots$$

if and only if the Turing machine $\mathcal{M}_z$ does not halt on the input w.

On the other hand it is well known that the halting problem is Σ^0_1-complete and thus the ω-MPCP is Π^0_1-hard since the complement of the halting problem, which is Π^0_1-complete, is reduced to the ω-MPCP. Moreover the ω-MPCP can be reduced to the ω-PCP thus the ω-PCP is also Π^0_1-hard.

We now show that the ω-PCP is in the class Π^0_1.

Let now an instance Ins of the ω-PCP be given by two n-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ of non-empty words in $\Gamma^\star$. We can easily associate in a recursive manner to this instance a deterministic Turing machine $\mathcal{M}$ with $1'$-acceptance condition reading infinite words over the alphabet $\{1, \ldots, n\}$ and accepting an infinite word $x \in \{1, \ldots, n\}^\omega$ if and only if x is a solution of the ω-PCP of instance Ins.

On the other hand, the set of infinite words accepted by such a deterministic Turing machine with $1'$-acceptance condition is known to be an effective Π^0_1-subset of $\{1, \ldots, n\}^\omega$ [Sta97]. Thus the set of solutions of the ω-PCP of instance Ins is an effective Π^0_1-set accepted by a deterministic Turing machine $\mathcal{M}$ with $1'$-acceptance condition which can be constructed from Ins.

Staiger proved in [Sta93, page 638] that it is Π^0_1-complete to decide whether such a Π^0_1-set is non-empty. This is also stated by Cenzer and Remmel in [CR03, Theorem 4.1 (ii)].

Therefore, the problem to determine whether a given instance Ins of the ω-PCP has a solution is in the class Π^0_1. This ends the proof.

$\square$

3 Concluding remarks

We have given the exact complexity of the infinite Post Correspondence Problem, showing that it is Π^0_1-complete. Thus the infinite Post Correspondence Problem is not "more complex" than the Post Correspondence Problem, which is known to be Σ^0_1-complete, but has the exact dual complexity.

We hope that this result will help to get a better understanding of the exact complexity of some other decision problems. Indeed, when the PCP is reduced to a decision problem P then we know that P is Σ^0_1-hard, and in particular P is not recursive. But if we can also reduce the infinite Post Correspondence Problem to P then P is Π^0_1-hard, and in particular it is not in the class Σ^0_1, so it is not even recursively enumerable. For instance, Blondel and Canterini proved in [BC03] that some problems about probabilistic automata are undecidable, using a reduction from the ω-PCP, and we can now infer from the above result that these problems are not even recursively enumerable.
Finally, we mention also that in another paper [Fin12], we gave a complete proof of the Σ^1_1-completeness of the ω-PCP in a regular ω-language, also denoted ω-PCP(Reg), and we applied this result to get the exact complexity of several highly undecidable problems about infinitary rational relations and ω-rational functions.

Acknowledgement. I wish to thank the anonymous referees for useful comments on a preliminary version of this paper.

References

[BC03] V. D. Blondel and V. Canterini. Undecidable problems for probabilistic automata of fixed dimension. *Theory of Computing Systems*, 36(3):231–245, 2003.

[CG78a] R.S. Cohen and A.Y. Gold. ω-computations on deterministic pushdown machines. *Journal of Computer and System Science*, 16:275–300, 1978.

[CG78b] R.S. Cohen and A.Y. Gold. ω-computations on Turing machines. *Theoretical Computer Science*, 6:1–23, 1978.

[CR03] D. A. Cenzer and J. B. Remmel. Index sets for omega-languages. *Mathematical Logic Quaterly*, 49(1):22–33, 2003.

[Fin03] O. Finkel. Undecidability of topological and arithmetical properties of infinitary rational relations. *RAIRO-Theoretical Informatics and Applications*, 37(2):115–126, 2003.

[Fin12] O. Finkel. Three applications to rational relations of the high undecidability of the infinite Post correspondence problem in a regular -language. *International Journal of Foundations of Computer Science*, 23(7):1481–1498, 2012.

[Gir86] F. Gire. Two decidability problems for infinite words. *Information Processing Letters*, 22(3):135–140, 1986.

[Har02] T. Harju. Decision questions on integer matrices. In *Proceedings of the International Conference Developments in language theory (Vienna, 2001)*, volume 2295 of *Lecture Notes in Computer Science*, pages 57–68. Springer, Berlin, 2002.

[HH06] V. Halava and T. Harju. Undecidability of infinite Post correspondence problem for instances of size 9. *Theoretical Informatics and Applications*, 40(4):551–557, 2006.

[HHK06] V. Halava, T. Harju, and J. Karhumäki. Undecidability in omega-regular languages. *Fundamamenta Informaticae*, 73(1–2):119–125, 2006.

[HMU01] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to automata theory, languages, and computation.* Addison-Wesley Publishing Co., Reading, Mass., 2001. Addison-Wesley Series in Computer Science.

[Pri00] C. Prieur. *Fonctions Rationnelles de Mots Infinis et Continuité.* PhD thesis, Université Paris VII, 2000.

[Rog67] H. Rogers. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, New York, 1967.

[Ruo85] K. Ruohonen. Reversible machines and Post's correspondence problem for biprefix morphisms. *Elektronische Informationsverarbeitung und Kybernetik*, 21(12):579–595, 1985.

[Sim10] P. Simonnet. 2010. Personal communication.

[Sta93] L. Staiger. Recursive automata on infinite words. In P. Enjalbert, A. Finkel, and K. W. Wagner, editors, *Proceedings of the*

10th Annual Symposium on Theoretical Aspects of Computer Science, STACS 93, Würzburg, Germany, February 25-27, 1993, volume 665 of *Lecture Notes in Computer Science*, pages 629–639. Springer, 1993.

[Sta97] L. Staiger. ω-languages. In *Handbook of formal languages, Vol. 3*, pages 339–387. Springer, Berlin, 1997.

[Tho90] W. Thomas. Automata on infinite objects. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, Formal models and semantics, pages 135–191. Elsevier, 1990.