Theory Comput. Systems **36**, 231–245 (2003)
DOI: 10.1007/s00224-003-1061-2

Theory of Computing Systems
© 2003 Springer-Verlag
New York Inc.

Undecidable Problems for Probabilistic Automata of Fixed Dimension*

Vincent D. Blondel and Vincent Canterini

Division of Applied Mathematics, University of Louvain,
Bâtiment Euler, Avenue Georges Lemaitre 4,
B-1348 Louvain-la-Neuve, Belgium
{blondel,canterini}@inma.ucl.ac.be

Abstract. We prove that several problems associated with probabilistic finite automata are undecidable for automata whose number of input letters and number of states are fixed. As a corollary of one of our results we prove that the problem of determining if the set of all products of two 47×47 matrices with nonnegative rational entries is bounded is undecidable.

1. Introduction

In this paper we provide new undecidability proofs for several problems associated with probabilistic finite automata (PFAs). Probabilistic finite automata accept words with a certain probability, they were introduced in the 1960s by Rabin as a generalization of finite deterministic automata [R1] (see also [P3] for a book-length treatment). The first problem we consider is the emptiness problem: we are given a PFA M and a probability threshold λ and we are asked if there is a word that is accepted by M with probability exceeding λ. We show that this problem is undecidable for PFAs with two input letters and 46 states. We then consider problems related to isolated thresholds. A probability threshold is said to be isolated if it cannot be approached arbitrarily closely. One motivation for considering isolated thresholds follows from the fact that the set of words accepted with a probability exceeding an isolated threshold is regular. We prove that the problems of deciding if a given threshold is isolated, and the problem of deciding if a given PFA has an isolated threshold are both undecidable for automata of fixed dimensions (two input letters and respectively 420 and 2354 states). In order to derive these two results, we first

* This paper presents research results of the Belgian Programme on Interuniversity Attraction Poles, initiated by the Belgian State, Prime Minister's Office for Science, Technology and Culture. The scientific responsibility rests with its authors.

prove that an infinite version of the classical Post correspondence problem is undecidable for a fixed number of pairs of words. This result appears to be of independent interest.

We now describe our results in some more detail. Let Σ be a finite set of input letters and let Σ^* denote the set of all finite input words; typical elements of Σ^* will be denoted $w = \sigma_1 \cdots \sigma_N$. A *deterministic finite automaton* partitions the elements of Σ^* between those that it accepts and those that it rejects. A *probabilistic finite automaton* assigns an acceptance *probability* to the elements of Σ^*. This acceptance probability is obtained as follows. The probabilistic automaton M is given by a finite set Q of n states, $n \times n$ row-stochastic transition matrices T_σ (one for each symbol $\sigma \in \Sigma$), one initial state, and one final state (the initial and finite states need not be distinct). At time $k = 1$ the system is in its initial state. At a typical time $k \geq 1$, the state of the system is equal to some $i \in Q$, an input letter $\sigma \in \Sigma$ is chosen, and the next state is chosen at random and is equal to j with probability $(T_\sigma)_{ji}$. We denote by $f_M(w)$ the probability of being in the final state upon input of the word $w = \sigma_1 \cdots \sigma_N$. Thus, $f_M(w)$ is equal to the probability of going from the initial to the final state after the actions $\sigma_1, \ldots, \sigma_N$ have been taken; we say that the automaton *accepts the word* w *with probability* $f_M(w)$. It is easy to see that the function f_M can be obtained as

$$f_M(w) = \pi^{\mathrm{T}} T_w \eta,$$

where $\cdot^{\mathrm{T}}$ denotes matrix transposition, $T_w = T_{\sigma_1} \cdots T_{\sigma_N}$, and π (respectively, η) is a column vector whose entries are all equal to zero except for the entry whose index is that of the input state (respectively, output state) which is equal to one.

The emptiness problem for PFAs is the following problem. Assume that we are given a PFA M and some probability threshold ("cut-point") λ with $0 \leq \lambda \leq 1$. The set $\{w \in \Sigma^*\colon\ f_M(w) > \lambda\}$ is the set of words accepted with a probability exceeding λ. The *emptiness problem* (also known as the *threshold problem* or the *string existence problem*) is the problem of deciding for a given PFA and a given threshold λ whether or not this set is empty, i.e., whether or not there is a string that is accepted with a probability exceeding λ. The emptiness problem has been proved undecidable by Paz by reduction from a problem on context-free languages (Theorem 6.17 in Chapter III of [P3]). This context-free problem is proved undecidable in [G] by reduction from Post's correspondence problem. The complete reduction can be reconstructed from the long chain of arguments appearing in these two references.[1] Paz was not interested in deriving bounds on the PFA for which the problem is undecidable. His proof uses on several occasions a construction which leads to an exponentiation of the number of states. A conceptually different proof—by reduction from the halting problem for 2-counter machines—is given in [CL] for the purpose of studying bounded interactive proofs. In Section 2 we provide a new elementary proof. Our proof is by reduction from Post's correspondence problem. In addition from being elementary (it only uses elementary linear algebra), our reduction has the advantage that it provides bounds on the number of states of the automaton for which the problem is undecidable; a feature that was not present in the two previous proofs. More explicitly, we prove in Theorem 2.1 that the emptiness problems is undecidable for PFAs with two input letters and with $6k+4$ states, where k is any number of pairs of words for which Post's correspondence problem is

[1] Theorem 6.17 of [P3] refers to [Ginzburg, 1966]; a reference that is not present in the reference list given in [P3]. The correct reference is [G].

undecidable. Post's correspondence problem is known to be undecidable for seven pairs and so the emptiness problem is undecidable for 46 states; we do not expect this bound to be sharp. In fact, we do not even know if there is an effective procedure for the case of PFAs with two states. By using small variations of our proof we show that the similar problems of determining if there are words w for which $f(w) > \lambda$, $f(w) \leq \lambda$, or $f(w) < \lambda$ are all undecidable for PFAs with two input letters and 46 states.

We now describe problems associated with isolated thresholds ("isolated cutpoints"). A probability threshold λ is said to be *isolated* for some PFA M if there exists some $\epsilon > 0$ such that $|f_M(w) - \lambda| > \epsilon$ for all $w \in \Sigma^*$. In other words, a threshold is isolated if it cannot be approached arbitrarily closely by probabilities associated with input words. The interest for considering isolated thresholds is that the languages they define are in general less expressive than those associated with arbitrary thresholds. The language $\{w \in \Sigma^*\colon\ f_M(w) > \lambda\}$ need not be regular in general but is regular when λ is isolated (see [R3] for a proof). This naturally raises the question of deciding if a given threshold is isolated (the *threshold isolation problem*), and the question of deciding if a given PFA has an isolated threshold (the *isolated threshold existence problem*). These two problems are stated in [R3] and in [P3]. The threshold isolation problem is proved undecidable in [BMT] (a first incomplete version of the proof appears in [B1]). This result has been recently rediscovered in [MHC] using a completely different proof technique.[2] The proof in [MHC] proceeds by reduction from the halting problem whereas that in [BMT] uses a reduction from an infinite version of Post's correspondence problem. In [BMT] the authors also prove that the isolated threshold existence problem is undecidable. None of these proofs provide undecidability for PFAs with a fixed number of states. In Section 4 we prove that both problems are undecidable for PFAs with a fixed number of states. In order to fix the number of states, we first prove in Section 3 that the infinite correspondence problem is undecidable for 105 pairs of words. This result appears to be of independent interest.

We finally remark that all the above questions can also be phrased in terms of the *range* of the function f_M associated with the PFA M. For a given PFA M, define the range of f_M by $\Omega_M = \{f_M(w)\colon\ w \in \Sigma^*\}$. The emptiness problem is the problem of deciding if Ω_M contains a value exceeding λ, the threshold isolation problem is the problem of deciding if there is an open set centered on λ that is not contained in Ω_M, and the isolated threshold existence problem is the problem of deciding if the set Ω_M is dense in the unit interval [0, 1].

The concept of a PFA appears in a number of different contexts. They are used to study Arthur–Merlin games [BM], [CHPW], space bounded interactive proofs [CL], rational series and semigroups of matrices [BT2], and Markov decision processes and planning questions [B2], [MHC], [PT] (see Section 5 of [BT3] for a survey). The results we prove here have implications for all problems that were proved undecidable by reduction from one of the problems we consider. In particular, using a reduction that appears in [BT2], we prove as a corollary of Theorem 2.1 that the problem of determining if the set of all products of two 47×47 matrices with nonnegative rational entries is bounded is undecidable. This result was so far only known for matrices of unbounded dimensions and has implications for the stability analysis of switched systems, as explained in [BT2].

[2] The author of [MHC] does not seem to be aware of the references [B1] and [BMT].

2. Threshold Problems

The emptiness problem is the problem of determining, for a given PFA and probability threshold λ, if there exists a word that is accepted with a probability exceeding λ. We show that this problem is undecidable for PFAs with two letters and 46 states. Our proof is by reduction from Post's correspondence problem on n pairs of words (PCP(n)):

> PCP(n)
>
> *Instance*: A finite alphabet $\mathcal{A}$, n pairs of words $(u_i, v_i) \in \mathcal{A}^* \times \mathcal{A}^*$.
> *Question*: Does there exist some $N \geq 1$ and indices $i_1, \ldots, i_N \in \{1, \ldots, n\}$ for which $u_{i_1} \cdots u_{i_N} = v_{i_1} \cdots v_{i_N}$?

Post's correspondence problem is trivially decidable for one letter alphabets but is undecidable when the alphabet contains more than one letter; for a proof of this result see the original paper [P4] or [HU]. The decidability of PCP(n) does not depend on the cardinality of $\mathcal{A}$ when $\#\mathcal{A} \geq 2$ but depends on the number of pairs of words. The number of pairs of words for which the problem is undecidable has been successively improved. It is now known that the case of $n = 7$ pairs is undecidable, see [MS2]. The decidability status of PCP(2) was a long standing open problem until it was proved to be decidable in [EKR] and [P2]. The cases $n = 3, \ldots, 6$ are yet unresolved.

Post's correspondence problem can also be formulated as follows. Consider k words $u_i \in \mathcal{A}^*$ and $v_i \in \mathcal{A}^*$. To the sequence of indices $w = i_1 i_2 \cdots i_N$ with $i_j \in \{1, \ldots, k\}$ we associate the words $u_w = u_{i_1} \cdots u_{i_N} \in \mathcal{A}^*$ and $v_w = v_{i_1} \cdots v_{i_N} \in \mathcal{A}^*$. Post's correspondence problem is the problem of determining if there exists a sequence w of indices for which the associated words u_w and v_w are identical.

Theorem 2.1. *For a given PFA and a given cut-point* $0 \leq \lambda \leq 1$, *the problems of deciding if*

(1) *there exists a word w for which $f(w) \geq \lambda$,*
(2) *there exists a word w for which $f(w) > \lambda$,*
(3) *there exists a word w for which $f(w) \leq \lambda$,*
(4) *there exists a word w for which $f(w) < \lambda$*

are all undecidable. Moreover, these problems remain undecidable for PFAs that have two letters, and that have $6k+4$ *states where k denotes any number of pairs of words for which Post's correspondence problem is undecidable* (*Post's correspondence problem is undecidable for $k = 7$ pairs*; *see* [MS2]).

Proof. We give a complete proof only for the first case. The other three cases can be proved similarly, a sketch of these cases is provided below. The proof is by reduction from Post's correspondence problem and proceeds in several steps. We start from an instance of Post's correspondence problem. In a first step we use a variation of an encoding originally due to Paterson [P1] (see also [HK]) to construct a rational series whose terms are all nonnegative and whose zero terms exactly correspond to the solutions to Post's correspondence problem. A series with this property can be obtained by constructing the series whose coefficients are the square of the coefficients of the series constructed in [P1]. Such a construction is described, e.g., in [SS]. We provide a slightly different proof that has the advantage that the resulting matrices are of dimension six rather than nine. In a second step we reduce the cardinality of the alphabet to two at the expense of an increase of the state dimension. In a third step we modify this series to obtain a series whose terms that are positive are those that correspond to the solutions of Post's correspondence problem. In a fourth step we go through a sequence of modifications and eventually obtain a series whose associated matrices are stochastic, and with canonical input and output vectors.

Let $(u_i, v_i) \in \mathcal{A}^* \times \mathcal{A}^*$ $(i = 1, \ldots, k)$ be an instance of PCP(k). We assume without loss of generality that the cardinality of $\mathcal{A}$ is equal to two and define $\mathcal{A} = \{1, 2\}$.

Step 1. We first encode the correspondence problem as a problem for rational series. Let therefore $\sigma\colon \mathcal{A}^* \to \mathbb{N}$ give the 10-adic representation of words of $\mathcal{A}^*$. To the pair of words $(u, v) \in \mathcal{A}^* \times \mathcal{A}^*$ we associate the nonnegative matrix $A(u, v) \in \mathbb{N}^{6\times 6}$ as follows:

$$A(u,v) = \begin{pmatrix} 10^{2|u|} & 0 & 0 & 0 & 0 & 0 \\ 0 & 10^{|u|+|v|} & 0 & 0 & 0 & 0 \\ 0 & 0 & 10^{2|v|} & 0 & 0 & 0 \\ \sigma(u)10^{|u|} & \sigma(v)10^{|u|} & 0 & 10^{|u|} & 0 & 0 \\ 0 & \sigma(u)10^{|v|} & \sigma(v)10^{|v|} & 0 & 10^{|v|} & 0 \\ \sigma(u)^2 & 2\sigma(u)\sigma(v) & \sigma(v)^2 & 2\sigma(u) & 2\sigma(v) & 1 \end{pmatrix}.$$

Straightforward calculations show that this particular matrix structure is preserved under matrix multiplication, i.e., $\gamma(u_1, v_1)\gamma(u_2, v_2) = \gamma(u_1u_2, v_1v_2)$ for all words u_1, u_2, v_1, v_2. We define $A_i \in \mathbb{N}^{6\times 6}$ by $A_i = A(u_i, v_i)$ and $A_w = A_{i_1} \cdots A_{i_N}$ for $w = i_1 \cdots i_N$. Post's correspondence problem is the problem of determining if there exists a word w and an associated product A_w whose (6, 4)th and (6, 5)th entries are equal. We now define $\alpha = (0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1)^{\mathrm{T}}$ and $\beta = (1\ \ -2\ \ 1\ \ 0\ \ 0\ \ 0)^{\mathrm{T}}$. Then

$$\alpha^{\mathrm{T}} A(u, v)\beta = \sigma(u)^2 - 2\sigma(u)\sigma(v) + \sigma(v)^2 = (\sigma(u) - \sigma(v))^2 \geq 0,$$

and we have equality to zero in this inequality if and only if $u = v$. The correspondence problem is thus equivalent to the problem of deciding if there exists a word w for which $\alpha^{\mathrm{T}} A_w \beta = 0$.

Step 2. As a next step, we reduce the number of matrices to two. Let $\{A_1, \ldots, A_k\}$ be the 6×6 matrices defined above. Define two $6k \times 6k$ matrices B_1, B_2 by $B_1 = \mathrm{diag}(A_1, \ldots, A_k)$ (i.e., B_1 is block-diagonal with blocks $A_1, \ldots, A_k$ in that order) and

$$B_2 = \begin{pmatrix} 0 & I_{6(k-1)} \\ I_6 & 0 \end{pmatrix},$$

where I_r is the $r \times r$ identity matrix. Define then $\alpha_1 = (\alpha^{\mathrm{T}}\ \ 0)^{\mathrm{T}}$ and $\beta_1 = (\beta^{\mathrm{T}}\ \ 0)^{\mathrm{T}}$. To $w = i_1 \cdots i_N \in \{1, 2\}^*$ we associate the matrix $B_w = B_{i_1} \cdots B_{i_N}$ and claim that

$\alpha_1^{\mathrm{T}} B_w \beta_1 \geq 0$ with equality to zero only if there exists a word w for which $\alpha^{\mathrm{T}} A_w \beta = 0$. The proof of this claim is analogous to the proof of Theorem 1 in [BT1] and is not detailed here. It essentially uses the observation that $B_2^k = I_{6k}$ and

$$B_2^{i-1} B_1 B_2^{k-(i-1)} = \operatorname{diag}(A_i, \ldots, A_k, A_1, \ldots, A_{i-1})$$

for $i = 1, \ldots, k$.

Step 3. We define two new matrices $C_1, C_2 \in \mathbb{N}^{(6k+1)\times(6k+1)}$ by $C_1 = \operatorname{diag}(B_1, 1)$ and $C_2 = \operatorname{diag}(B_2, 1)$. We then let $\alpha_2 = (\alpha_1^{\mathrm{T}} \;\, 1)^{\mathrm{T}}$ and $\beta_2 = (-\beta_1^{\mathrm{T}} \;\, 1)^{\mathrm{T}}$. Then $\alpha_2^{\mathrm{T}} C_w \beta_2 = 1 - \alpha_1^{\mathrm{T}} B_w \beta_1$ and so $\alpha_2^{\mathrm{T}} C_w \beta_2 \geq 0$ for all words w and there exists a word w for which $\alpha_2^{\mathrm{T}} C_w \beta_2 > 0$ if and only if the correspondence problem has a solution.

Step 4. We finally need to transform our problem into an emptiness problem for a PFA. Several substeps are needed for this. In a first substep we show how to reduce our problem to a situation where the vectors α and β are normalized. In a second subset we reduce the problem to a situation where all matrices have row and column sum equal to zero. Finally, we use a transformation to obtain stochastic matrices. The transformations we use are analogous to those used in the proof of the main result of [T].

(a) We define two new matrices $D_1, D_2 \in \mathbb{N}^{(6k+2)\times(6k+2)}$ by

$$D_i = \begin{pmatrix} 0 & \alpha_2^{\mathrm{T}} C_i \\ 0 & C_i \end{pmatrix}, \qquad \alpha_3 = (1 \;\; 0 \;\; \cdots \;\; 0)^{\mathrm{T}}, \qquad \beta_3 = (1 \;\; \beta_2^{\mathrm{T}})^{\mathrm{T}}.$$

Then $\alpha_3^{\mathrm{T}} D_\varepsilon \beta_3 = \alpha_3^{\mathrm{T}} \beta_3 = 1$ (ε denotes the empty word) and $\alpha_3^{\mathrm{T}} D_w \beta_3 = \alpha_2^{\mathrm{T}} C_w \beta_2$ for $w \neq \varepsilon$. Let $\{\beta_3, v_2, v_3, \ldots, v_{6k+2}\}$ be an orthogonal basis of $\mathbb{R}^{6k+2}$; such a basis can be effectively constructed by using the Gram–Schmidt process. Then the vectors $\alpha_3, v_2, \ldots, v_{N+1}$ are linearly independent (indeed, assume not, then α_3 is a linear combination of the vectors v_i and therefore $\alpha_3 \beta_3$ must be equal to zero). Hence the matrix

$$R = \begin{pmatrix} \alpha_3 \\ v_2 \\ \vdots \\ v_{N+1} \end{pmatrix}$$

is nonsingular. Define α_4 and β_4 by $\alpha_4 = R^{-1}\alpha_4$ and $\beta_4 = R\beta_3$. Then

$$\alpha_4 = \beta_4 = (1 \;\; 0 \;\; \cdots \;\; 0)^{\mathrm{T}}.$$

We further define $E_i = R D_i R^{-1}$ and obtain

$$\alpha_4^{\mathrm{T}} E_w \, \beta_4 = \alpha_3^{\mathrm{T}} D_w \, \beta_3 = \alpha_2^{\mathrm{T}} C_w \, \beta_2 \qquad (w \neq \varepsilon).$$

(b) Next we construct two matrices $F_1, F_2 \in \mathbb{N}^{(6k+4)\times(6k+4)}$. The matrices are defined by

$$F_i = \begin{pmatrix} 0 & 0 & 0 \\ t_i & E_i & 0 \\ s_i & r_i & 0 \end{pmatrix}$$

and the entries s_i, t_i, and r_i are chosen so that the row and column sums of F_i are equal to zero. This property is equivalent to $F_i\mathbf{1} = 0$ and $\mathbf{1}^{\mathrm{T}}F_i = 0$ where $\mathbf{1}$ is the vector whose entries are all equal to one. Every matrix F_w with $w \neq \varepsilon$ has this property. Denoting now

$$\alpha_5 = (0 \;\; \alpha_4^{\mathrm{T}} \;\; 0)^{\mathrm{T}} \quad \text{and} \quad \beta_5 = (0 \;\; \beta_4^{\mathrm{T}} \;\; 0)^{\mathrm{T}}$$

we obtain

$$\alpha_5^{\mathrm{T}} F_w\, \beta_5 = \alpha_4^{\mathrm{T}} E_w\, \beta_4 = \alpha_3^{\mathrm{T}} D_w\, \beta_3 = \alpha_2^{\mathrm{T}} C_w\, \beta_2 \qquad (w \neq \varepsilon).$$

(c) Let Q denote the matrix whose entries are all equal to one and notice that $Q^i = n^{i-1}Q$ where n is the dimension of Q. Since the row and column sums of F_w are equal to zero we have

$$F_w Q = QF_w = 0 \qquad (w \neq \varepsilon).$$

We now define $G_i = F_i + \gamma Q$ for $\gamma \geq 0$ so large that all the entries of the matrices G_i are positive. Then the matrices H_i defined by

$$H_i = \frac{1}{\gamma(6k+4)} G_i$$

are doubly stochastic. Using

$$G_w = F_w + \gamma^{|w|} Q^{|w|} = F_w + \gamma^{|w|}(6k+4)^{|w|-1} Q$$

for any nonempty word w we also observe that

$$H_w = \frac{1}{\gamma(6k+4)^{|w|}} F_w + \frac{1}{(6k+4)} Q.$$

Defining $\alpha_6 = \alpha_5$, $\beta_6 = \beta_5$ we obtain

$$\begin{aligned} \alpha_6^{\mathrm{T}} H_w \beta_6 &= \frac{1}{\gamma(6k+4)^{|w|}} \alpha_5^{\mathrm{T}} F_w \beta_5 + \frac{1}{(6k+4)} \\ &= \frac{1}{\gamma(6k+4)^{|w|}} \alpha_2^{\mathrm{T}} C_w\, \beta_2 + \frac{1}{(6k+4)} \end{aligned}$$

for all nonempty word w. Post's correspondence problem has a solution if and only if there exists a nonempty word w for which $\alpha_2^{\mathrm{T}} C_w \beta_2 > 0$. This will be the case if and only if there exists a nonempty word w for which

$$\alpha_6^{\mathrm{T}} H_w \beta_6 > \frac{1}{6k+4}.$$

The matrices H_1 and H_2 together with the vectors $\alpha_6 = \beta_6$ define a PFA on two letters and $6k + 4$ states. The proof therefore follows by setting $\lambda = 1/(6k + 4)$.

Step 5. We now briefly comment on the adaptation of this proof for proving the cases $f(w) \geq \lambda$, $f(w) < \lambda$, and $f(w) \leq \lambda$. The only modification that is needed is at step 3. In the present proof we construct C_1, C_2 and α_2, β_2 such that there exists a word w for which $\alpha_2^{\mathrm{T}} C_w \beta_2 > 0$ if and only if the correspondence problem has a solution. We can easily construct matrices and vectors such that $\alpha_2^{\mathrm{T}} C_w \beta_2 \geq 0$, $\alpha_2^{\mathrm{T}} C_w \beta_2 < 0$, and $\alpha_2^{\mathrm{T}} C_w \beta_2 \leq 0$ if and only if the correspondence problem has a solution. □

Let Σ be a finite set of matrices and let $\|\cdot\|$ be some matrix norm. We say that the set Σ is (product) *bounded* if the set $\{\|A_1 \cdots A_k\| : A_i \in \Sigma,\ i = 1, \ldots, k\}$ is bounded. The undecidability of the emptiness problem for PFAs is used in [BT2] to prove that product boundedness of sets consisting of two matrices is undecidable. By adapting the reduction used in [BT2], we easily deduce the following corollary.

Corollary 2.1. *The problem of determining if the set of all products of two* 47×47 *matrices with nonnegative rational entries is bounded is undecidable.*

The fact that the matrices have rational (and not just integer) entries is crucial here. Indeed, for matrices with integer entries, product boundedness of Σ is equivalent to the finiteness of the semigroup generated by Σ and the later property is proved decidable in [J] and [MS1]. Thus, boundedness of the semigroup generated by two matrices is undecidable when the matrices have rational entries, but is decidable when they have integer entries.

3. Infinite Post Correspondence

In this section we extend Post's original correspondence problem to infinite correspondences. It is clear that when a finite correspondence between pairs of words is possible, then an infinite correspondence is also possible. The converse of this statement is not true. Consider for instance the following pairs:[3] (*aab*, *a*) and (*aa*, *baa*). The associated correspondence problem does not have a finite solution but an infinite correspondence is possible. Several definitions of what is meant by an "infinite correspondence" appear to be possible. We first show that all definitions we introduce are equivalent and then show that these infinite correspondence problems (w-PCP(n)) are undecidable for $n = 105$

[3] Personal communication of J. Karhumäki.

pairs of words. This result will be used in the next section to prove that questions related to isolated cut-points for PFAs are undecidable for automata of fixed dimension. The fact that the infinite Post correspondence problem is undecidable is proved in [B1] and is later mentioned in [R5], but so far it was unknown that the problem is undecidable for a fixed number of pairs [K]. Compared with the seven pairs of words for which PCP is undecidable, our bound of 105 appears to be conservative and it seems likely that there is room for improvement. Our bound is in fact directly related to the size of a small universal Turing machine and the minimal size of universal computing devices is the object of ongoing research and regular improvements; see, e.g., [KR].

On the decidability side, it is unknown if, as for the finite case, the case of two pairs of words is decidable [K]. Recently it was shown that the existence of an infinite solution is decidable for the particular case of *marked* morphisms; see [HH]. Marked morphisms correspond to the situation where the pairs of words (u_i, v_i) are such that no two words u_i start with the same letter, and similarly for v_i. This result is close to giving the decidability for two pairs of words, but does not quite do so.

Related to these questions, we also mention here that in [R5] Ruohonen has studied variations of Post's correspondence problem for different set-ups; in particular, doubly infinite words, doubly infinite powers of words, and circular words.

Let $\mathcal{A}$ and $\mathcal{B}$ be finite alphabets. An instance of the infinite Post correspondence problem is a couple (h, g) of functions $h, g\colon \mathcal{B} \to \mathcal{A}^+$. Every function $f\colon \mathcal{B} \to \mathcal{A}^+$ can be naturally extended to a morphism $f\colon \mathcal{B}^{\mathbb{N}} \to \mathcal{A}^{\mathbb{N}}$ and the infinite correspondence problem is then the problem of determining if there exists a word w for which $f(w) = g(w)$. In order to introduce other extensions of Post's correspondence problem to infinite words we need one more definition. The *longest common prefix* of two words $u, v \in \mathcal{A}^*$ is denoted by $u \wedge v$ and is given by $w \in \mathcal{A}^*$ with $w_i = u_i = v_i$ $(i = 1, \dots, |w|)$ and $u_{|w|+1} \neq v_{|w|+1}$ or $|w| = |u|$ or $|w| = |v|$. This operation can also be extended to infinite words.

Theorem 3.1. *Let $\mathcal{B}$ be an alphabet of n letters, let $\mathcal{A}$ be a finite alphabet, and let $h, g\colon \mathcal{B} \to \mathcal{A}^+$. Then the following are equivalent*:

(1) $\exists W \in \mathcal{B}^{\mathbb{N}}$ *such that* $h(W) = g(W)$;
(2) $\#\{\bigcup_{w\in\mathcal{B}^*} h(w) \wedge g(w)\} = +\infty$;
(3) $\forall L \in \mathbb{N}, \exists w_L \in \mathcal{B}^*, |h(w_L) \wedge g(w_L)| \geq L$.

When these conditions are satisfied, we say that the infinite correspondence problem has a solution.

Proof. Let h, g be two functions $\mathcal{B} \to \mathcal{A}^+$.

(1) $\Rightarrow$ (2) Let $W \in \mathcal{B}^{\mathbb{N}}$ be such that $h(W) = g(W)$. Then the map $\mathbb{N} \to \mathcal{A}^*\colon N \mapsto h(W_0 \cdots W_{N-1}) \wedge g(W_0 \cdots W_{N-1})$ is strictly increasing and the result follows.

(2) $\Rightarrow$ (3) Suppose (3) is false, that is $\exists L_0 \in \mathbb{N}, \forall w \in \mathcal{B}^*, |h(w) \wedge g(w)| < L_0$. Then the set $\{\bigcup_{w\in\mathcal{B}^*} h(w) \wedge g(w)\}$ is finite. This contradicts (2).

(3) $\Rightarrow$ (1) There exists a sequence $(w_n)_{n\geq 0}$ such that $\forall n \in \mathbb{N}, |h(w_n) \wedge g(w_n)| \geq n$. Since $\mathcal{B}^{\mathbb{N}}$ is compact as a metric space with the discrete topology, it follows that there exists a convergent subsequence $(w_{n_i})_{i\geq 0}$. We define $\lim_{i\to\infty} w_{n_i} = W \in \mathcal{B}^{\mathbb{N}}$. Since

the morphisms h and g are continuous, it follows that $h(W) = \lim_{i\to\infty} h(w_{n_i}) = \lim_{i\to\infty} g(w_{n_i}) = g(W)$ and so $h(W) = g(W)$. □

Since all the above definitions are equivalent, we choose one of them and state the infinite Post correspondence problem as follows:

ω-PCP(n)

Instance: Let $\mathcal{A}$ be a finite alphabet, let $\mathcal{B}$ be an alphabet of size at most n, and let (h, g) be two morphisms $\mathcal{B} \to \mathcal{A}^+$.

Question: Does there exists an infinite sequence $W \in \mathcal{B}^{\mathbb{N}}$ such that $h(W) = g(W)$?

It is possible to define a "left" infinite Post correspondence problem, in which we ask for the existence of a left-infinite word rather than a right-infinite word. Contrary to the finite case for which it is equivalent to proceed from the left or from the right, in the infinite case there are instances for which only one of the correspondences has a solution, e.g., the instance (a, ab), (b, a) has a right-infinite correspondence $(abababa\cdots)$ but no left-infinite correspondence since the last letters in the words of any given pair are always different. Nevertheless, the right and the left infinite problems are computationally equivalent, as we can easily reduce one to the other using the reversal map which to a word $w = w_1 \cdots w_l$ associates its mirror $\tilde{w} = w_l \cdots w_1$.

As for the classical proof that PCP is undecidable, we prove that ω-PCP is undecidable by reduction from a modified version of the problem in which we impose the first letter of the solution word. We obtain our result by combining the proof of Bertoni [B1] with a universal Turing machine encoding and sharp bounds on small universal Turing machines taken from [R4].

Theorem 3.2. ω-PCP(105) *is undecidable.*

Proof. The proof proceeds in two steps. First, from a small universal Turing machine U and an input x to U, we construct two morphisms h and g such that there exists a infinite word W whose first letter is given and such that $h(W) = g(W)$ if and only if U halts on x. In this construction the cardinality of the morphisms' alphabet does not depend on x. In a second step we reduce this modified correspondence problem with n rules to ω-PCP with $n + 1$ rules.

Step 1. We use a variation of the universal Turing machine with ten states and three letters given by Rogozhin (see [R4]). It is easy to see how to modify this machine to obtain a machine U with the following features. The machine has ten states $\{q_1, \ldots, q_{10}\}$ with q_1 the starting state. The tape alphabet has four letters (0, 1, b, and #) and the transition function of the machine is given by some function

$$\delta\colon \{q_1, \ldots, q_{10}\} \times \{0, 1, b, \#\} \to \{q_1, \ldots, q_{10}\} \times \{0, 1, b, \#\} \times \{L, R\}.$$

There are 40 state/symbol combinations for which this function needs to be defined. In 19 cases the resulting image has an R instruction; in 20 cases it has an L instruction, and in one case the transition function is not defined; this case corresponds to the machine being in a halting state. Consider now an input word $y \in \{0, 1, b\}^*$ to the machine. Let U start in state q_1 with its head on the first letter of y and with the rest of the tape filled with #. The problem of determining if U ever enters the state/symbol combination for which δ is not defined is undecidable.

We now describe how to construct morphisms that simulate U. We use words of $\{q_1, \dots, q_{10}, 0, 1, b\}^*$ to encode state/tape content combinations. Thus for example the word $01bq_7 1101b0$ means that the machine is in state q_7, the tape content is $\cdots \#01b1101b0\# \cdots$, and the machine reads the symbol 1 (i.e., the symbol immediately to the right of the head). The morphisms h, g take value in the set of words $\{q_1, \dots, q_{10}, 0, 1, b, \#\}^*$ and are defined as follows.

Starting correspondence: Let $y \in \{0, 1, b\}^*$ be the input word to the machine. Then we set

$$h(1) = \# \quad \text{and} \quad g(1) = \#q_1 y\#. \tag{1}$$

Propagation correspondences:

$$\begin{aligned} h(2) &= g(2) = 0, \\ h(3) &= g(3) = 1, \\ h(4) &= g(4) = b, \\ h(5) &= g(5) = \#. \end{aligned} \tag{2}$$

Instruction correspondences: For each instruction of the type $\delta(q, X) = (p, Y, R)$, we define

$$h(j) = qX \quad \text{and} \quad g(j) = Yp \tag{3}$$

and for each instruction of the type $\delta(q, X) = (p, Y, L)$ and for each $Z \in \{0, 1, b, \#\}$ we define

$$h(j) = ZqX \quad \text{and} \quad g(j) = pZY. \tag{4}$$

There is 1 starting correspondence, 4 propagation correspondences, 19 (right) instruction correspondences, and 4 × 20 (left) instruction correspondences. This leads to a total of 104 correspondences. Note that this total number of correspondences does not depend on the input word y. If the machine U does not halt on y, then it is clear how to construct an infinite word W that appropriately simulates this. On the other hand, if the machine halts on y, then the correspondence is no longer possible once the machine has halted and there exists no infinite word W for which $f(W) = g(W)$.

Step 2. We reduce the problem obtained above with n rules to ω-PCP($n + 1$). The reduction is similar to the standard reduction of the modified Post correspondence problem MPCP(n) to PCP($n + 2$) in the finite case; see, e.g., [HU]. Let $h, g\colon \mathcal{C} \to \Delta^+$ with $\mathcal{C} = \{c_1, \dots, c_n\}$. Let $\bar{b}$ be a symbol not in Δ. We define the alphabets $\mathcal{B} = \mathcal{C} \cup \{c_0\}$ and $\mathcal{A} = \Delta \cup \{\bar{b}\}$, and the *right* and *left* morphisms L and R defined on Δ by

$$L\colon \Delta \to \mathcal{A}^+,\ L(d) = \bar{b}d, \qquad R\colon \Delta \to \mathcal{A}^+,\ R(d) = d\bar{b}.$$

We then define an instance (h', g') of ω-PCP$(n+1)$ with h' and g': $\mathcal{B} \to \mathcal{A}^+$ by

$$g'(c_0) = L(g(c_1)) \quad \text{and} \quad h'(c_0) = \bar{b}R(h(c_1)) \tag{5}$$

and

$$g'(c) = L(g(c)) \quad \text{and} \quad h'(c) = R(h(c)) \qquad \text{for all} \quad c \in \mathcal{C}. \tag{6}$$

If $Z \in \mathcal{C}^{\mathbb{N}}$ is an infinite word such that $h(c_1 Z) = g(c_1 Z)$, then obviously $h'(c_0 Z) = g'(c_0 Z)$. Conversely, if $Y \in \mathcal{B}^{\mathbb{N}}$ is such that $h'(Y) = g'(Y)$, then clearly (5) implies that $Y_0 = c_0$ and $h(c_1 Y_1 Y_2 \cdots) = g(c_1 Y_1 Y_2 \cdots)$. Since the problem obtained in Step 1 has 104 correspondences this one has 105 correspondences. □

4. Threshold Isolation Problems

In this final section we consider two questions related to isolated thresholds. A probability threshold λ is said to be *isolated* for a PFA M if there exists some $\epsilon > 0$ such that $|f_M(w) - \lambda| > \epsilon$ for all $w \in \Sigma^*$. Bertoni et al. have proved (see [B1] and [BMT]) that the question of deciding if a given threshold is isolated (the *isolation threshold problem*) and the question of deciding if a given PFA has an isolated threshold (the *isolated threshold existence problem*) are both undecidable. We show that they are undecidable even if the PFA has a fixed number of states.

Theorem 4.1. ω-PCP(n) *is reducible to the isolation threshold problem for PFAs with two letters and* $4n$ *states and is reducible to the isolated threshold existence problem for PFAs with two letters and* $22n + 44$ *states. Since* w-PCP(105) *is undecidable, the isolation threshold problem is undecidable for PFAs with two letters and* 420 *states, and the isolated threshold existence problem is undecidable for PFAs with two letters and* 2354 *states.*

Proof. Let h, g: $\mathcal{B} \to \mathcal{A}^*$ be morphisms. Define $n = |\mathcal{B}|$ and let $q \geq |\mathcal{A}|$. For clarity of the presentation and without loss of generality we assume that $q = 9$. Let ρ: $\mathcal{A}^* \to [0, 1]$ be defined by $\rho(\varepsilon) = 0$ and

$$\rho(a_{i_1} \cdots a_{i_l}) = \sum_{j=1}^{l} i_j (10)^{j-l-1}. \tag{7}$$

Let A_h (respectively, A_g) be the probabilistic automaton that generates the probabilistic event $\varphi = \rho \circ f$ (respectively, $\psi = \rho \circ g$). The probabilistic automaton A_h can be given by the following two-states automaton on n letters:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, A_h(b) = \begin{pmatrix} 1 - \varphi(b) & \varphi(b) \\ 1 - \varphi(b) - 10^{|h(b)|} & \varphi(b) + 10^{|h(b)|} \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{8}$$

and similarly for A_g. It is clear from the construction that 0 is isolated in the set $\bigcup_{w\in\mathcal{B}^*}(\varphi(w)-\psi(w))$ if and only if there does not exist $W \in \mathcal{B}^{\mathbb{N}}$ such that $h(W) = g(W)$.

The function $e = \frac{1}{2} + (\varphi - \psi)/2$ can be obtained by the following probabilistic four-states automaton E on n letters:

$$\begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix}, E(b) = \begin{pmatrix} A_h(b) & 0 \\ 0 & A_g(b) \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}. \tag{9}$$

Then 0 is isolated for $\varphi - \psi$ if and only if $\frac{1}{2}$ is isolated for E. We now construct an automaton on two letters whose range is identical to that of E. From the second step of the proof of Theorem 2.1, it is easy to see how to construct two matrices A, T of size $4n \times 4n$ and two $4n$-dimensional vectors η, ν such that the following equality holds:

$$\bigcup_{w\in\mathcal{B}^*} e(w) = \bigcup_{w'\in\{A,T\}^*} \eta^{\mathrm{T}} w' \nu.$$

Moreover A, T, η, ν obviously define a $4n$-states PFA on two letters for which $\frac{1}{2}$ is an isolated cut-point if and only if 0 is isolated for $\varphi - \psi$. This shows that ω-PCP(n) is reducible to the problem of deciding if $\lambda = \frac{1}{2}$ is not isolated for a probabilistic finite $4n$-states automaton on two letters and so the first part of the proof is complete.

To prove the second part of the statement of the theorem, notice that the proof given in [BMT] is by reduction from ω-PCP, and that is obviously working in the bounded case. The proof in [BMT] gives a PFA on $n + 2$ letters and 22 states. Using the same technique as above for obtaining a PFA on two letters we finally obtain a PFA on two letters and with $22n + 44$ states. □

Acknowledgment

The original version of this paper has benefited from comments by Pascal Koiran and by two anonymous reviewers whom we gratefully acknowledge.

References

[B1] A. Bertoni. The solution of problems relative to probabilistic automata in the frame of the formal languages theory. In *Vierte Jahrestagung der Gesellschaft für Informatik*, pages 107–112, Berlin, 1974. Lecture Notes in Computer Science, Vol. 26. Springer-Verlag, Berlin, 1975.

[B2] J. Blythe. An overview of planning under uncertainty. In *Artificial Intelligence Today*, pages 85–110. Springer-Verlag, Berlin, 1999.

[BM] L. Babai and S. Moran. Arthur–Merlin games: a randomized proof system, and a hierarchy of complexity classes. *J. Comput. System Sci.*, 36:254–276, 1988.

[BMT] A. Bertoni, G. Mauri, and M. Torelli. Some recursively unsolvable problems relating to isolated cutpoints in probabilistic automata. In *Automata, Languages and Programming*, pages 87–94, Fourth Colloq., Univ. Turku, Turku, 1977. Lecture Notes in Computer Science, Vol. 52. Springer-Verlag, Berlin, 1977.

[BT1] V. D. Blondel and J. N. Tsitsiklis. When is a pair of matrices mortal? *Inform. Process. Lett.*, 63(5):283–286, 1997.

[BT2] V. D. Blondel and J. N. Tsitsiklis. The boundedness of all products of a pair of matrices is undecidable. *Systems Control Lett.*, 41(2):135–140, 2000.

[BT3] V. D. Blondel and J. N. Tsitsiklis. A survey of computational complexity results in systems and control. *Automatica*, 36(9):1249–1274, 2000.

[CHPW] A. Condon, L. Hellerstein, S. Pottle, and A. Wigderson. On the power of finite automata with both nondeterministic and probabilistic states. *SIAM J. Comput.*, 27(3):739–762, 1998.

[CL] A. Condon and R. J. Lipton. On the complexity of space bounded interactive proofs. In *Proceedings of the* 29*th Annual Symposium on Foundations of Computer Science*, pages 462–467, 1989.

[EKR] A. Ehrenfeucht, J. Karhumäki, and G. Rozenberg. The (generalized) Post correspondence problem with lists consisting of two words is decidable. *Theoret. Comput. Sci.*, 21(2):119–144, 1982.

[G] S. Ginsburg. *The Mathematical Theory of Context-Free Languages*, XII. McGraw-Hill, New York, 1966.

[HH] V. Halava and T. Harju. Infinite solutions of marked Post correspondence problems. In W. Brauer, H. Ehrig, J. Karhumaki, and A. Salomaa (eds.), *Formal and Natural Computing Essays Dedicated to Grzegorz Rozenberg*, pages 57–68. Lecture Notes in Computer Science, Vol. 2300. Springer-Verlag, Berlin, 2002.

[HK] T. Harju and J. Karhumäki. Morphisms. In *Handbook of Formal Languages*, Vol. 1, pages 439–510. Springer-Verlag, Berlin, 1997.

[HU] J. E. Hopcroft and J. D. Ullman. *Formal Languages and Their Relation to Automata*. Addison-Wesley, Reading, MA, 1969.

[J] G. Jacob. La finitude des représentations linéaires de semi-groupes est décidable. *J. Algebra*, 52:437–459, 1978.

[K] J. Karhumäki. Personnal communication. Email dated 8 Feb 2001.

[KR] M. Kudlek and Y. Rogozhin. New small universal circular Post machines. In R. Freivalds (ed.). *Fundamentals of Computation Theory* 13*th International Symposium*, *FCT* 2001, *Riga*, *Latvia*, *August* 22–24, 2001, pages 217–226. Lecture Notes in Computer Sciences, Vol. 2138. Springer-Verlag, Berlin, 2001.

[MHC] O. Madani, S. Hanks, and A. Condon. On the undecidability of probabilistic planning and infinite-horizon partially observable Markov decision problems. In *Proceedings of the Sixteenth National Conference on Artificial Intelligence*, pages 541–548, 1999.

[MS1] A. Mandel and I. Simon. On finite semigroups of matrices. *Theoret. Comput. Sci.*, 5:101–111, 1977.

[MS2] Y. Matiyasevich and G. Sénizergues. Decision problems for semi-Thue systems with a few rules. In *Proceedings of the* 11*th Annual IEEE Symposium on Logic in Computer Science* (*New Brunswick*, *NJ*, 1996), pages 523–531. IEEE Computer Society Press, Los Alamitos, CA, 1996.

[P1] M. S. Paterson. Unsolvability in 3 × 3 matrices. *Stud. Appl. Math.*, 49:105–107, 1970.

[P2] V. A. Pavlenko. The Post combinatorial problem for two pairs of words (in Russian). *Akad. Nauk. Ukrain. SSR Inst. Mat. Preprint*, **1982**(16), 65pp.

[P3] A. Paz. *Introduction to Probabilistic Automata*. Academic Press, New York, 1971.

[P4] E. L. Post. A variant of a recursively unsolvable problem. *Bull. Amer. Math. Soc.*, 52:264–268, 1946.

[PT] C. H. Papadimitriou and J. N. Tsitsiklis. The complexity of Markov decision processes. *Math. Oper. Res.*, 12(3):441–450, 1987.

[R1] M. O. Rabin. Probabilistic automata. *Inform. and Control*, 6:230–245, 1963.

[R2] M. O. Rabin. Lectures on classical and probabilistic automata. In E. R. Caianiello (ed.), *Automata Theory*. Academic Press, New York, 1966.

[R3] M. O. Rabin. Mathematical theory of automata *Proc. Sympos. Appl. Math.*, 19:153–175, 1967.

[R4] Y. Rogozhin. Small universal Turing machines. *Theoret. Comput. Sci.*, 168(2):215–240, 1996.

[R5] K. Ruohonen. On some variants of Post's correspondence problem. *Acta Inform.*, 19(4):357–367, 1983.

[SS] A. Salomaa and M. Soittola. *Automata-Theoretic Aspects of Formal Power Series*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1978.

[T] P. Turakainen. Generalized automata and stochastic languages. *Proc. Amer. Math. Soc.*, 21:303–309, 1969.

Received December 16, 2001, *and in final form January* 17, 2003. *Online publication March* 19, 2003.