LABORATORY FOR
COMPUTER SCIENCE

MASSACHUSETTS
INSTITUTE OF
TECHNOLOGY

MIT/LCS/TM-285

TWO UNDECIDABILITY RESULTS IN PROBABILISTIC AUTOMATA THEORY

Joseph J. Kilian

June 1985

545 TECHNOLOGY SQUARE, CAMBRIDGE, MASSACHUSETTS 02139

Two Undecidability Results in Probabilistic Automata Theory

by

Joseph J. Kilian

Submitted to the
Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements
for the degree of

BACHELOR OF SCIENCE

at the

Massachusetts Institute of Technology

June, 1985

Signature of Author .....

Department of Electrical Engineering and Computer Science, May 17, 1985

Certified by .....

Prof. Albert R. Meyer, Thesis Supervisor

Accepted by .....

Prof. David Adler, Chairman, Department Committee

Two Undecidability Results In Probabilistic Automata Theory

Abstract

The language accepted by a probabilistic finite state acceptor with an isolated cutpoint is known to be regular. We show that determining if a cutpoint is isolated is undecidable.

Keywords: Probabilistic Automaton, Probabilistic Acceptor, Post Correspondence Problem, Undecidability.

This research was supported in part by NSF Grant MCS80-10707.

Table of Contents

1 The isolated cutpoint problem.

1.1 Introduction.

Given a probabilistic finite automaton M, we define the function $v_M(w)$ as the probability that M will accept w(complete definitions are given in section 1.2 below). Rabin [R] establishes the following sufficient condition for the set of strings accepted by a probabilistic finite acceptor to be regular(this is sometimes referred to as the *isolated cutpoint theorem*).

Theorem (Rabin [R]): Given a probabilistic acceptor $A = (M, \lambda)$, the cutpoint λ is said to be *isolated* if $\exists \epsilon > 0 \forall w \in \Sigma^*, |v_M(w) - \lambda| > \epsilon$. If λ is isolated, then the language accepted by A is regular.

This result motivates the question of how one determines if a cutpoint is isolated. This question can be found in the literature[A, P], and was previously open. Our results "answer" this question by showing that no such answer exists.

We prove the following:

Theorem 1: Given a probabilistic finite automaton M, it is undecidable whether there exists a string w such that $v_M(w) = \frac{1}{2}$.

Theorem 2: Given a probabilistic finite automaton M, it is undecidable whether $\forall \epsilon > 0 \exists w$ such that $|v_M(w) - \frac{1}{2}| < \epsilon$.

Nasu and Honda [NH] showed that given a probabilistic finite automaton M, it is undecidable whether $\exists w$ such that $v_M(w) > \frac{1}{2}$. Their result and ours are incomparable in that neither result implies the other in any way obvious to us. Also, the proof techniques involved have no apparent similarity.

In the rest of this section we give a rigorous matrix formulation of probabilistic finite automata and probabilistic acceptors. We review modified Post correspondence systems, two known results concerning them, and discuss the connection between these results and the ones we wish to prove.

In section 2 we describe a mapping from modified Post correspondence systems to probabilistic finite automata. We show a trivial mapping from pairs and pair sequences

in Post correspondence systems to input words in probabilistic finite automata. We prove a lemma relating these mappings. We prove a lemma describing a relationship between solutions or approximate solutions to modified Post correspondence systems and properties of the corresponding input words to the corresponding probabilistic acceptors. This lemma is shown to imply Theorems 1 and 2 almost immediately.

In section 3 we discuss an open question arising from our work.

1.2 Matrix formulation of probabilistic finite automata.

For the rest of the paper we use the following matrix formulation. It is based on the definition used by Arbib[A], and the two can be easily shown to be equivalent. Standard notation from automata theory follows [L&P]

Let X_n be the set of nonnegative $n \times n$ matrices whose rows sum to one.
Let V_n be the set of nonnegative n component row vectors whose components sum to one.

Definition: An *n state probabilistic finite automaton* is a quadruple (F, S, δ, Σ) where Σ is the alphabet, F is a length n row vector of 0's and 1's, $S \in V_n$, and δ is a mapping from Σ to X_n.

Definition: An *n state probabilistic acceptor*, A, is an ordered pair (M, λ), where M is an n state probabilistic finite automaton, and λ is a rational number between 0 and 1. The number λ is referred to as a *cutpoint.*

Given an n state probabilistic acceptor $A = (M, \lambda)$, where $M = (F, S, \delta, \Sigma)$, define ρ_M: $\Sigma^* \rightarrow X_n$ by
1)$\rho_M(e)$ =I(the identity matrix)
2) $\rho_M(wx) = \rho_M(w) \times \delta(x)$, where $x \in \Sigma$.

We can calculate $v_M(w)$ as $S \times \rho_M(w) \times F^T$.

For w in Σ^*, A *accepts* w iff $v_M(w) > \lambda$.

In principle, λ could range the reals. From a computational view, however, but then it is not clear how to represent arbitrary cutpoints. For this reason, we restrict ourselves to the rationals.

1.3 Undecidable problems about modified Post correspondence systems.

We define modified Post correspondence systems as per Lewis and Papadimitriou [L&P]. Given some alphabet Σ, a modified Post correspondence system P is defined by an ordered pair of strings over Σ^+, (x_s, y_s), and a set of pairs $\{(x_1, y_1), (x_2, y_2), ...(x_n, y_n)\}$.

In the rest of the paper, we also use the following terminology:

Given a modified Post correspondence system P consisting of pairs $\{(x_1, y_1), (x_2, y_2), ...(x_n, y_n)\}$ over Σ^+ with a given starting pair, (x_s, y_s), a *P-sequence*, S, is defined to be a sequence of pairs, $[(x_s, y_s), (x_{i_1}, y_{i_1}), (x_{i_2}, y_{i_2}), ...(x_{i_k}, y_{i_k})]$.

S is a *match* if $x_s x_{i_1} x_{i_2} ... x_{i_k} = y_s y_{i_1} y_{i_2} ... y_{i_k}$

S *matches up to the first l letters* if $x_s x_{i_1} x_{i_2} ... x_{i_k}$ and $y_s y_{i_1} y_{i_2} ... y_{i_k}$ agree up to their first l letters.

We use the following two undecidability results concerning modified Post correspondence systems:

1) Given P, a modified Post correspondence system as defined above, determining if there exists a P-sequence S such that S is a match is r.e. complete.

2) Given P, a modified Post correspondence system as defined above, determining if $\forall l \exists S$, S is a match or matches up to the first l letters is co-r.e. complete.

These theorems remain true for any finite non-unary alphabet.

Result 1 is proven in [L&P], and the proof technique there can be used to prove result two.

We shall reduce these problems to corresponding problems about cutpoints, thereby proving Theorems 1 and 2.

2 Post Correspondence Problems Reduce to Cutpoint Problems.

2.1 Coding words into vectors and matrices.

Given a string $w \in \{a,b\}^*$, define $\nu(w)$ as .1 times the "numerical value" of w in base ten notation, interpreting a's as 1's, and b's as 2's, with the decimal point to the left of the digits. Thus, $\nu(ab) = .012$, $\nu(bababb) = .0212122$, etc. define $\nu(e) = 0$. Clearly, ν is an injective mapping.

One can easily verify the identity:

$$\nu(xy) = \nu(x) + 10^{-|x|}\nu(y). \qquad (1)$$

The following useful inequality also follows from the definition of ν:

If x and y agree up to their l^{th} letters(from the left), and differ on their $(l+1)^{th}$ letters, or exactly one of the two strings is of length l, then

$$10^{-l-1} > |\nu(x) - \nu(y)| > 10^{-l-3}. \qquad (2)$$

These bounds aren't tight, but are sufficient for our purposes.

Given $x, y \in \{a,b\}^*$, define $\tau(x,y)$ to be the length 8 row vector

$$[\frac{10^{-|x|-1}}{2}, \frac{10^{-|x|-1}}{2}, \frac{10^{-|y|-1}}{2}, \frac{10^{-|y|-1}}{2}, \nu(x), \nu(y), q, q]$$

where q is defined as the value necessary to make the components sum to 1. Note that the first 6 components of the vector are are nonnegative and bounded above by .05. This implies that q will be nonnegative and less than 1.

Define the 8×8 matrix $\Omega(x,y)$ as follows:

$$\begin{pmatrix}
\frac{10^{-|x|}}{2} & \frac{10^{-|x|}}{2} & 0 & 0 & 10\nu(x) & 0 & q_1 & q_1 \\
\frac{10^{-|x|}}{2} & \frac{10^{-|x|}}{2} & 0 & 0 & 10\nu(x) & 0 & q_2 & q_2 \\
0 & 0 & \frac{10^{-|y|}}{2} & \frac{10^{-|y|}}{2} & 0 & 10\nu(y) & q_3 & q_3 \\
0 & 0 & \frac{10^{-|y|}}{2} & \frac{10^{-|y|}}{2} & 0 & 10\nu(y) & q_4 & q_4 \\
0 & 0 & 0 & 0 & 1 & 0 & q_5 & q_5 \\
0 & 0 & 0 & 0 & 0 & 1 & q_6 & q_6 \\
0 & 0 & 0 & 0 & 0 & 0 & q_7 & q_7 \\
0 & 0 & 0 & 0 & 0 & 0 & q_8 & q_8
\end{pmatrix}$$

The q_i's are defined so as to make each row sum to 1. It is easily verified that the q_i's will be nonnegative.

2.2 A relationship between Ω and τ.

We prove the following lemma:

Lemma 0: $\tau(s,t) \times \Omega(x,y) = \tau(sx, ty)$

Proof: By definition, $\tau(s,t) \times \Omega(x,y) =$ (collecting all terms)

$$[\frac{10^{-|s|-|x|-1}}{2}, \frac{10^{-|s|-|x|-1}}{2}, \frac{10^{-|t|-|y|-1}}{2}, \frac{10^{-|t|-|y|-1}}{2}, \nu(s)+10^{-|s|}\nu(x), \nu(t)+10^{-|t|}\nu(y), q', q''].$$

Since by equation (1), $\nu(mn) = \nu(m) + 10^{-|m|}\nu(n)$, and $|mn| = |m| + |n|$, the above simplifies to

$$[\frac{10^{-|sx|-1}}{2}, \frac{10^{-|sx|-1}}{2}, \frac{10^{-|ty|-1}}{2}, \frac{10^{-|ty|-1}}{2}, \nu(sx), \nu(ty), q', q''].$$

By inspection, the first six components of this vector are the same as $\tau(sx, ty)$. In order to show that the last two components are correct, it must be shown that they are the same and that the sum of the components is 1. But $q' = q''$, since the last two columns of $\Omega(x,y)$ are identical.

Obviously, the sum of the components of $\tau(s,t) \times \Omega(x,y)$ is equal to
$(\tau(s,t) \times \Omega(x,y)) \times [1\,1\,1\,1\,1\,1\,1\,1]^T =$
$\tau(s,t) \times (\Omega(x,y) \times [1\,1\,1\,1\,1\,1\,1\,1]^T)$ =(by associativity)
$\tau(s,t) \times [1\,1\,1\,1\,1\,1\,1\,1]^T$ =(Since the rows of $\Omega(x,y)$ sum to 1)
1.(Since the components of $\tau(s,t)$ sum to 1)

Q.E.D.

2.3 Definition of reduction mapping.

We exhibit a mapping from modified post correspondence systems to probabilistic finite automata

Given a modified post correspondence system P consisting of pairs $\{(x_1,y_1),(x_2,y_2),...(x_n,y_n)\}$ over $\{a,b\}^*$ with a given starting pair, (x_s,y_s), define the probabilistic acceptor A_P as $(M_P,\frac{1}{2})$, where

$M_P = (F,S,\delta,\Sigma)$

$\Sigma = \{1,...,n\}$

$S = \tau(x_s,y_s)$

$F = [1\,0\,1\,0\,1\,0\,1\,0]$

$\delta(i) = \Omega(x_i,y_i)$

> jksct3 >

Given a modified Post correspondence system P consisting of pairs $\{(x_1,y_1),(x_2,y_2),...(x_n,y_n)\}$ over $\{a,b\}^*$ with a given starting pair, (x_s,y_s), we define the mapping Φ, from P-sequences to $\{1,...,n\}^*$, by $\Phi(S) = i_1 i_2 ... i_k$, where S is the sequence of pairs $[(x_s,y_s),(x_{i_1},y_{i_1}),(x_{i_2},y_{i_2}),...(x_{i_k},y_{i_k})]$.

This correspondence is clearly one to one between the set of modified sequences and the set of strings in $\{1,...,n\}^*$.

2.4 A property of Φ.

There is a simple but crucial relationship between S and $\Phi(S)$ as shown in the following lemma.

Lemma 1: Given a modified Post correspondence system P, and a P-sequence $S = [(x_s, y_s), (x_{i_1}, y_{i_1}), (x_{i_2}, y_{i_2}), ...(x_{i_k}, y_{i_k})]$, then

$$v_{M_P}(\Phi(S)) = \frac{1}{2} + \frac{(\nu(x_s x_{i_1} x_{i_2} ... x_{i_k}) - \nu(y_s y_{i_1} y_{i_2} ... y_{i_k}))}{2}.$$

Proof: It follows from definition of ρ_{M_P} that $\rho_{M_P}(\Phi(S)) = \tau(x_s, y_s) \times \Omega(x_{i_1}, y_{i_1}) \times \Omega(x_{i_2}, y_{i_2}) \times ...\Omega(x_{i_k}, y_{i_k})$. By repeated application of Lemma 0, this simplifies to $\tau(x_s x_{i_1} x_{i_2} ... x_{i_k}, y_s y_{i_1} y_{i_2} ... y_{i_k})$.

By the definition of τ, and simple algebra,

$\tau(x, y) \times [1\,1\,1\,1\,1\,1\,1\,1]^T = 1 = 2(\tau(x, y) \times [1\,0\,1\,0\,1\,0\,1\,0]^T) + \nu(y) - \nu(x)$

Therefore, $(\tau(x, y) \times [1\,0\,1\,0\,1\,0\,1\,0]^T) = \frac{1}{2} + \frac{(\nu(x) - \nu(y))}{2}$.

Since $v_{M_P}(\Phi(S)) = \rho_{M_P}(\Phi(S)) \times [1\,0\,1\,0\,1\,0\,1\,0]^T$ it follows that

$v_{M_P}(\Phi(S)) = \frac{1}{2} + \frac{(\nu(x_s x_{i_1} x_{i_2} ... x_{i_k}) - \nu(y_s y_{i_1} y_{i_2} ... y_{i_k}))}{2}$.

2.5 Two Undecidability Results

Using the identity proven in Lemma 1, and equation (2), we now prove two undecidability results.

Theorem 1: Given a probabilistic finite automaton M, it is r.e. complete whether $\exists w$ such that $v_M(w) = \frac{1}{2}$.

Proof: Note that this question is trivially r.e., since one can easily verify for a given M whether a given string w has this property.

Given a modified Post correspondence system P consisting of pairs $\{(x_1, y_1), (x_2, y_2), ...(x_n, y_n)\}$ over $\{a, b\}^*$ with a given starting pair, (x_s, y_s), consider its associated probabilistic finite automaton M_P as defined above.

We show there exists a P-sequence $S = [(x_s, y_s), (x_{i_1}, y_{i_1}), (x_{i_2}, y_{i_2}), ...(x_{i_k}, y_{i_k})]$ such that $x_s x_{i_1} x_{i_2} ... x_{i_k} = y_s y_{i_1} y_{i_2} ... y_{i_k}$ (i.e. S is a match) iff there exists a word w such that $v_{M_P}(w) = \frac{1}{2}$.

Thus, the r.e. complete problem 1.3.(1) reduces to the problem of whether for some w, $v_{M_P}(w) = \frac{1}{2}$, which will complete the proof.

Given some P-sequence S, $v_{M_P}(\Phi(S)) = \frac{1}{2} + \frac{(\nu(x_s x_{i_1} x_{i_2} ... x_{i_k}) - \nu(y_s y_{i_1} y_{i_2} ... y_{i_k}))}{2}$ by Lemma 1.

This will equal $\frac{1}{2}$ iff $\nu(x_s x_{i_1} x_{i_2} ... x_{i_k}) = \nu(y_s y_{i_1} y_{i_2} ... y_{i_k})$. Since ν is injective, this will be true iff $x_s x_{i_1} x_{i_2} ... x_{i_k} = y_s y_{i_1} y_{i_2} ... y_{i_k}$

Thus, if S is a match, $v_{M_P}(\Phi(S)) = \frac{1}{2}$, and if $v_{M_P}(w) = \frac{1}{2}$, $\Phi^{-1}(w)$ will be a match. Our result follows.

Q.E.D.

Theorem 2: Given a probabilistic finite automaton M, it is undecidable whether $\forall \epsilon > 0 \exists w$ such that $|v_M(w) - \frac{1}{2}| < \epsilon$.

The proof is nearly the same as with Theorem 1, and uses the same conventions.

We show that for a modified Post correspondence system P, $\forall l \exists S$, a P-sequence, such that S matches up to the first l letters iff $\forall \epsilon > 0 \exists w$ such that $|v_{M_P}(w) - \frac{1}{2}| < \epsilon$.

Thus the co-r.e. complete problem 1.3.(2) reduces to whether $\forall \epsilon > 0 \exists w$ such that $|v_{M_P}(w) - \frac{1}{2}| < \epsilon$, which will complete the proof.

Given $S = [(x_s, y_s), (x_{i_1}, y_{i_1}), (x_{i_2}, y_{i_2}), ...(x_{i_k}, y_{i_k})]$

$v_{M_P}(\Phi(S)) = \frac{1}{2} + \frac{(\nu(x_s x_{i_1} x_{i_2} ... x_{i_k}) - \nu(y_s y_{i_1} y_{i_2} ... y_{i_k}))}{2}$, so

$|v_{M_P}(\Phi(w)) - \frac{1}{2}| = |\frac{(\nu(x_s x_{i_1} x_{i_2} ... x_{i_k}) - \nu(y_s y_{i_1} y_{i_2} ... y_{i_k}))}{2}|$.

In the proof of Theorem 1 we noted that this quantity was 0 iff $x_s x_{i_1} x_{i_2} ... x_{i_k} = y_s y_{i_1} y_{i_2} ... y_{i_k}$

Otherwise, by equation (2) this quantity is bounded below by $.5 \times 10^{-l-3}$ and above by $.5 \times 10^{-l-1}$, where l is such that $x_s x_{i_1} x_{i_2} ... x_{i_k}$ and $y_s y_{i_1} y_{i_2} ... y_{i_k}$ agree up to the first l characters and don't agree on the $(l+1)^{th}$ character.

These bounds are tight enough to prove our result. If $\forall l \exists S$ such that S is a match or S matches up to the first l letters, then by the above upper bound it is clear that $\forall \epsilon > 0 \exists S$ such that $|v_{M_P}(\Phi(S)) - \frac{1}{2}| < \epsilon$.

Furthermore, if $\forall \epsilon > 0 \exists w$ such that $|v_{M_P}(w) - \frac{1}{2}| < \epsilon$, then by the above lower bound, $\forall l \exists w$ such that $\Phi^{-1}(w)$ is a match, or matches in the first l letters. The proof is now complete.

Q.E.D.

3 Conclusion and an Open Problem

Theorem 2 settles an open problem that arose in the early sixties. The question "How does one determine if a cutpoint is isolated?" was not answered because it could not be answered.

However, this paper does not completely resolve the issue. Unlike Theorem 1, which determines the exact position the problem has on the arithmetic hierarchy (Σ_1^0 complete), Theorem 2 merely determines a lower bound on the complexity of the problem.

The problem of determining if a cutpoint is isolated has been shown to be Σ_1^0 hard. It is easily seen that this problem is in Σ_2^0, since it is a statement of the form, "there exists an ϵ such that for all w... <an obviously recursive predicate>". Exactly where this problem lies on the recursive hierarchy is an open question.

Acknowledgements

I would like to thank Albert Meyer for his valuable assistance in this research, and for his equally valuable insistence that I write these results up in a coherent fashion.

References

Arbib, M. A. [1969], *Theories of Abstract Automata.* Toronto: Prentice-Hall, Inc.

Lewis, H. R. and Papadimitriou, C. H.[1981], *Elements of the Theory of Computation.* Englewood Cliffs: Prentice-Hall, Inc.

Nasu, M. and Honda, N. [1969] "Mappings induced by PGSM-mappings and some recursively unsolvable problems of finite probabilistic automata," *Information and Control* **15**, 250-273.

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

Rabin, M. O. [1963], "Probabilistic Automata," *Information and Control*, VI.