Reachability Problems for Markov Chains

S. Akshay[a], Timos Antonopoulos[b], Joël Ouaknine[b], James Worrell[b]

[a] *Department of Computer Science and Engineering, Indian Institute of Technology Bombay, India*
[b] *Department of Computer Science, University of Oxford, UK*

Abstract

We consider the following decision problem: given a finite Markov chain with distinguished source and target states, and given a rational number r, does there exist an integer n such that the probability to reach the target from the source in n steps is r? This problem, which is not known to be decidable, lies at the heart of many model checking questions on Markov chains. We provide evidence of the hardness of the problem by giving a reduction from the Skolem Problem: a number-theoretic decision problem whose decidability has been open for many decades.

1. Introduction

By now there is a large body of work on model checking Markov chains; see [3] for references. Most of this work focuses on verifying linear- and branching-time properties of trajectories, typically by solving systems of linear equations or by linear programming. An alternative approach [1, 2, 4, 5, 6] considers specifications on the state distribution of the Markov chain at each time step, e.g., whether the probability to be in a given state is always at least 1/3. With this shift in view the associated algorithmic questions become surprisingly subtle, with not even decidability assured. Strikingly the works [1, 2, 4] only present incomplete or approximate verification algorithms. Similarly, in [5, 6], the authors make additional assumptions (e.g., contraction properties, boundary assumptions) to obtain model-checking procedures.

The paper [4] highlights the following fundamental decision problem on Markov chains:

> **Markov Reachability.** Given a finite stochastic matrix M with rational entries and a rational number r, does there exist $n \in \mathbb{N}$ such that $(M^n)_{1,2} = r$?

This problem asks whether there exists n such that the probability to go from State 1 to State 2 in n steps is exactly r. This is quite different from asking for the probability to go from State 1 to State 2 in any number of steps. Whereas the latter quantity can be computed in polynomial time by solving a system of linear equations, the Markov Reachability Problem is not known even to be decidable.

In Section 3 we observe that the Markov Reachability Problem can be encoded in the model checking frameworks of [1, 2, 4]. An inequality variant of the problem, asking for n such that $(M^n)_{1,2} > r$, is essentially the threshold problem for unary probabilistic automata [9], whose decidability is also open.

The paper [4] notes the close resemblance of the Markov Reachability Problem with the Skolem Problem in number theory and raises the question of whether the latter can be reduced to the Markov Reachability Problem.

> **Skolem Problem.** Given a $k \times k$ integer matrix M, does there exist n such that $(M^n)_{1,2} = 0$?

The closely related *Positivity Problem* [8] asks whether there exists n such that $(M^n)_{1,2} > 0$.[1] There is a straightforward reduction of the Skolem Problem to the Positivity Problem (which however does not preserve the dimension of the matrices involved).

The Skolem and Positivity Problems have been the subject of much study, and their decidability has been open for several decades. Currently the Skolem Problem is only known to be decidable for matrices of dimension at most 4 (see, e.g., [7, 11]) while the Positivity Problem is known only to be decidable up to dimension 5 (cf. [8]). Moreover for matrices of dimension 6 a decision procedure for the Positivity Problem would necessarily entail significant new results in Diophantine approximation—specifically the computability of the Lagrange constants of a general class of transcendental numbers [8].

While the Markov Reachability Problem and the Skolem Problem are very similar in form, the well-behaved spectral theory of stochastic matrices might lead one to conjecture that the former is more tractable. However in this note we give a reduction of the Skolem Problem to the Markov Reachability Problem. The same reduction transforms the Positivity Problem to the inequality version of the Markov Reachability Problem. In conjunction with the above-mentioned results of [8], this entails that the computability of some of the most basic problems in probabilistic verification will require significant advances in number theory.

2. Main Result

In this section we give a polynomial-time reduction of the Skolem Problem to the Markov Reachability Problem. This is accomplished in two steps via the following intermediate problem:

[1] Strictly speaking [8] defines the Positivity Problem to be the complement of the problem stated here. Since we are interested in questions of decidability the difference is inconsequential.

Problem A. Given a $k \times k$ stochastic matrix M and column vector $\boldsymbol{y} \in \{0,1,2\}^k$, does there exist n such that $\boldsymbol{e}^T M^n \boldsymbol{y} = 1$, where $\boldsymbol{e} = (1,0,\ldots,0)^T$.

Thinking of M as the transition matrix of a Markov chain, Problem A asks if there exists n such that, starting from state 1, the state distribution $\boldsymbol{w}$ after n steps satisfies $\boldsymbol{w}^T \boldsymbol{y} = 1$.

Proposition 1. *The Skolem Problem can be reduced in polynomial time to Problem A.*

Proof. Given a $k \times k$ integer matrix $M = (m_{ij})$, we construct a stochastic $(2k+1) \times (2k+1)$ matrix $\widetilde{P}$ and a vector $\widetilde{\boldsymbol{v}} \in \{0,1,2\}^{2k+1}$, such that for all $n \in \mathbb{N}$, $(M^n)_{1,2} = 0$ if and only if $\widetilde{\boldsymbol{e}}^T \widetilde{P}^n \widetilde{\boldsymbol{v}} = 1$, where $\widetilde{\boldsymbol{e}}$ is the $(2k+1)$-dimensional coordinate vector $(1,0,\ldots,0)^T$.

Let P be a $2k \times 2k$ matrix of non-negative integers obtained by replacing each entry m_{ij} of M by the symmetric matrix $\begin{pmatrix} p_{ij} & q_{ij} \\ q_{ij} & p_{ij} \end{pmatrix}$, where $p_{ij} := \max(m_{ij}, 0)$ and $q_{ij} := \max(-m_{ij}, 0)$ satisfy $p_{ij} - q_{ij} = m_{i,j}$.

The map φ sending $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ to $a - b$ is a homomorphism from the ring of 2×2 symmetric integer matrices to $\mathbb{Z}$. By definition of P, partitioning P into 2×2 blocks and applying φ to each block one obtains M. Since matrix products can be computed block-wise and φ is a homomorphism, it follows that applying φ to each 2×2 sub-block of P^n one obtains the matrix M^n. Thus $(M^n)_{1,2} = \boldsymbol{e}^T P^n \boldsymbol{v}$, where $\boldsymbol{e} = (1,0,\ldots,0)^T$ and $\boldsymbol{v} = (0,0,1,-1,0,\ldots,0)^T$ are $2k$-dimensional vectors.

Since P is non-negative, there exists a non-negative scalar $s \in \mathbb{Q}$ such that sP is *sub-stochastic*, i.e., the sum of the entries in each row is at most one. Now define a $(2k+1)$-dimensional matrix $\widetilde{P}$ and vectors $\widetilde{\boldsymbol{e}}, \widetilde{\boldsymbol{v}}$ by

$$\widetilde{\boldsymbol{e}} = \begin{pmatrix} \boldsymbol{e} \\ 0 \end{pmatrix} \qquad \widetilde{P} = \begin{pmatrix} sP & \boldsymbol{1} - sP\boldsymbol{1} \\ 0 & 1 \end{pmatrix} \qquad \widetilde{\boldsymbol{v}} = \begin{pmatrix} \boldsymbol{v} \\ 0 \end{pmatrix} + \boldsymbol{1}\,,$$

where $\boldsymbol{1} = (1,\ldots,1)^T$ denotes a column vector of 1's of the appropriate dimension. The rightmost column of $\widetilde{P}$ is defined to make $\widetilde{P}$ a stochastic matrix.

Since $\widetilde{P}^n$ is stochastic for each $n \in \mathbb{N}$, we have that

$$\widetilde{\boldsymbol{e}}^T \widetilde{P}^n \widetilde{\boldsymbol{v}} = \widetilde{\boldsymbol{e}}^T \widetilde{P}^n \begin{pmatrix} \boldsymbol{v} \\ 0 \end{pmatrix} + \widetilde{\boldsymbol{e}}^T \widetilde{P}^n \boldsymbol{1} = \boldsymbol{e}^T (sP)^n \boldsymbol{v} + 1 = s^n (M^n)_{1,2} + 1\,.$$

From this we conclude that $(M^n)_{1,2} = 0$ iff $\widetilde{\boldsymbol{e}}^T \widetilde{P}^n \widetilde{\boldsymbol{v}} = 1$. □

The next step shows how the vector $\widetilde{\boldsymbol{v}}$ can be made into a coordinate vector.

Proposition 2. *Problem A can be reduced in polynomial time to the Markov Reachability Problem.*

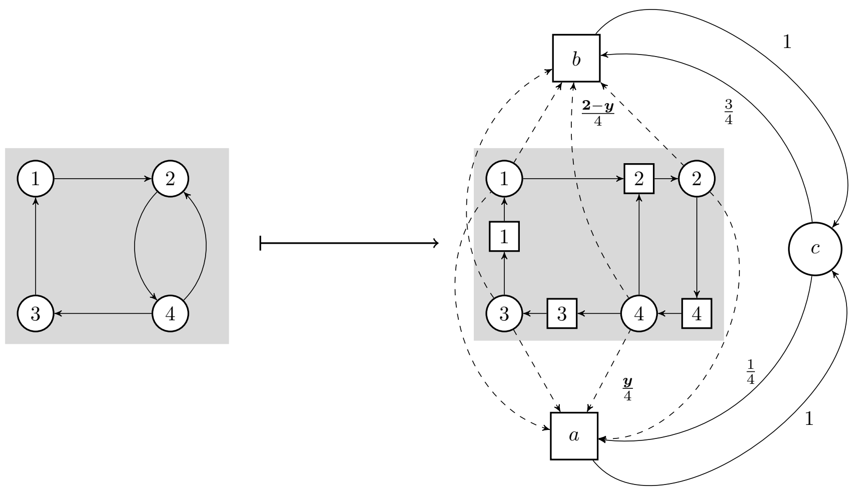

Figure 1: The chains Q and $\widetilde{Q}$.

Proof. Given k-dimensional vectors $\boldsymbol{e} = (1, 0, \ldots, 0)^T$ and $\boldsymbol{y} \in \{0, 1, 2\}^k$, and a $k \times k$ stochastic matrix Q, we construct a $2k+3$-dimensional stochastic matrix $\widetilde{Q}$ such that $\boldsymbol{e}^T Q^n \boldsymbol{y} = 1$ if and only if $(\widetilde{Q}^{2n+1})_{1,2k+1} = \frac{1}{4}$ for all $n \in \mathbb{N}$. In addition, the construction of $\widetilde{Q}$ is such that for all n, $(\widetilde{Q}^{2n})_{1,2k+1} = 0$, and thus by rearranging the rows and columns of $\widetilde{Q}$ we get an instance of the Markov Reachability Problem.

We first give an informal description of $\widetilde{Q}$, making reference to the example in Figure 1. Thinking of Q as the transition matrix of a Markov chain, the idea is that $\widetilde{Q}$ contains two copies of each state of Q (the circle and square states in Figure 1). Each transition of Q is split into a length-two path in $\widetilde{Q}$ connecting two circle states via an intermediate square state. Thus the underlying transition graph of $\widetilde{Q}$ is bipartite. We also create a new bottom strongly connected component in $\widetilde{Q}$ with three states (states a, b and c in Figure 1). The transition weights from Q are halved in $\widetilde{Q}$, with half of the mass in each transition redirected to the new bottom strongly connected component according to the final-state vector $\boldsymbol{y}$. Looking at Figure 1, the total mass entering state a from the shaded region in the $(2n+1)$-th transition step is proportional to $\boldsymbol{e}^T Q^n \boldsymbol{y}$. The new bottom strongly connected component has period 2. After an even number of steps all the mass in this component is concentrated in state c, while in the next step this mass is redistributed to states a and b in fixed proportion. The overall effect of this construction is to establish Equation (1) below.

Formally, define $\widetilde{Q}$ to be the following stochastic matrix, where $I_{k\times k}$ denotes that $k \times k$ identity matrix and $0_{k\times l}$ the $k \times l$ zero matrix.

$$\frac{1}{4} \cdot \begin{pmatrix} 0_{k\times k} & 2Q & \boldsymbol{y} & \boldsymbol{2}-\boldsymbol{y} & 0_{k\times 1} \\ 4I_{k\times k} & 0_{k\times k} & 0_{k\times 1} & 0_{k\times 1} & 0_{k\times 1} \\ 0_{1\times k} & 0_{1\times k} & 0 & 0 & 4 \\ 0_{1\times k} & 0_{1\times k} & 0 & 0 & 4 \\ 0_{1\times k} & 0_{1\times k} & 1 & 3 & 0 \end{pmatrix}$$

It is straightforward to verify by induction on $n \geq 0$ that $\widetilde{Q}^{2n+1}$ is equal to

$$\frac{1}{2^{n+2}} \begin{pmatrix} 0_{k\times k} & 2Q^{n+1} & \boldsymbol{2^n}-\boldsymbol{1}+Q^n\boldsymbol{y} & 3\cdot\boldsymbol{2^n}-\boldsymbol{1}-Q^n\boldsymbol{y} & 0_{k\times 1} \\ 4Q^n & 0_{k\times k} & 0_{k\times 1} & 0_{k\times 1} & \boldsymbol{2^{n+2}}-\boldsymbol{4} \\ 0_{1\times k} & 0_{1\times k} & 0 & 0 & 2^{n+2} \\ 0_{1\times k} & 0_{1\times k} & 0 & 0 & 2^{n+2} \\ 0_{1\times k} & 0_{1\times k} & 2^n & 3\cdot 2^n & 0 \end{pmatrix}$$

The base case is immediate. The induction step follows by routine calculations, relying on the fact that $Q\boldsymbol{1} = \boldsymbol{1}$ since Q is stochastic. We omit details.

It now follows that

$$(\widetilde{Q}^{2n+1})_{1,2k+1} = \frac{1}{2^{n+2}}(2^n - 1 + \boldsymbol{e}^T Q^n \boldsymbol{y}) \tag{1}$$

and we conclude that $\boldsymbol{e}^T Q^n \boldsymbol{y} = 1$ if and only if $(\widetilde{Q}^{2n+1})_{1,2k+1} = \frac{1}{4}$. □

Composing the two reductions in Propositions 1 and 2, we have our main result.

Theorem 3. *The Skolem Problem can be reduced in polynomial time to the Markov Reachability Problem.*

The above reduction can be applied *mutatis mutandis* to transform an instance of the Positivity Problem to an instance of the inequality version of the Markov Reachability Problem. (One applies the same transformation on matrices, just changing equalities to inequalities where necessary.)

Corollary 4. *The Positivity Problem can be reduced in polynomial time to the inequality version of the Markov Reachability Problem.*

Theorem 3 is related to the main result of Turakainen [10], which shows that for any generalized stochastic language L there is a generalized probabilistic automaton and a cut-point that accepts this language. In particular, Theorem 3 is a sharpening of [10] in the special case of languages over a unary alphabet. The result in [10] can be used to reduce the Skolem problem to the question of, given a stochastic vector $\boldsymbol{v} \in \mathbb{R}^k$ a stochastic matrix $M \in \mathbb{R}^{k\times k}$, a vector $\boldsymbol{w} \in \{0,1\}^k$ and $r \in \mathbb{R}$, whether there exists n such that $\boldsymbol{v}^T M^n \boldsymbol{w} = r$. Here we strengthen to the case that $\boldsymbol{w}$ is a coordinate vector, with most of the work being in Proposition 2.

If the scaling factor s in the definition of $\widetilde{P}$ in the proof of Proposition 1 is chosen to be a power of 2, then the above reduction will produce a stochastic matrix all of whose entries are dyadic rationals. It is not difficult to see that by padding with extra states we can arrange that the target of the reduction be a stochastic matrix with all entries either 0 or $\frac{1}{2}$.

3. Applications to Model Checking

In this section we apply Theorem 3 to show that two previously studied model checking problems on Markov chains are both at least as hard as the Skolem and Positivity problems.

3.1. PMLO

In [4], Beauquier *et al.* introduce *PMLO (probabilistic monadic logic of order)*, which extends the monadic logic of order with a probability quantifier $\mathbf{Prob}_{>q}$. PMLO formulas are evaluated over infinite runs of a finite state-labelled Markov chain. A formula $\mathbf{Prob}_{>q}(\varphi)$ is satisfied by a run ρ if the probability measure of all runs with the same initial state as ρ and which satisfy φ is at least q. We refer the reader to [4] for full details of the syntax and semantics of PMLO.

The paper [4] gives a partial decision procedure for model checking a subclass of PMLO formulas on Markov chains. The authors also propose to consider the relationship between PMLO model checking and the Skolem Problem as a subject for further research. Here we will show that model checking for a very restricted class of PMLO formulas is at least as hard as both the Skolem Problem and the Positivity Problem.

For our purposes it suffices to consider two simple formulas:

$$\exists x\ \mathbf{Prob}_{=q}(Q(x)) \ \text{ and } \ \exists x\ \mathbf{Prob}_{>q}(Q(x))\,,$$

where Q is a monadic predicate. These formulas are interpreted on a Markov chain whose states are labelled by the set of monadic predicates (such as Q above) they satisfy. The formula $\exists x\ \mathbf{Prob}_{=q}(Q(x))$ is satisfied by the Markov chain if there exists $n \in \mathbb{N}$ such that the probability to be in a Q-labelled state after n steps is exactly q. Likewise the formula $\exists x\ \mathbf{Prob}_{>q}(Q(x))$ is satisfied by the Markov chain if there exists $n \in \mathbb{N}$ such that the probability to be in a Q-labelled state after n steps is strictly greater than n. Thus the Markov Reachability Problem (both the equality and inequality versions) can easily be reduced to the model checking problem for PMLO. From Theorem 3 and Corollary 4, we conclude that:

Corollary 5. *The Skolem and Positivity Problems can be reduced to the model checking problem for PMLO on finite Markov chains.*

3.2. LTL$_{\mathcal{I}}$

In [1], the authors view a Markov chain M over nodes $\{1,\ldots,k\}$ as a linear transformer of probability distributions and define a logic interpreted over symbolic dynamics of M. This is done by discretizing the probability value space $[0,1]$ into a finite disjoint set of intervals $\mathcal{I} = \{[0,p_1),\ldots[p_m,1]\}$. Then, any distribution μ can be associated with a tuple of intervals from $\mathcal{I}$, whose i^{th} component is the interval in which the probability $\mu(i)$ falls. Thus any run, i.e., an infinite sequence of distributions over the nodes of M, induces an infinite sequence of tuples of intervals from $\mathcal{I}$, called a symbolic trajectory. The set of all such symbolic trajectories generated from an initial tuple of intervals IN defines the symbolic dynamics $L_{M,IN}$ of M.

The linear temporal logic $LTL_{\mathcal{I}}$, interpreted over symbolic trajectories, is defined over the set of atomic propositions $AP = \{\langle i, d\rangle \mid 1 \leq i \leq k, d \in \mathcal{I}\}$, where $\langle i, d\rangle$ asserts that "the current probability of node i of the Markov chain lies in the interval d". The formulas of $LTL_{\mathcal{I}}$ comprise these atomic propositions and their closure under boolean and temporal (next, until) operators. We refer the reader to [2] for the formal semantics, and the proof that $LTL_{\mathcal{I}}$ is incomparable with PMLO, as well as the usual $PCTL, PCTL^*$ logics.

The *model checking problem for* $LTL_{\mathcal{I}}$ is to determine, given M, IN and φ, if each word in the symbolic dynamics $L_{M,IN}$ is a model of φ. In [1], an approximate variant of this problem was solved but the general problem was left open. In [2] it was shown that $L_{M,IN}$ is not always regular and the authors commented that therefore the decidability of the model checking problem seems hard. We now show that this problem is as hard as the Skolem and the Positivity Problems.

Given an instance of the Markov Reachability Problem, i.e., a stochastic matrix M and $r \in \mathbb{Q} \cap [0, 1]$, we fix the discretization $\mathcal{I} = \{[0, 0], (0, r), [r, r], (r, 1), [1, 1]\}$ and consider:

$$\varphi = \Diamond\big(\langle 2, [r, r]\rangle\big) \text{ and } \psi = \Diamond\big(\langle 2, (r, 1)\rangle \vee \langle 2, [1, 1]\rangle\big).$$

Intuitively, φ (resp. ψ) expresses the property that we eventually reach a tuple of intervals D whose 2^{nd} component is the interval $[r, r]$ (resp. $(r, 1)$ or $[1, 1]$). Let $IN = \{(I_1, \ldots, I_k)\}$ where $I_1 = [1, 1]$ and $I_\ell = [0, 0]$ for all $\ell \neq 1$. Then, there exists $n \in \mathbb{N}$ such that $(M^n)_{1,2} = r$ (resp. $(M^n)_{1,2} > r$) if and only if $M, IN \models \varphi$ (resp. $M, IN \models \psi$). Thus, by Theorem 3 and Corollary 4 we have the following corollary.

Corollary 6. *The Skolem and Positivity Problems can be reduced to the model checking problem for the logic* $LTL_{\mathcal{I}}$.

References

[1] M. Agrawal, S. Akshay, B. Genest, and P. S. Thiagarajan. Approximate verification of the symbolic dynamics of Markov chains. In *LICS*, pages 55–64. IEEE Computer Society, 2012.

[2] M. Agrawal, S. Akshay, B. Genest, and P. S. Thiagarajan. Approximate verification of the symbolic dynamics of Markov chains. *Accepted to Journal of the ACM. To appear*, 2014.

[3] C. Baier and J.-P. Katoen. *Principles of model checking.* MIT Press, 2000.

[4] D. Beauquier, A. Rabinovich, and A. Slissenko. A logic of probability with decidable model checking. *J. Log. Comput.*, 16(4):461–487, 2006.

[5] V. A. Korthikanti, M. Viswanathan, G. Agha, and Y. Kwon. Reasoning about MDPs as transformers of probability distributions. In *QEST*, pages 199–208. IEEE Computer Society, 2010.

[6] Y. Kwon and G. Agha. Linear inequality LTL (iLTL): A model checker for discrete time Markov chains. In *ICFEM*, volume 3308 of *Lecture Notes in Computer Science*, pages 194–208. Springer, 2004.

[7] M. Mignotte, T. N. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik*, 349, 1984.

[8] J. Ouaknine and J. Worrell. Positivity problems for low-order linear recurrence sequences. In *SODA*, pages 366–379. IEEE, 2014.

[9] M. O. Rabin. Probabilistic automata. *Information and Control*, 6 (3):230–245, 1963.

[10] P. Turakainen. Generalized automata and stochastic languages. *Proceedings of the American Mathematical Society*, 21(2):pp. 303–309, 1969.

[11] N. K. Vereshchagin. The problem of appearance of a zero in a linear recurrence sequence (in Russian). *Mat. Zametki*, 38(2), 1985.