

# Skolem and Positivity Completeness of Ergodic Markov Chains

Mihir Vahanwala<sup>1</sup>[0009–0008–5709–899X]

MPI-SWS, Saarland Informatics Campus, Saarbrücken, Germany  
 mvahanwa@mpi-sws.org

**Abstract.** We consider the following decision problems: given a finite, rational Markov chain, source and target states, and a rational threshold, does there exist an  $n$  such that the probability of reaching the target from the source in  $n$  steps is equal to the threshold (resp. crosses the threshold)? These problems are known to be equivalent to the Skolem (resp. Positivity) problems for Linear Recurrence Sequences (LRS). These are number-theoretic problems whose decidability has been open for decades. We present a short, self-contained, and elementary reduction from LRS to Markov Chains that improves the state of the art as follows: (a) We reduce to ergodic Markov Chains, a class is widely used in Model Checking. (b) We reduce LRS to Markov Chains of significantly lower order than before. We thus get sharper hardness results for a more ubiquitous class of Markov Chains. Immediate applications include problems in modeling biological systems, and regular automata-based counting problems.

**Keywords:** Ergodic Markov Chains · Reachability · Model checking · Linear Recurrence Sequences · Skolem · Positivity

## 1 Introduction

Markov Chains are a natural mathematical framework to describe probabilistic systems, such as those arising in computational biology. There is an extensive body of work on model checking Markov Chains: see [3] for a comprehensive set of references. Most of the focus has been on the verification of linear- and branching-time properties of Markov Chains through solving systems of linear equations, or linear programs. An alternative approach [1,4,7,8] is to consider specifications on the state distribution at each time step, e.g., whether the probability of being in a given state is at least  $1/4$ . Decidability in this setting is a lot more inaccessible: [1,4] only present incomplete or approximate verification procedures, while [7,8] owe their model-checking procedures to additional mathematical assumptions. In [2], it is formally shown that verifying these specifications is tantamount to solving the Skolem/Positivity Problem for Linear Recurrence Sequences (LRS). However, the reduction therein is from LRS of order  $k$  to periodic Markov Chains of order  $2k + 4$ . However, it is the ergodic Markov Chains (irreducible and *aperiodic*) that are widely assumed in practice. **Our novelty** is a reduction from order  $k$  LRS to ergodic Markov Chains of

order  $k + 1$ . An interesting feature of our reduction is that it shows that hard instances exist for *every* stationary distribution. In doing so, the translation of number-theoretic hardness for LRS (cf. [11]) to Markov Chains also becomes much sharper.

## 2 Markov Chain Preliminaries

**Notation:** We use  $\mathbf{1}$  to denote the column vector whose entries are all 1.

**Definition 1 (Markov Chain).** A  $k$ -state Markov Chain over  $\mathbb{Q}$  is a matrix  $\mathbf{M} \in \mathbb{Q}^{k \times k}$ , such that  $m_{ij} = \mathbf{e}_i^T \mathbf{M} \mathbf{e}_j$  denotes the probability of moving from state  $j$  to state  $i$ . We have  $\mathbf{1}^T \mathbf{M} = \mathbf{1}^T$ .

**Definition 2 (Irreducible Markov Chain).** A Markov Chain is called irreducible if every state has a path to every other state.

**Definition 3 (Periodicity).** The period  $d_i$  of a state  $i$  of a Markov chain  $\mathbf{M}$  is defined as

$$\gcd\{n \geq 1 : \mathbf{e}_i^T \mathbf{M}^n \mathbf{e}_i > 0\}$$

State  $i$  is called aperiodic if  $d_i = 1$ .  $\mathbf{M}$  is said to be aperiodic iff all its states are aperiodic.

**Definition 4 (Stationary distribution).** A distribution  $\mathbf{s}$  is said to be a stationary distribution of a Markov chain  $\mathbf{M}$ , if  $\mathbf{M}\mathbf{s} = \mathbf{s}$ .

**Theorem 1 (Fundamental Theorem of (Ergodic) Markov Chains).** A Markov chain  $\mathbf{M}$  is called ergodic if it is irreducible and aperiodic. An ergodic Markov chain has a unique stationary distribution.

In the sequel, we consider the hardness of reachability problems on ergodic Markov chains. Let  $\mathbf{M}$  be an ergodic Markov chain, and let  $\mathbf{s}$  be its stationary distribution. Let  $\mathbf{S}$  denote the square matrix, each of whose columns is  $\mathbf{s}$ . By definition,  $\mathbf{M}\mathbf{S} = \mathbf{S}$ , and  $\lim_{n \rightarrow \infty} \mathbf{M}^n = \mathbf{S}$ . We can write  $\mathbf{M} = \mathbf{S} + \mathbf{D}$ , where  $\mathbf{D}\mathbf{S} = \mathbf{S}\mathbf{D} = \mathbf{O}$ . Here  $\mathbf{O}$  denotes the null matrix. Note that  $\mathbf{1}^T \mathbf{D} = \mathbf{0}^T$ . We observe, in particular, that  $\mathbf{M}^n = \mathbf{S} + \mathbf{D}^n$ .

Conversely, consider a matrix  $\mathbf{S}$  whose columns are identical probability distributions  $\mathbf{s}$  with all entries strictly positive. Let  $\mathbf{D}$  be a matrix with spectral radius less than 1, (i.e.  $\lim_{n \rightarrow \infty} \mathbf{D}^n = \mathbf{O}$ ) such that  $\mathbf{D}\mathbf{S} = \mathbf{S}\mathbf{D} = \mathbf{O}$ . Then, if the entries of  $\mathbf{M} = \mathbf{S} + \mathbf{D}$  are all non-negative, then  $\mathbf{M}$  is an ergodic Markov chain with stationary distribution  $\mathbf{s}$ .

## 3 Overview of Problems

*Problem 1 (Ergodic Markov Chain Reachability).* Given an ergodic Markov Chain  $\mathbf{M} \in \mathbb{Q}^{k \times k}$  and  $r \in \mathbb{Q}$ , the Ergodic Markov Chain Reachability problem asks whether there exists an  $n \in \mathbb{N}$  such that the probability of returning to state 1 after  $n$  steps is exactly  $r$ , i.e.  $\mathbf{e}_1^T \mathbf{M}^n \mathbf{e}_1 = r$ .

*Problem 2 (Threshold Ergodic Markov Chain Reachability).* Given an ergodic Markov Chain  $\mathbf{M} \in \mathbb{Q}^{k \times k}$  and  $r \in \mathbb{Q}$ , the Threshold Ergodic Markov Chain Reachability problem asks whether for all  $n \in \mathbb{N}$ , the probability of returning to state 1 after  $n$  steps is at least  $r$ , i.e.  $\mathbf{e}_1^T \mathbf{M}^n \mathbf{e}_1 \geq r$ .

*Problem 3 (Off-diagonal Ergodic Markov Chain Reachability).* Given an ergodic Markov Chain  $\mathbf{M} \in \mathbb{Q}^{k \times k}$  and  $r \in \mathbb{Q}$ , the Off-diagonal Ergodic Markov Chain Reachability problem asks whether there exists an  $n \in \mathbb{N}$  such that the probability of reaching state 1 from state 2 after  $n$  steps is exactly  $r$ , i.e.  $\mathbf{e}_1^T \mathbf{M}^n \mathbf{e}_2 = r$ .

*Problem 4 (Off-diagonal Threshold Ergodic Markov Chain Reachability).* Given an ergodic Markov Chain  $\mathbf{M} \in \mathbb{Q}^{k \times k}$  and  $r \in \mathbb{Q}$ , the Off-diagonal Threshold Ergodic Markov Chain Reachability problem asks whether for all  $n \in \mathbb{N}$ , the probability of reaching state 1 from state 2 after  $n$  steps is at most  $r$ , i.e.  $\mathbf{e}_1^T \mathbf{M}^n \mathbf{e}_2 \leq r$ .

Note the difference in the inequalities in the diagonal and off-diagonal cases. The diagonal and off-diagonal variants seem to have some inherent structural differences. The trivial justification for making this choice of inequalities is that regardless of choice of  $r$ , for  $n = 0$ , the probability of being in the source state is 1, and can never be less than  $r$ . Similarly, for  $n = 0$  the probability of being in a state different from the starting state is 0. On a philosophical note, the diagonal variant can be thought of as a liveness property (e.g. a fraction of the population is guaranteed to be in the desirable state we started off in), whereas the off-diagonal variant can be thought of as a safety property (e.g. at any point, the fraction of the population in an undesirable state is upper bounded). We do not have more technical insights (e.g. what if the problem were defined for  $n \geq 1$ ): if any, they are likely to be beyond the scope of the simple reduction we present here.

We observe that these problems resemble problems on Linear Recurrence Sequences.

**Definition 5 (Linear Recurrence Sequence a.k.a. LRS).** An LRS of order  $k$  over  $\mathbb{Q}$  is an infinite sequence  $\langle u_n \rangle_{n=0}^\infty$  satisfying a recurrence relation

$$u_{n+k} = \sum_{i=0}^{k-1} a_i u_{n+i}$$

for all  $n \in \mathbb{N}$ . The recurrence relation is given by the tuple  $(a_0, \dots, a_{k-1}) \in \mathbb{Q}^k$  with  $a_0 \neq 0$ . The sequence is uniquely determined by the starting values  $(u_0, \dots, u_{k-1}) \in \mathbb{Q}^k$ .

*Problem 5 (Skolem Problem for LRS).* Given an LRS  $\langle u_n \rangle_{n=0}^\infty$  (via the recurrence relation and starting values), the Skolem problem asks whether there exists an  $n \in \mathbb{N}$  such that  $u_n = 0$ .

*Problem 6 (Positivity Problem for LRS).* Given an LRS  $\langle u_n \rangle_{n=0}^\infty$  (via the recurrence relation and starting values), the Positivity problem asks whether for all  $n \in \mathbb{N}$ ,  $u_n \geq 0$ .

The Skolem Problem is known to be decidable for LRS of order up to 4, see [9,12]. Very recently, there have been conditional decidability results for LRS of order 5 [5]. The Positivity Problem is decidable up to order 5, decidability at order 6 would entail significant number-theoretic breakthroughs [11]. If we restrict ourselves to the class of *simple* LRS (no repeated characteristic roots), then Positivity is decidable up to order 9, see [10].

We are now ready to state our main results.

**Theorem 2 (Main Result).** *Problem 5 reduces to Problem 1, while Problem 6 reduces to Problem 2.*

It is well known that for any matrix  $\mathbf{M}$ ,  $\langle m_{ij}^{(n)} \rangle_{n=1}^{\infty}$ , i.e. the entries in the  $i^{\text{th}}$  row and  $j^{\text{th}}$  column in the powers of  $\mathbf{M}$  form an LRS, and that LRS are closed under pointwise addition. Thus, the converse reductions are trivial, and we have:

**Theorem 3.** *Problem 5 is equivalent to Problem 1, while Problem 6 is equivalent to Problem 2.*

The equivalences hold for the off-diagonal variants with an almost identical proof. We discuss the difference after presenting the reduction.

## 4 The Reduction

The key idea is to construct an ergodic Markov chain via the decomposition  $\mathbf{M} = \mathbf{S} + \mathbf{D}$ . Given an LRS  $\langle u_n \rangle_{n=0}^{\infty}$  of order  $k$  over  $\mathbb{Q}$ , we will choose  $\mathbf{S}, \mathbf{D} \in \mathbb{Q}^{(k+1) \times (k+1)}$ , a rational  $\eta$  and a large rational  $\rho$  in such a way that for all  $n \geq 1$ ,  $d_{11}^{(n)} = \eta u_n / \rho^n$ . Then, deciding the Skolem (resp. Positivity) problem reduces to checking whether there exists  $n$  such that  $m_{11}^{(n)} = s_{11}$  (resp. for all  $n$ ,  $m_{11}^{(n)} \geq s_{11}$ ).

We assume that none of the initial terms of the LRS are 0, and that  $u_0 > 0$ .

To begin with, we choose some arbitrary probability distribution  $\mathbf{s} = [s_0 \ s_1 \ \dots \ s_k]^T \in \mathbb{Q}^{k+1}$ , such that all the entries of  $\mathbf{s}$  are strictly positive.  $\mathbf{S}$  denotes the square matrix, each of whose columns is  $\mathbf{s}$ .

Let  $\mathbf{A} \in \mathbb{Q}^{k \times k}$  be the companion matrix of the given LRS, i.e.

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{k-1} \end{bmatrix}$$

and let  $\mathbf{u} = [u_0 \ u_1 \ \dots \ u_{k-1}]^T$ . We have that  $u_n = \mathbf{e}_1^T \mathbf{A}^n \mathbf{u}$

Now, we choose  $\eta \in \mathbb{Q}$ ,  $\eta > 0$  such that  $\eta u_0 = 1 - s_0$ . Let  $\mathbf{F} \in \mathbb{Q}^{k \times k}$  be the invertible diagonal matrix such that

$$\mathbf{F} \begin{bmatrix} 1 - s_0 \\ -s_1 \\ \vdots \\ -s_{k-1} \end{bmatrix} = \eta \mathbf{u}$$

i.e.  $\mathbf{F} = \text{diag}(1, -\eta u_1/s_1, \dots, -\eta u_{k-1}/s_{k-1})$  Observe that the top left entry in both  $\mathbf{F}$  and  $\mathbf{F}^{-1}$  is 1. Now, let  $\mathbf{B} = \mathbf{F}^{-1}\mathbf{A}\mathbf{F}$ .

Let  $\mathbf{C} \in \mathbb{Q}^{(k+1) \times (k+1)}$  be the matrix

$$\begin{bmatrix} \mathbf{B} & \mathbf{0} \\ -\mathbf{1}^T \mathbf{B} & 0 \end{bmatrix}$$

We note, by a simple induction, that for  $n \geq 1$

$$\mathbf{C}^n = \begin{bmatrix} \mathbf{B}^n & \mathbf{0} \\ -\mathbf{1}^T \mathbf{B}^n & 0 \end{bmatrix}$$

By construction  $\mathbf{1}^T \mathbf{C} = \mathbf{0}^T$ , and hence  $\mathbf{S}\mathbf{C} = \mathbf{O}$ . Let  $\mathbf{D} = \frac{1}{\rho}(\mathbf{C} - \mathbf{C}\mathbf{S})$ .  $\rho$  is chosen to be large enough to ensure that:

- The entries of  $\mathbf{S} + \mathbf{D}$  are non-negative.
- The spectral radius of  $\mathbf{D}$  is less than 1.

This makes  $\mathbf{M} = \mathbf{S} + \mathbf{D}$  an ergodic Markov chain with stationary distribution  $\mathbf{s}$ , since, indeed,  $\mathbf{D}\mathbf{S} = \mathbf{S}\mathbf{D} = \mathbf{O}$ .

We now observe that for  $n \geq 1$ ,  $\mathbf{D}^n = \frac{1}{\rho^n} \mathbf{C}^n (\mathbf{I} - \mathbf{S})$ . We see this inductively:  $(\mathbf{C} - \mathbf{C}\mathbf{S})(\mathbf{C}^n - \mathbf{C}^n \mathbf{S}) = \mathbf{C}^{n+1} - \mathbf{C}^{n+1} \mathbf{S} - \mathbf{C}\mathbf{S}\mathbf{C}^n + \mathbf{C}\mathbf{S}\mathbf{C}^n \mathbf{S} = \mathbf{C}^{n+1} - \mathbf{C}^{n+1} \mathbf{S}$ , since  $\mathbf{S}\mathbf{C} = \mathbf{O}$ .

To complete the proof, we now compute the top-left entry of  $\mathbf{D}^n$ ,  $n \geq 1$ :

$$\begin{aligned} \mathbf{e}_1^T \mathbf{D}^n \mathbf{e}_1 &= \frac{1}{\rho^n} \mathbf{e}_1^T \mathbf{C}^n (\mathbf{I} - \mathbf{S}) \mathbf{e}_1 \\ &= \frac{1}{\rho^n} \mathbf{e}_1^T \begin{bmatrix} \mathbf{B}^n & \mathbf{0} \\ -\mathbf{1}^T \mathbf{B}^n & 0 \end{bmatrix} \begin{bmatrix} 1 - s_0 \\ -s_1 \\ \vdots \\ -s_{k-1} \\ -s_k \end{bmatrix} \\ &= \frac{1}{\rho^n} \mathbf{e}_1^T \mathbf{B}^n \begin{bmatrix} 1 - s_0 \\ -s_1 \\ \vdots \\ -s_{k-1} \end{bmatrix} \quad (\text{note the change in dimension of } \mathbf{e}_1) \\ &= \frac{1}{\rho^n} (\mathbf{e}_1^T \mathbf{F}^{-1}) \mathbf{A}^n \left( \mathbf{F} \begin{bmatrix} 1 - s_0 \\ -s_1 \\ \vdots \\ -s_{k-1} \end{bmatrix} \right) \\ &= \frac{\eta}{\rho^n} \mathbf{e}_1^T \mathbf{A}^n \mathbf{u} \\ &= \frac{\eta u_n}{\rho^n} \end{aligned}$$

which is precisely a scaled version of our LRS, and we're done.

## 5 Equivalence for the off-diagonal variant

**Theorem 4.** *Problem 5 (Skolem Problem for LRS) is equivalent to Problem 3 (Off-diagonal reachability), while Problem 6 (Positivity Problem for LRS) is equivalent to Problem 4 (Off-diagonal threshold reachability).*

The proof proceeds identically, except for the choice of  $\eta$  and diagonal matrix  $\mathbf{F}$ . Here, we ensure that

$$\mathbf{F} \begin{bmatrix} -s_0 \\ 1 - s_1 \\ \vdots \\ -s_{k-1} \end{bmatrix} = \eta \mathbf{u}$$

Here, we choose  $\eta = -u_0/s_0 < 0$ , and thus  $\mathbf{F} = \text{diag}(1, \eta u_1/(1-s_1), -\eta u_2/s_2, \dots, -\eta u_{k-1}/s_{k-1})$ . In the same way as above, we get  $d_{12}^{(n)} = \frac{\eta u_n}{\rho^n}$ .

In the previous case,  $d_{11}^{(n)}$  and  $u_n$  had the same sign, however,  $d_{12}^{(n)}$  and  $u_n$  have opposite signs here. Thus, Positivity is equivalent to  $m_{12}^{(n)} \leq s_{12}$  for all  $n$ , whereas Skolem is still equivalent to  $m_{12}^{(n)} = s_{12}$  for some  $n$ .

## 6 An automata-theoretic application

We conclude with an application that reflects how far LRS and Markov Chains permeate through the field of Formal Methods. We consider the *Exponential Bound Problem* that arises in [6], in the context of decomposing automatic relations. For a regular language  $L$ , let  $L_n$  be the set of words in  $L$  of length  $n$ . The problem asks whether, given a regular language  $L$  and a bound  $b$ ,  $|L_n| \leq b^n$  for all  $n$ .

The problem relates to Linear Recurrences as follows: consider the minimal DFA  $\mathcal{A}$  that accepts  $L$ , and let  $\mathbf{M}$  be its transition matrix, i.e.  $\mathbf{M}_{i,j}$  denotes the number of transitions going from state  $q_j$  to state  $q_i$ . Let state  $q_1$  be the initial state. Then,

$$|L_n| = \left( \sum_{i: q_i \in \text{Acc}} \mathbf{e}_i \right) \mathbf{M}^n \mathbf{e}_1 \quad (1)$$

We are using powers of the transition matrix to count runs of length  $n$ , from the initial state to the final state. Such a computation also applies to weighted automata. We notice that by construction,  $\mathbf{1}^T \mathbf{M} = |\Sigma|$ , the size of the alphabet. Indeed, each state must have a total of  $|\Sigma|$  outgoing transitions. Thus,  $\mathbf{M}/|\Sigma|$  is a *stochastic* matrix.

We can thus reduce Positivity to the Exponential Bound Problem as follows: first, reduce Positivity to a rational ergodic Markov Chain. Next, scale the entries of the stochastic entries so that they are all integers. We now can interpret this as the transition matrix of a DFA with  $k+1$  states.

## References

1. Agrawal, M., Akshay, S., Genest, B., Thiagarajan, P.S.: Approximate verification of the symbolic dynamics of markov chains. *Journal of the ACM (JACM)* **62**, 1 – 34 (2015)
2. Akshay, S., Antonopoulos, T., Ouaknine, J., Worrell, J.: Reachability problems for markov chains. *Information Processing Letters* **115**(2), 155–158 (2015). <https://doi.org/https://doi.org/10.1016/j.ipl.2014.08.013>, <https://www.sciencedirect.com/science/article/pii/S0020019014001781>
3. Baier, C., Katoen, J.P.: Principles of model checking. MIT Press (2000)
4. Beauquier, D., Rabinovich, A., Slissenko, A.: A logic of probability with decidable model checking. *J. Log. Comput.* **16**, 461–487 (08 2006). <https://doi.org/10.1093/logcom/exl004>
5. Bilu, Y., Luca, F., Nieuwveld, J., Ouaknine, J., Purser, D., Worrell, J.: Skolem meets schanuel (2022)
6. Fried, D., Legay, A., Ouaknine, J., Vardi, M.Y.: Sequential relational decomposition. In: Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science. p. 432–441. LICS '18, Association for Computing Machinery, New York, NY, USA (2018). <https://doi.org/10.1145/3209108.3209203>, <https://doi.org/10.1145/3209108.3209203>
7. Korthikanti, V.A., Viswanathan, M., Agha, G., Kwon, Y.M.: Reasoning about mdps as transformers of probability distributions. In: QEST. pp. 199–208 (2010)
8. Kwon, Y., Agha, G.: Linear inequality ltl (iltl): A model checker for discrete time markov chains. In: Davies, J., Schulte, W., Barnett, M. (eds.) *Formal Methods and Software Engineering*. pp. 194–208. Springer Berlin Heidelberg (2004)
9. Mignotte, M., Shorey, T.N., Tijdeman, R.: The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik* **349**, 63–76 (1984)
10. Ouaknine, J., Worrell, J.: On the positivity problem for simple linear recurrence sequences. In: *International Colloquium on Automata, Languages, and Programming*. pp. 318–329. Springer (2014)
11. Ouaknine, J., Worrell, J.: Positivity problems for low-order linear recurrence sequences. In: *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*. pp. 366–379. SIAM (2014)
12. Vereshchagin, N.K.: The problem of appearance of a zero in a linear recurrence sequence. *Matematicheskije Zametki (in Russian)* **38**, 177–189 (1985)