A Probabilistic Logic for Verifying Continuous-time Markov Chains

Ji Guan[1] and Nengkun Yu[2](✉)

[1] State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China.
guanji1992@gmail.com
[2] Centre for Quantum Software and Information, University of Technology Sydney, Sydney, Australia.
nengkunyu@gmail.com

Abstract. A continuous-time Markov chain (CTMC) execution is a continuous class of probability distributions over states. This paper proposes a probabilistic linear-time temporal logic, namely continuous-time linear logic (CLL), to reason about the probability distribution execution of CTMCs. We define the syntax of CLL on the space of probability distributions. The syntax of CLL includes multiphase timed until formulas, and the semantics of CLL allows time reset to study relatively temporal properties. We derive a corresponding model-checking algorithm for CLL formulas. The correctness of the model-checking algorithm depends on Schanuel's conjecture, a central open problem in transcendental number theory. Furthermore, we provide a running example of CTMCs to illustrate our method.

1 Introduction

As a popular model of probabilistic continuous-time systems, *continuous-time Markov chains (CTMCs)* have been extensively studied since Kolmogorov [25]. In the recent 20 years, probabilistic continuous-time model checking receives much attention. Adopting *probabilistic computational tree logic (PCTL)* [22] to this context with extra *multiphase timed until formulas* $\Phi_1 U^{\mathcal{T}_1} \Phi_2 \cdots U^{\mathcal{T}_K} \Phi_{K+1}$, for state formula Φ and time interval $\mathcal{T}$, Aziz et al. proposed *continuous stochastic logic (CSL)* to specify the branching-time properties of CTMCs and the model-checking problem for CSL is decidable [8]. After that, efficient model-checking algorithms were developed by transient analysis of CTMCs using uniformization [9] and stratification [41] for a restricted version (path formulas are restricted to single until formulas $\Phi_1 U^{\mathcal{I}} \Phi_2$) and a full version of CSL, respectively. These algorithms have been practically implemented in model checkers PRISM [26], MRMC [24] and STORM [18]. Further details can be found in an excellent survey [23].

There are also different ways to specify the linear-time properties of CTMCs. Timed automata were first used to achieve this task [11,13,14,15,19], and then

D. Fisman and G. Rosu (Eds.): TACAS 2022, LNCS 13244, pp. 3–21, 2022.
https://doi.org/10.1007/978-3-030-99527-0_1

metric temporal logic (MTL) [12] was also considered in this context. Subsequently, the probability of "the system being in *state* s_0 within five-time units after having continuously remained in *state* s_1" can be computed. However, some statements cannot be specified and verified because of the lack of a probabilistic linear-time temporal logic, for instance "the system being in *state* s_0 with high probability (≥ 0.9) within five-time units after having continuously remained in *state* s_1 with low probability (≤ 0.1)". Furthermore, this probabilistic property cannot be expressed by CSL because CSL cannot express properties that are defined across several state transitions of the same time length in the execution of a CTMC.

In this paper, targeting to express the mentioned probabilistic linear-time properties, we introduce *continuous-time linear logic (CLL)*. In particular, we adopt the viewpoint used in [2] by regarding CTMCs as transformers of probability distributions over states. CLL studies the properties of the probability distribution execution generated by a given initial probability distribution over time. By the fundamental difference between the views of state executions and probability distribution executions of CTMCs, CLL and CSL are incomparable and complementary, as the relation between *probabilistic linear-time temporal logic (PLTL)* and PCTL in model checking discrete-time Markov chains [2, Section 3.3].

The atomic propositions of CLL are explained on the space of probability distributions over states of CTMCs. We apply the method of symbolic dynamics to the probability distributions of CTMCs. To be specific, we symbolize the probability value space $[0, 1]$ into a finite set of intervals $\mathscr{I} = \{\mathcal{I}_k \subseteq [0, 1]\}_{k=1}^{m}$. A probability distribution μ over its set of states $S = \{s_0, s_2, \ldots, s_{d-1}\}$ is then represented symbolically as a set of symbols

$$\mathbb{S}(\mu) = \{\langle s, \mathcal{I}\rangle \in S \times \mathscr{I} : \mu(s) \in \mathcal{I}\}$$

where each symbol $\langle s, \mathcal{I}\rangle$ asserts $\mu(s) \in \mathcal{I}$, i.e., the probability of state s in distribution μ falls in interval $\mathcal{I}$. For example, $\langle s_0, [0.9, 1]\rangle$ means the system is in *state* s_0 with a probability in 0.9 to 1. The symbolization idea of distributions has been considered in [2]: choosing a disjoint cover of $[0, 1]$:

$$\mathcal{I} = \{[0, p_1), [p_1, p_2), ..., [p_n, 1]\}.$$

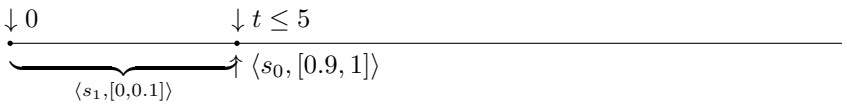
Here, we remove this restriction and enrich the expressiveness of $\mathscr{I}$. A crucial fact about this symbolization is that the set $S \times \mathscr{I}$ is finite. Consequently, the (probability distribution) execution path generated by an initial probability distribution μ induces a sequence of symbols in $S \times \mathscr{I}$ over time. Therefore, the dynamics of CTMCs can be studied in terms of a (real-time) language over the alphabet $S \times \mathscr{I}$, which is the set of atomic propositions of CLL.

Different from non-probabilistic linear-time temporal logics — *linear-time temporal logic (LTL)* and MTL, CLL has two types of formulas: state formulas and path formulas. The state formulas are constructed using propositional connectives. The path formulas are obtained by propositional connectives and a temporal modal operator *timed until* $U^{\mathcal{T}}$ for a bounded time interval $\mathcal{T}$, as in

MTL and CSL. The standard next-step temporal operator in LTL is meaningless in continuous-time systems since the time domain (real numbers) is uncountable. As a result, CLL can express the above mentioned probabilistic property "the system is at *state* s_0 with high probability (≥ 0.9) within 5 time units after having continuously remained at *state* s_1 with low probability (≤ 0.1)" in a path formula:

$$\varphi = \langle s_1, [0, 0.1]\rangle U^{[0,5]} \langle s_0, [0.9, 1]\rangle.$$

In this single until formula, there is a time instant $0 \leq t \leq 5$ at which *state* s_1 with low probability transits to *state* s_0 with high probability. Then we illustrate this on the following timeline.

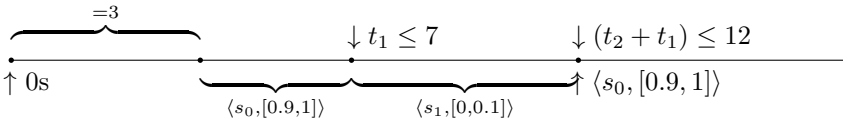


Furthermore, CLL allows *multiphase timed until formulas*. The semantics of the formulas focuses on relative time intervals, i.e., time can be reset as in timed automata [5,6], while those of CSL [8] are for absolute time intervals. Subsequently, CLL can express not only *relatively* but also *absolutely* temporal properties of CTMCs.

We illustrate the significant difference between *relatively* temporal properties and *absolutely* temporal properties of CTMCs. For instance, "before probability distributions transition φ happening in 3 to 7 time units, the system always stays at *state* s_0 with a high probability (≥ 0.9)" can be formalized in path formulae

$$\varphi' = \langle s_0, [0.9, 1]\rangle U^{[3,7]} (\langle s_1, [0, 0.1]\rangle U^{[0,5]} \langle s_0, [0.9, 1]\rangle).$$

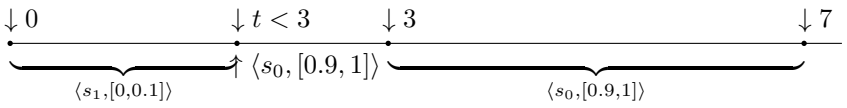
As we can see, there are two time instants, namely t_1 and t_2, happening distribution transitions. Time is reset to 0 after the first distribution transition happens and thus t_2 is relative to t_1. More clearly, we depict this on the following timeline.



An absolute version is "probability distribution transition φ happens and the system always stays at *state* s_0 with a high probability (≥ 0.9) in 3 to 7 time units"

$$\varphi'' = \Box^{[3,7]} \langle s_0, [0.9, 1]\rangle \wedge \langle s_1, [0, 0.1]\rangle U^{[0,5]} \langle s_0, [0.9, 1]\rangle).$$

We can get a clear timeline representation by simply adding $\Box^{[3,7]} \langle s_0, [0.9, 1]\rangle$ to that of φ. Assume that $t < 3$,



Time reset enriches the expressiveness of CLL but introduces more difficulties to model checking CLL than CSL. We cross this by translating relative time to the absolute one. As a result, we develop an algorithm to model check CTMCs against CLL formulas. More precisely, we reduce the model-checking problem to a reachability problem of absolute time intervals. The reachability problem corresponds to the real root isolation problem of *real polynomial-exponential functions (PEFs)* over the field of algebraic numbers, an extensively studied question in recent symbolic and algebraic computation community (e.g. [1,20,28]). By developing a state-of-the-art real root isolation algorithm, we resolve the latter problem under the assumption of the validity of Schanuel's conjecture, a central open question in transcendental number theory [27]. This conjecture has also been the footstone of the correctness of many recent model-checking algorithms, including the decidability of continuous-time Markov decision processes [30], the synthesizing inductive invariants for continuous linear dynamical systems [4], the termination analysis for probabilistic programs with delays [39], and reachability analysis for dynamical systems [20].

In summary, the main contributions of this paper are as follows.

- *Introducing a probabilistic logic*, namely continuous-time linear logic (CLL), for reasoning about CTMCs;
- *Developing* a state-of-the-art real root isolation algorithm for PEFs over the field of algebraic numbers for checking atomic propositions of CLL;
- *Proving* that model checking CTMCs against CLL formulas is decidable subject to Schanuel's conjecture.

Organization of this paper. In the next section, we give the mathematical preliminaries used in this paper. In Section 3, we recall the view of CTMCs as distribution transformers. After that, the symbolic dynamics of CTMCs are introduced by symbolizing distributions over states of CTMCs in Section 4. In the subsequent section, we present our continuous-time probabilistic temporal logic CLL. In Section 6, we develop an algorithm to solve the CLL model checking problem. A case study and related works are shown in Sections 7 and 8, respectively. We summarize our results and point out future research directions in the final section.

2 Preliminaries

For the convenience of the readers, we review basic definitions and notations of number theory, particularly Schanuel's conjecture.

Throughout this paper, we write $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ and $\mathbb{A}$ for the fields of all complex, real, rational and algebraic numbers, respectively. In addition, $\mathbb{Z}$ denotes the set of all integer numbers. For $\mathbb{F} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{A}\}$, we use $\mathbb{F}[t]$ and $\mathbb{F}^{n\times m}$ to denote the set of polynomials in t with coefficients in $\mathbb{F}$ and n-by-m matrices with every entry in $\mathbb{F}$, respectively. Furthermore, for $\mathbb{F} \in \{\mathbb{R}, \mathbb{Q}, \mathbb{Z}\}$, we use $\mathbb{F}^+$ to denote the set of positive elements (including 0) of $\mathbb{F}$.

A bounded (time) *interval* $\mathcal{T}$ is a subset of $\mathbb{R}^+$, which may be open, half-open or closed with one of the following forms:

$$[t_1, t_2], [t_1, t_2), (t_1, t_2], (t_1, t_2),$$

where $t_1, t_2 \in \mathbb{R}^+$ and $t_2 \geq t_1$ ($t_1 = t_2$ is only allowed in the case of $[t_1, t_2]$). Here, t_1 and t_2 are called the *left* and *right endpoints* of $\mathcal{T}$, respectively. Conveniently, we use $\inf \mathcal{T}$ and $\sup \mathcal{T}$ to denote t_1 and t_2, respectively. In this paper, we only consider **bounded intervals**.

For reasoning about the temporal properties, we further define the *addition* and *subtraction* of (time) intervals. The expression $\mathcal{T} + t$ or $t + \mathcal{T}$, for $t \in \mathbb{R}^+$, denotes the interval $\{t + t' : t' \in \mathcal{T}\}$. Similarly, $\mathcal{T} - t$ stands for the interval $\{-t + t' : t' \in \mathcal{T}\}$ if $t \leq \inf \mathcal{T}$. Furthermore, for two intervals $\mathcal{T}_1$ and $\mathcal{T}_2$,

$$\mathcal{T}_1 + \mathcal{T}_2 = \{t \in (t' + \mathcal{T}_2) : t' \in \mathcal{T}_1\} = \{t_1 + t_2 : t_1 \in \mathcal{T}_1 \text{ and } t_2 \in \mathcal{T}_2\}.$$

Two intervals $\mathcal{T}_1$ and $\mathcal{T}_2$ are *disjoint* if their intersection is an empty set, i.e., $\mathcal{T}_1 \cap \mathcal{T}_2 = \emptyset$. Let us see some concrete examples: $1 + (2, 3) = (3, 4)$, $(2, 3) - 1 = (1, 2)$, $(2, 3) + [3, 4] = (5, 7)$ and $(2, 3), [3, 4]$ are disjoint. It is obvious that all calculations of time intervals in the above are easy to be computed.

An *algebraic number* is a complex number that is a root of a non-zero polynomial in one variable with rational coefficients (or equivalent to integer coefficients, by eliminating denominators). An algebraic number α is represented by $(P, (a, b), \varepsilon)$ where P is the minimal polynomial of α, $a, b \in \mathbb{Q}$ and $a + bi$ is an approximation of α such that $|\alpha - (a + bi)| < \varepsilon$ and α is the only root of P in the open ball $B(a + bi, \varepsilon)$. The minimal polynomial of α is the polynomial with the smallest degree in $\mathbb{Q}[t]$ such that α is a root of the polynomial and the coefficient of the highest-degree term is 1. Any root of $f(t) \in \mathbb{A}[t]$ is algebraic. Moreover, given the representations of $a, b \in \mathbb{A}$, the representations of $a \pm b$, $\frac{a}{b}$ and $a \cdot b$ can be computed in polynomial time, so does the equality checking [17].

Furthermore, a complex number is called *transcendental* if it is not an algebraic number. In general, it is challenging to verify relationships between transcendental numbers [33]. On the other hand, one can use the Lindemann-Weierstrass theorem to compare some transcendental numbers. The transcendence of e and π are direct corollaries of this theorem.

Theorem 1 (Lindemann-Weierstrass theorem). *Let $\eta_1, \cdots, \eta_n$ be pairwise distinct algebraic complex numbers. Then $\sum_k \lambda_k e^{\eta_k} \neq 0$ for non-zero algebraic numbers $\lambda_1, \cdots, \lambda_n$.*

The following concepts are introduced to study the general relation between transcendental numbers.

Definition 1 (Algebraic independence). *A set of complex numbers $S = \{a_1, \cdots, a_n\}$ is* algebraically independent *over $\mathbb{Q}$ if the elements of S do not satisfy any nontrivial (non-constant) polynomial equation with coefficients in $\mathbb{Q}$.*

By the above definition, for any transcendental number u, $\{u\}$ is algebraically independent over $\mathbb{Q}$, while $\{a\}$ for any algebraic number $a \in \mathbb{A}$ is not. Thus, a

set of complex numbers that is algebraically independent over $\mathbb{Q}$ must consist of transcendental numbers. $\{\pi, e^{\pi\sqrt{n}}\}$ is also algebraically independent over $\mathbb{Q}$ for any positive integer n [31]. Checking the algebraic independence is challenging. For example, it is still widely open whether $\{e, \pi\}$ is algebraically independent over $\mathbb{Q}$.

Definition 2 (Extension field). *Given two fields $E \subseteq F$, F is an extension field of E, denoted by F/E, if the operations of E are those of F restricted to E.*

For example, under the usual notions of addition and multiplication, the field of complex numbers is an extension field of real numbers.

Definition 3 (Transcendence degree). *Let L be an extension field of $\mathbb{Q}$, the transcendence degree of L over $\mathbb{Q}$ is defined as the largest cardinality of an algebraically independent subset of L over $\mathbb{Q}$.*

For instance, let $\mathbb{Q}(e)/\mathbb{Q} = \{a + be \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ be two extension fields of $\mathbb{Q}$. Then the transcendence degree of them are 1 and 0, respectively, by noting that e is a transcendental number and $\sqrt{2}$ is an algebraic number.

Now, Schanuel's conjecture is ready to be presented.

Conjecture 1 (Schanuel's conjecture). Given any complex numbers $z_1, \cdots, z_n$ that are linearly independent over $\mathbb{Q}$, the extension field $\mathbb{Q}(z_1, ..., z_n, e^{z_1}, ..., e^{z_n})$ has transcendence degree of at least n over $\mathbb{Q}$.

Stephen Schanuel proposed this conjecture during a course given by Serge Lang at Columbia in the 1960s [27]. Schanuel's conjecture concerns the transcendence degree of certain field extensions of the rational numbers. The conjecture, if proven, would generalize the most well-known results in transcendental number theory significantly [29,37]. For example, the algebraical independence of $\{e, \pi\}$ would simply follow by setting $z_1 = 1$ and $z_2 = \pi i$, and using *Euler's identity* $e^{\pi i} + 1 = 0$.

3 Continuous-time Markov Chains as Distributions Transformers

We begin with the definition of *continuous-time Markov chains (CTMCs)*. A CTMC is a Markovian (memoryless) *stochastic process* that takes values on a finite state set S ($|S| = d < \infty$) and evolves in continuous-time $t \in \mathbb{R}^+$. Formally,

Definition 4. *A CTMC is a pair $\mathcal{M} = (S, Q)$, where S ($|S| = d$) is a finite state set and $Q \in \mathbb{Q}^{d \times d}$ is a* transition rate matrix.

A transition rate matrix Q is a matrix whose off-diagonal entries $\{Q_{i,j}\}_{i \neq j}$ are nonnegative rational numbers, representing the transition rate from state i to

state j, while the diagonal entries $\{Q_{j,j}\}$ are constrained to be $-\sum_{j\neq i} Q_{i,j}$ for all $1 \leq j \leq d$. Consequently, the column summations of Q are all zero.

The evolution of a CTMC can be regarded as a *distribution transformer*. Given initial distribution $\mu \in \mathbb{Q}^{d\times 1} \in \mathcal{D}(\mathcal{S})$, the distribution at time $t \in \mathbb{R}^+$ is:

$$\mu_t = e^{Qt}\mu,$$

where $\mathcal{D}(\mathcal{S})$ is denoted as the set of all probability distributions over S. We call $\mathcal{D}(\mathcal{S})$ the *probability distribution space* of CTMCs. An *execution path* of CTMCs is a continuous function indexed by initial distribution $\mu \in \mathcal{D}(\mathcal{S})$:

$$\sigma_\mu \colon \mathbb{R}^+ \to \mathcal{D}(\mathcal{S}), \qquad \sigma_\mu(t) = e^{Qt}\mu. \tag{1}$$

Example 1. We recall the illustrating example of CTMC $\mathcal{M} = (S, Q)$ in [8, Figure 1] as the running example in our work. In particular, $\mathcal{M}$ is a 5-dimensional CTMC with initial distribution μ, where $S = \{s_0, s_1, s_2, s_3, s_4\}$ and

$$Q = \begin{pmatrix} -3 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & -7 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \end{pmatrix} \qquad \mu = \begin{pmatrix} 0.1 \\ 0.2 \\ 0.3 \\ 0.4 \\ 0 \end{pmatrix}.$$

4 Symbolic Dynamics of CTMCs

In this section, we introduce symbolic dynamics to characterize the properties of the probability distribution space of CTMCs.

First, we fix a finite set of intervals $\mathscr{I} = \{\mathcal{I}_k \subseteq [0,1]\}_{k\in K}$, where the endpoints of each $\mathcal{I}_k$ are rational numbers. With the states $S = \{s_0, s_1, \cdots, s_{d-1}\}$, we define the *symbolization* of distributions as a function:

$$\mathbb{S} : \mathcal{D}(\mathcal{S}) \to 2^{S\times\mathscr{I}} \qquad \mathbb{S}(\mu) = \{\langle s, \mathcal{I}\rangle \in S \times \mathscr{I} : \mu(s) \in \mathcal{I}\}, \tag{2}$$

where $\times$ denotes the Cartesian product, and $2^{S\times\mathscr{I}}$ is the power set of $S \times \mathscr{I}$. $\langle s, \mathcal{I}\rangle \in \mathbb{S}(\mu)$ asserts that the probability of *state* s in distribution μ is in the interval $\mathcal{I}$. The *symbolization of distributions* is a generalization of the discretization of distributions with $\mathcal{I}_k \cap \mathcal{I}_m = \emptyset$ for all $k \neq m$ which was studied in [2]. This generalization increases the expressiveness of our *continuous linear-time logic* introduced in the next section. Now, we can represent any given probability distribution by finite symbols from $S \times \mathscr{I}$. For example, suppose

$$\mathscr{I} = \{[0, 0.1], (0.1, 0.9), [0.9, 1], [1, 1], [0.4, 0.4]\}, \tag{3}$$

and then the initial distribution μ in Example 1 is symbolized as

$$\begin{aligned} \mathbb{S}(\mu) = \{&\langle s_0, [0, 0.1]\rangle, \langle s_1, (0.1, 0.9)\rangle, \langle s_2, (0.1, 0.9)\rangle, \\ &\langle s_3, (0.1, 0.9)\rangle, \langle s_3, [0.4, 0.4]\rangle, \langle s_4, [0, 0.1]\rangle\}. \end{aligned} \tag{4}$$

As we can see from the above example, the symbolization of distributions on states considers the exact probabilities (singleton intervals) of the states and the range of their possibilities.

Next, we introduce the symbolization to CTMCs,

Definition 5. *A* symbolized *CTMC is a tuple* $\mathcal{SM} = (S, Q, \mathscr{I})$*, where* $\mathcal{M} = (S, Q)$ *is a CTMC and* $\mathscr{I}$ *is a finite set of intervals in* $[0, 1]$.

As we can see, the set of intervals is picked depending on CTMCs. Then, we extend this symbolization to the path σ_μ:

$$\mathbb{S} \circ \sigma_\mu : \mathbb{R}^+ \to 2^{S \times \mathscr{I}}. \tag{5}$$

Definition 6. *Given a symbolized CTMC* $\mathcal{SM} = (S, Q, \mathscr{I})$*,* $\mathbb{S} \circ \sigma_\mu$ *is a* symbolic execution path *of* $\mathcal{M} = (S, Q)$.

Given a symbolized CTMC $\mathcal{SM} = (S, Q, \mathscr{I})$, the path σ_μ of CTMC $\mathcal{M} = (S, Q)$ over real numbers $\mathbb{R}^+$ generated by probability distribution μ induces a symbolic execution path $\mathbb{S} \circ \sigma_\mu$ over finite symbols $S \times \mathscr{I}$. Subsequently, the dynamics of CTMCs can be studied in terms of a language over $S \times \mathscr{I}$. In other words, we can study the temporal properties of CTMCs in the context of symbolized CTMCs.

5 Continuous Linear-time Logic

In this section, we introduce *continuous linear-time logic (CLL)*, a probabilistic linear-time temporal logic, to specify the temporal properties of a symbolized CTMC $\mathcal{SM} = (S, Q, \mathscr{I})$.

CLL has two types of formulas: state formulas and path formulas. The state formulas are constructed using propositional connectives. The path formulas are obtained by propositional connectives and a temporal modal operator *timed until* $U^{\mathcal{T}}$ for a bounded time interval $\mathcal{T}$, as in MTL and CSL. Furthermore, *multiphase timed until formulas* $\Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2 \dots U^{\mathcal{T}_n} \Phi_n$ are allowed to enrich the expressiveness of CLL. More importantly, *time reset* is involved in these multiphase formulas. Thus absolutely and relatively temporal properties of CTMCs can be studied.

Definition 7. *The* state formulas *of CLL are described according to the following syntax:*

$$\Phi := \mathbf{true} \mid a \in AP \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2$$

where AP *denotes* $S \times \mathscr{I}$ *as the set of atomic propositions.*

The path formulas *of CLL are constructed by the following syntax:*

$$\varphi := \mathbf{true} \mid \Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2 \dots U^{\mathcal{T}_n} \Phi_n \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2$$

where $n \in \mathbb{Z}^+$ *is a positive integer, for all* $0 \leq k \leq n$*,* Φ_k *is a state formula, and* $\mathcal{T}_k$*'s are* time *intervals with the endpoints in* $\mathbb{Q}^+$*, i.e., each* $\mathcal{T}_k$ *is one of the following forms:*

$$(a, b), [a, b], (a, b], [a, b) \qquad \forall a, b \in \mathbb{Q}^+.$$

The semantics of CLL state formulas is defined on the set $\mathcal{D}(\mathcal{S})$ of probability distributions over S with the symbolized function $\mathbb{S}$ in Eq.(2) of Section 4.

(1) $\mu \models \mathbf{true}$ for all probability distributions $\mu \in \mathcal{D}(\mathcal{S})$;
(2) $\mu \models a$ iff $a \in \mathbb{S}(\mu)$;
(3) $\mu \models \neg\Phi$ iff it is not the case that $\mu \models \Phi$ (or written $\mu \not\models \Phi$);
(4) $\mu \models \Phi_1 \wedge \Phi_2$ iff $\mu \models \Phi_1$ and $\mu \models \Phi_2$.

The semantics of CLL path formulas is defined on execution paths $\{\sigma_\mu\}_{\mu\in\mathcal{D}(\mathcal{S})}$ of CTMC $\mathcal{M} = (S, Q)$.

(1) $\sigma_\mu \models \mathbf{true}$ for all probability distributions $\mu \in \mathcal{D}(\mathcal{S})$;
(2) $\sigma_\mu \models \Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2 \ldots U^{\mathcal{T}_n} \Phi_n$ iff there is a time instant $t \in \mathcal{T}_1$ such that $\sigma_{\mu_t} \models \Phi_1 U^{\mathcal{T}_2} \Phi_2 \ldots U^{\mathcal{T}_n} \Phi_n$, and for any $t' \in \mathcal{T}_1 \cap [0, t)$, $\mu_{t'} \models \Phi_0$, where $\sigma_{\mu_t} \models \Phi$ iff $\mu_t \models \Phi$, and μ_t is the distribution of the chain at time instant t, i.e., $\mu_t = e^{Qt}\mu \ \forall t \in \mathbb{R}^+$;
(3) $\sigma_\mu \models \neg\varphi$ iff it is not the case that $\sigma_\mu \models \varphi$ (written $\sigma_\mu \not\models \varphi$);
(4) $\sigma_\mu \models \varphi_1 \wedge \varphi_2$ iff $\sigma_\mu \models \varphi_1$ and $\sigma_\mu \models \varphi_2$.

Not surprisingly, other Boolean connectives are derived in the standard way, i.e., $\mathbf{false} = \neg\mathbf{true}$, $\Phi_1 \vee \Phi_2 = \neg(\neg\Phi_1 \wedge \neg\Phi_2)$ and $\Phi_1 \rightarrow \Phi_2 = \neg\Phi_1 \vee \Phi_2$, and the path formula φ follows the same way. Furthermore, we generalize temporal operators $\Diamond$ ("eventually") and $\Box$ ("always") of discrete-time systems into their timed variant $\Diamond^{\mathcal{T}}$ and $\Box^{\mathcal{T}}$, respectively, in the following:

$$\Diamond^{\mathcal{T}}\Phi = \mathbf{true} U^{\mathcal{T}} \Phi \qquad \Box^{\mathcal{T}}\Phi = \neg\Diamond^{\mathcal{T}}\neg\Phi.$$

For $n = 1$ in multiphase timed until formulas, the until operator $U^{\mathcal{T}_1}$ is a timed variant of the until operator of LTL; the path formula $\Phi_0 U^{\mathcal{T}_1} \Phi_1$ asserts that Φ_1 is satisfied at some time instant in the interval $\mathcal{T}_1$ and that at all preceding time instants in $\mathcal{T}_1$, Φ_0 holds. For example,

$$\varphi = \langle s_1, [0, 0.1]\rangle U^{[0,5]} \langle s_0, [0.9, 1]\rangle,$$

as mentioned in introduction section.

For general n, the CLL path formula $\Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2 \ldots U^{\mathcal{T}_n} \Phi_n$ is explained over the induction on n. We first mention that $U^{\mathcal{T}}$ is right-associative, e.g., $\Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2$ stands for $\Phi_0 U^{\mathcal{T}_1} (\Phi_1 U^{\mathcal{T}_2} \Phi_2)$. This makes time reset, i.e., $\mathcal{T}_1$ and $\mathcal{T}_2$ do not have to be disjoint, and the starting time point of $\mathcal{T}_2$ is based on some time instant in $\mathcal{T}_1$. Recall the multiphase timed until formula in introduction section and this formula expresses a relative time property:

$$\varphi' = \langle s_0, [0.9, 1]\rangle U^{[3,7]} (\langle s_1, [0, 0.1]\rangle U^{[0,5]} \langle s_0, [0.9, 1]\rangle),$$

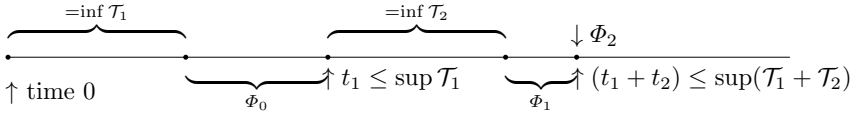
which is different to the following CLL path formula representing an absolutely temporal property of CTMCs:

$$\varphi'' = \Box^{[3,7]} \langle s_0, [0.9, 1]\rangle \wedge \langle s_1, [0, 0.1]\rangle U^{[0,5]} \langle s_0, [0.9, 1]\rangle).$$

As an example, we clarify the semantics of CLL by comparing the above two path formulas in general forms:

$$\Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2 \quad \text{and} \quad \Phi_0 U^{\mathcal{T}_1} \Phi_1 \wedge \Phi_1 U^{\mathcal{T}_2} \Phi_2.$$

(1) $\sigma_\mu \models \Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2$ asserts that there are time instants $t_1 \in \mathcal{T}_1, t_2 \in \mathcal{T}_2$ such that $\mu_{t_1+t_2} \models \Phi_2$ and for any $t_1' \in \mathcal{T}_1 \cap [0, t_1)$ and $t_2' \in \mathcal{T}_2 \cap [0, t_2)$, $\mu_{t_1'} \models \Phi_0$ and $\mu_{t_1+t_2'} \models \Phi_1$, where $\mu_t = e^{Qt}\mu \ \forall t \in \mathbb{R}^+$. This is more clear in the following timeline.



(2) $\sigma_\mu \models \Phi_0 U^{\mathcal{T}_1} \Phi_1 \wedge \Phi_1 U^{\mathcal{T}_2} \Phi_2$ asserts that there are time instants $t_1 \in \mathcal{T}_1, t_2 \in \mathcal{T}_2$ such that $\mu_{t_1} \models \Phi_1$ and $\mu_{t_2} \models \Phi_2$, and for any $t_1' \in \mathcal{T}_1 \cap [0, t_1)$ and $t_2' \in \mathcal{T}_2 \cap [0, t_2)$, $\mu_{t_1'} \models \Phi_0$ and $\mu_{t_2'} \models \Phi_1$, where $\mu_t = e^{Qt}\mu \ \forall t \in \mathbb{R}^+$.

Before solving the model-checking problem of CTMCs against CLL formulas in the next section, we shall first discuss what can be specified in our logic CLL.

Given a CTMC (S, Q), CLL path formula $\Diamond^{[0,1000]}\langle s, [1,1]\rangle$ expresses a liveness property that *state* $s \in S$ is eventually reached with probability one before time instant 1000. In terms of safety properties, formula $\Box^{[100,1000]}\langle s, [0,0]\rangle$ represents that state $s \in S$ is never reached (reached with probability zero) between time instants 100 and 1000. Furthermore, setting the intervals nontrivial (neither $[0,0]$ or $[1,1]$), liveness and safety properties can be asserted with probabilities, such as $\Diamond^{[0,1000]}\langle s, [0.5,1]\rangle$ and $\Box^{[100,1000]}\langle s, [0,0.5]\rangle$. For multiphase timed until formula $\langle s, [0.7,1]\rangle U^{[2,3]}\langle s, [0.7,1]\rangle \ldots U^{[2,3]}\langle s, [0.7,1]\rangle$, where the number of $U^{[2,3]}$ is 100, asserts that the probability of *state* s is beyond 0.7 in every time instant 2 to 3, and this happens at least 100 times.

Next, we can classify members of $\mathscr{I}$ as representing "low" and "high" probabilities. For example, if $\mathscr{I}$ contains 3 intervals $\{[0,0.1], (0.1,0.9), [0.9,1]\}$, we can declare the first interval as "low" and the last interval as "high". In this case $\Box^{[10,1000)}(\langle s_0, [0,0.1]\rangle \rightarrow \langle s_1, [0.9,1]\rangle)$ says that, in time interval $[10, 1000)$, whenever the probability of state s_0 is low, the probability of state s_1 will be high.

6 CLL Model Checking

In this section, we provide an algorithm to model check CTMCs against CLL formulas, i.e., the following CLL model-checking problem — Problem 1 is decidable.

Problem 1 (CLL Model-checking Problem). Given a symbolized CTMC $\mathcal{SM} = (S, Q, \mathscr{I})$ with an initial distribution μ and a CLL path formula φ on $AP = S \times \mathscr{I}$, the goal is to decide whether $\sigma_\mu \models \varphi$, where $\sigma_\mu(t) = e^{Qt}\mu$ is an execution path defined in Eq.(1).

In particular, we show that

Theorem 2. *Under the condition that Schanuel's conjecture holds, the CLL model-checking problem in Problem 1 is decidable.*

In the following, we prove the above theorem from checking basic formulas — atomic propositions to the most complex one — nontrivial multiphase timed until formulas. For readability, we put the proofs of all results in Appendix A of the extended version [21] of this paper.

We start with the simplest case of atomic proposition $\langle s, \mathcal{I}\rangle$. By the semantics of CLL, $\mu_t \models \langle s, \mathcal{I}\rangle$ if and only if $\mu_t = e^{Qt}\mu(s) \in \mathcal{I}$. To check this, we first observe that the execution path $e^{Qt}\mu$ of CTMCs is a system of *polynomial exponential functions (PEFs).*

Definition 8. *A function* $f : \mathbb{R} \to \mathbb{R}$ *is a* polynomial-exponential function (PEF) *if* f *has the following form:*

$$f(t) = \sum_{k=0}^{K} f_k(t) e^{\lambda_k t} \tag{6}$$

where for all $0 \leq k \leq K < \infty$, $f_k(t) \in \mathbb{F}_1[t], f_k(t) \neq 0$, $\lambda_k \in \mathbb{F}_2$ *and* $\mathbb{F}_1, \mathbb{F}_2$ *are fields. Without loss of generality, we assume that* λ_k*'s are distinct.*

Generally, for a PEF $f(t)$ with the range in complex numbers $\mathbb{C}$, $g(t) = f(t) + f^*(t)$ is a PEF with the range in real numbers $\mathbb{R}$, where $f^*(t)$ is the complex conjugate of $f(t)$. The factor t is omitted whenever convenient, i.e., $f = f(t)$. t is called a *root* of a function f if $f(t) = 0$. PEFs often appear in transcendental number theory as auxiliary functions in the proofs involving the exponential function [10].

Lemma 1. *Given a CTMC* $\mathcal{M} = (S, Q)$ *with* $S = \{s_0, \ldots, s_{d-1}\}$, $Q \in \mathbb{Q}^{d\times d}$, *and an initial distribution* $\mu \in \mathbb{Q}^{d\times 1}$, *for any* $0 \leq i \leq d-1$, $e^{Qt}\mu(s_i)$, *the* i*-th entry of* $e^{Qt}\mu$, *can be expressed as a PEF* $f : \mathbb{R}^+ \to [0, 1]$ *as in Eq.(6) with* $\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{A}$.

By the above lemma, for a given t in some bounded time interval $\mathcal{T}$ (to be specific in the latter discussion), $e^{Qt}\mu(s) \in \mathcal{I}$ is determined by the algebraic structure of PEF $g(t) = e^{Qt}\mu(s)$ in $\mathcal{T}$. That is all *maximum intervals* $\mathcal{T}_{\max} \subseteq \mathcal{T}$ such that $g(t) \in \mathcal{I}$ for all $t \in \mathcal{T}_{\max}$, where interval $\mathcal{T}_{\max} \neq \emptyset$ is called maximum for $g(t) \in \mathcal{I}$ if no sub-intervals $\mathcal{T}' \subsetneq \mathcal{T}_{\max}$ such that the property holds, i.e., $g(t) \in \mathcal{I}$ for all $t \in \mathcal{T}'$. Then $e^{Qt}\mu(s) \in \mathcal{I}$ if and only if $t \in \mathcal{T}_{\max}$ for some maximum interval $\mathcal{T}_{\max}$. So, we aim to compute the set $\mathscr{T}$ of all maximum intervals. By the continuity of PEF $g(t)$, this can be done by identifying a *real root isolation* of the following PEF $f(t)$ in $\mathcal{T}$: $f(t) = (g(t) - \inf \mathcal{I})(g(t) - \sup \mathcal{I})$.

A (real) *root isolation* of function $f(t)$ in interval $\mathcal{T}$ is a set of mutually disjoint intervals, denoted by $\mathrm{Iso}(f)_{\mathcal{T}} = \{(a_j, b_j) \subseteq \mathcal{T}\}$ for $a_j, b_j \in \mathbb{Q}$ such that

- for any j, there is one and only one root of $f(t)$ in (a_j, b_j);

– for any root t^* of $f(t)$, $t^* \in (a_j, b_j)$ for some j.

Furthermore, if f has no any root in $\mathcal{T}$, then $\text{Iso}(f)_{\mathcal{T}} = \emptyset$.

Although there are infinite kinds of real root isolations of $f(t)$ in $\mathcal{T}$, the number of isolation intervals equals to the number of distinct roots of $f(t)$ in $\mathcal{T}$.

Finding real root isolations of PEFs is a long-standing problem and can be at least backtracked to Ritt's paper [34] in 1929. Some following results were obtained since the last century (e.g. [7,38]). This problem is essential in the reachability analysis of dynamical systems, one active field of symbolic and algebraic computation. In the case of $\mathbb{F}_1 = \mathbb{Q}$ and $\mathbb{F}_2 = \mathbb{N}^+$ in [1], an algorithm named ISOL was proposed to isolate all real roots of $f(t)$. Later, this algorithm has been extended to the case of $\mathbb{F}_1 = \mathbb{Q}$ and $\mathbb{F}_2 = \mathbb{R}$ [20]. A variant of the problem has also been studied in [28]. The correctness of these algorithms is based on Schanuel's conjecture. Other works are using Schanuel's conjecture to do the root isolation of other functions, such as exp-log functions [35] and tame elementary functions [36].

By Lemma 1, we pursue this problem in the context of CTMCs. The distinct feature of solving real root isolations of PEFs in our paper is to deal with complex numbers $\mathbb{C}$, more specifically algebraic numbers $\mathbb{A}$, i.e., $\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{A}$. At the same time, to the best of our knowledge, all the previous works can only handle the case over $\mathbb{R}$. Here, we develop a state-of-the-art real root isolation algorithm for PEFs over algebraic numbers. Thus from now on, we always assume that PEFs are over $\mathbb{A}$, i.e., $\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{A}$ in Eq.(6). In this case, it is worth noting that whether a PEF has a root in a given interval, $\mathcal{T} \subseteq \mathbb{R}^+$ is decidable subject to Schanuel's Conjecture if $\mathcal{T}$ is bounded [16], which falls in the situation we consider in this paper.

Theorem 3 ([16]). *Under the condition that Schanuel's conjecture holds, there is an algorithm to check whether a PEF $f(t)$ has a root in interval $\mathcal{T}$, i.e., whether $Iso(f)_{\mathcal{T}} = \emptyset$.*

In this paper, we extend the above checking $\text{Iso}(f)_{\mathcal{T}} = \emptyset$ to computing $\text{Iso}(f)_{\mathcal{T}}$ of PEF $f(t)$.

Theorem 4. *Under the condition that Schanuel's conjecture holds, there is an algorithm to find real root isolation $Iso(f)_{\mathcal{T}}$ for any PEF $f(t)$ and interval $\mathcal{T}$. Furthermore, the number of real roots is finite, i.e., $|Iso(f)_{\mathcal{T}}| < \infty$.*

We can compute the set $\mathscr{T}$ of all maximum intervals with the above theorem to check atomic propositions. Furthermore, we can compare the values of any real roots of PEFs, which is important in model checking general multiphase timed until formulas at the end of this section.

Lemma 2. *Let $f_1(t)$ and $f_2(t)$ be two PEFs with the domains in $\mathcal{T}_1$ and $\mathcal{T}_2$, and $t_1 \in \mathcal{T}_1$ and $t_2 \in \mathcal{T}_2$ are roots of them, respectively. Under the condition that Schanuel's conjecture holds, there is an efficient way to check whether or not $t_1 - t_2 < g$ for any given rational number $g \in \mathbb{Q}$.*

For model checking general state formula Φ, we can also use real root isolation of some PEF to obtain the set of all maximum intervals $\mathcal{T}_{\max}$ such that $\mu_t \models \Phi$ for all $t \in \mathcal{T}_{\max}$. The reason is that Φ admits *conjunctive normal form* consisting of atomic propositions. See the proof of the following lemma in Appendix A of the extended version [21] of this paper for the details.

Lemma 3. *Under the condition that Schanuel's conjecture holds, given a time interval $\mathcal{T}$, the set $\mathscr{T}$ of all maximum intervals in $\mathcal{T}$ satisfying $\mu_t \models \Phi$ can be computed, where Φ is a state formula of CLL. Furthermore, the number of all intervals in $\mathscr{T}$ is finite; the left and right endpoints of each interval in $\mathscr{T}$ are roots of PEFs.*

At last, we characterize the multiphase timed until formulas by the reachability analysis of time intervals (instants).

Lemma 4. *$\sigma_\mu \models \Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2 \cdots U^{\mathcal{T}_n} \Phi_n$ if and only if there exist time intervals $\{\mathcal{I}_k \subseteq \mathbb{R}^+\}_{k=0}^n$ with $\mathcal{I}_0 = [0,0]$ such that*

- The satisfaction of intervals*: for all $1 \le k \le n$, $\mu_t \models \Phi_{k-1}$ for all $t \in \mathcal{I}_k$, and $\mu_{t^*} \models \Phi_n$, where $t^* = \sup \mathcal{I}_n$ and $\mu_t = e^{Qt}\mu$ $\forall t \in \mathbb{R}^+$;*
- The order of intervals*: for all $1 \le k \le n$, $\mathcal{I}_k \subseteq \mathcal{I}_{k-1} + \mathcal{T}_k$ and $\inf \mathcal{I}_k = \sup \mathcal{I}_{k-1} + \inf \mathcal{T}_k$.*

By the above lemma, the problem of checking multiphase timed until formulas is reduced to verify the existence of a sequence of time intervals.

Now we can show the proof of Theorem 2.

Proof. Recall that the nontrivial step is to model check multiphase timed until formula $\Phi_0 U^{\mathcal{T}_1} \Phi_1 U^{\mathcal{T}_2} \Phi_2 \cdots U^{\mathcal{T}_n} \Phi_n$, where $\{\mathcal{T}_j\}_{j=1}^n$ is a set of bounded rational intervals in $\mathbb{R}^+$, and for $0 \le k \le n+1$, Φ_k is a state formula.

By Lemma 4, for model checking the above formula, we only need to check the existence of time intervals $\{\mathcal{I}_k\}_{k=0}^n$ illustrated in the lemma. The following procedure can construct such a set of intervals if it exists:

- (1) Let $\mathscr{I}_0 = \{\mathcal{I}_0 = [0,0]\}$;
- (2) For each $1 \le k \le n$, obtaining the set $\mathscr{I}_k$ in $[0, \sum_{j=1}^k \sup \mathcal{T}_j]$ of all maximum intervals such that $\mu_t \models \Phi_{k-1}$ for all $t \in \mathcal{I}$ of $\mathcal{I} \in \mathscr{I}$, where $\mu_t = e^{Qt}\mu$; this can be done by Lemma 3. Noting that $\mathscr{I}_k$ can be the empty set, i.e., $\mathscr{I}_k = \emptyset$;
- (3) Let k from 1 to n. First, updating $\mathscr{I}_k$:

$$\mathscr{I}_k = \{\mathcal{I} \cap (\mathcal{I}' + \mathcal{T}_k) : \mathcal{I} \in \mathscr{I}_k \text{ and } \mathcal{I}' \in \mathscr{I}_{k-1}\}. \tag{7}$$

  The above updates can be finished by Lemma 2. If $\mathscr{I}_k = \emptyset$, then the formula is not satisfied;
- (4) Updating $\mathscr{I}_n$: for each $\mathcal{I} \in \mathscr{I}_n$, we replace $\mathcal{I}$ with $[s-\varepsilon, s)$ for some constant $\varepsilon > 0$ if there is an $s \in \mathcal{I}$ with $s - \varepsilon \in \mathcal{I}$ such that $\mu_s \models \Phi_n$ where $\mu_s = e^{Qs}\mu$; Otherwise, remove this element from $\mathscr{I}_n$. Again, this can be done by Lemma 3. If $\mathscr{I}_n = \emptyset$, then the formula is not satisfied;

– (5) Finally, let k from $n-1$ to 1, updating $\mathscr{I}_k$:

$$\mathscr{I}_k = \{[s - \inf \mathcal{T}_k, s - \inf \mathcal{T}_k] : [s-\varepsilon, s) \in \mathscr{I}_{k+1}]\}.$$

Thus after the above procedure, we have non-empty sets $\{\mathscr{I}_k\}_{k=0}^n$ with the following properties.

– for each $1 \leq k \leq n$, $\mu_t \models \Phi_{k-1}$ for all $t \in \mathcal{I}_k$ and $\mathcal{I}_k \in \mathscr{I}_k$, and $\mu_{t^*} \models \Phi_n$, where $t^* = \sup \mathcal{I}_n$;
– for each $1 \leq k \leq n$, $\mathcal{I} \in \mathscr{I}_k$, there exists at least one $\mathcal{I}' \in \mathscr{I}_{k-1}$ such that $\mathcal{I} \subseteq \sup \mathcal{I}' + \mathcal{T}_k$ and $\inf \mathcal{I} = \sup \mathcal{I}' + \inf \mathcal{T}_k$.

Therefore, we can get a set of intervals $\{\mathcal{I}_k\}_{k=0}^n$ satisfying the two conditions in Lemma 4 if it exists. On the other hand, it is easy to check that all such $\{\mathcal{I}_k\}_{k=0}^n$ must be in $\{\mathscr{I}_k\}_{k=0}^n$, i.e., for each k, $\mathcal{I}_k \subseteq \mathcal{I}$ for some $\mathcal{I} \in \mathscr{I}_k$. This ensures the correctness of the above procedure.

By the above constructive analysis, we give an algorithm for model checking CTMCs against CLL formulas. Focusing on the decidability problem, we do not provide the pseudocode of the algorithm. Alternatively, we implement a numerical experiment to illustrate the checking procedure in the next section.

7 Numerical Implementation

In this section, we implement a case study of checking CTMCs against CLL formulas. Here, we consider a symbolized CTMC $\mathcal{SM} = (S, Q, \mathscr{I})$, where $\mathcal{M} = (S, Q)$ is the CTMC in Example 1 and finite set $\mathscr{I}$ is the one considered in Eq.(3). We check the properties of $\mathcal{M}$ given by the following two CLL path formulas mentioned in the introduction for different initial distributions.

$$\varphi = \langle s_1, [0, 0.1]\rangle U^{[0,5]} \langle s_0, [0.9, 1]\rangle.$$
$$\varphi' = \langle s_0, [0.9, 1]\rangle U^{[3,7]} \langle s_1, [0, 0.1]\rangle U^{[0,5]} \langle s_0, [0.9, 1]\rangle.$$

By Jordan decomposition, we have $Q = SJS^{-1}$ where

$$S = \begin{pmatrix} 0 & -6 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 \\ -7 & -3 & 0 & 0 & 0 \\ 3 & 3 & 0 & 1 & 0 \\ 4 & 4 & 1 & 0 & 0 \end{pmatrix} \quad J = \begin{pmatrix} -7 & 0 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad S^{-1} = \begin{pmatrix} \frac{1}{14} & 0 & -\frac{1}{7} & 0 & 0 \\ -\frac{1}{6} & 0 & 0 & 0 & 0 \\ \frac{8}{21} & 0 & \frac{4}{7} & 0 & 1 \\ \frac{2}{7} & 0 & \frac{3}{7} & 1 & 0 \\ \frac{1}{3} & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then, we consider an initial distribution μ as the same as the one in Example 1. Then we have that the value of $e^{Qt}\mu$ is as follows:

$$\begin{pmatrix} e^{-3t} & 0 & 0 & 0 & 0 \\ -\frac{1}{3}(e^{-3t}-1) & 1 & 0 & 0 & 0 \\ \frac{1}{2}(e^{-3t}-e^{-7t}) & 0 & e^{-7t} & 0 & 0 \\ \frac{3}{14}e^{-7t} - \frac{1}{2}e^{-3t} + \frac{2}{7} & 0 & -\frac{3}{7}e^{-7t} + \frac{3}{7} & 1 & 0 \\ \frac{2}{7}e^{-7t} - \frac{2}{3}e^{-3t} + \frac{8}{21} & 0 & -\frac{4}{7}e^{-7t} + \frac{4}{7} & 0 & 1 \end{pmatrix} \begin{pmatrix} 0.1 \\ 0.2 \\ 0.3 \\ 0.4 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{10}e^{-3t} \\ -\frac{1}{30}e^{-3t} + \frac{7}{30} \\ \frac{1}{20}e^{-3t} + \frac{1}{4}e^{-7t} \\ -\frac{1}{20}e^{-3t} - \frac{3}{28}e^{-7t} + \frac{39}{70} \\ -\frac{1}{15}e^{-3t} - \frac{1}{7}e^{-7t} + \frac{22}{105} \end{pmatrix}.$$

As we only consider states s_0 and s_1 in formulas φ and φ', we focus on the following PEFs: $f_0(t) = \frac{1}{10}e^{-3t}$ and $f_1(t) = -\frac{1}{30}e^{-3t} + \frac{7}{30}$.

Next, we initialize the model checking procedures introduced in the proof of Theorem 2. First, we compute the set $\mathscr{T}$ of all maximum intervals $\mathcal{T} \subseteq [0,5]$ such that $e^{Qt}\mu \models \langle s_0, [0.9,1]\rangle$ for $t \in \mathcal{T}$, i.e., $f_0(t) \in [0.9,1]$ for $t \in \mathcal{T}$. We obtain $\mathscr{T} = \emptyset$ by the real root isolation algorithm mentioned in Theorem 4, and this indicates that $\sigma_\mu \not\models \varphi$ where $\sigma_\mu(t) = e^{Qt}\mu$ is the path induced by μ and defined in Eq.(1).

To check whether $\sigma_\mu \models \varphi'$, we compute the set $\mathscr{T}$ of all maximum intervals $\mathcal{T} \subseteq [0,12]$ such that $e^{Qt}\mu \models \langle s_0, [0.9,1]\rangle$ for $t \in \mathcal{T}$, i.e., $f_0(t) \in [0.9,1]$ for $t \in \mathcal{T}$. Again, we obtain $\mathscr{T} = \emptyset$ by the real root isolation algorithm in Theorem 4. Therefore, $\sigma_\mu \not\models \varphi'$.

In the following, we consider a different initial distribution μ_1 as follows:

$$e^{Qt}\mu_1 = e^{Qt}\begin{pmatrix}0.9\\0\\0.1\\0\\0\end{pmatrix} = \begin{pmatrix}\frac{9}{10}e^{-3t}\\ -\frac{3}{10}(e^{-3t}-1)\\ \frac{9}{20}e^{-3t} - \frac{7}{20}e^{-7t}\\ -\frac{9}{20}e^{-3t} + \frac{3}{20}e^{-7t} + \frac{3}{10}\\ -\frac{3}{5}e^{-3t} + \frac{1}{5}e^{-7t} + \frac{2}{5}\end{pmatrix}.$$

The key PEFs are: $g_0(t) = \frac{9}{10}e^{-3t}$ and $g_1(t) = -\frac{3}{10}(e^{-3t}-1)$.

Again, we initialize the model checking procedures introduced in the proof of Theorem 2. We first compute the set $\mathscr{T}$ of all maximum intervals $\mathcal{T} \subseteq [0,5]$ such that $e^{Qt}\mu_1 \models \langle s_1, [0,0.1]\rangle$ for $t \in \mathcal{T}$, i.e., $g_1(t) \in [0,0.1]$ for $t \in \mathcal{T}$. This can be done by finding a real root isolation of the following PEF: $g_1^0(t) = -\frac{3}{10}(e^{-3t} - 1) - \frac{1}{10}$.

By implementing the real root isolation algorithm in Theorem 4, we have

$$\mathrm{Iso}(g_1^0)_{[0,5]} = \{(0.13, 0.14)\} \text{ and then } \mathscr{T} = \{[0, t^*]\} \text{ for } t^* \in (0.13, 0.14).$$

Following the same way, we compute $\mathscr{T}$ for $e^{Qt}\mu_1 \models \langle s_0, [0.9,1]\rangle$. Then we complete the model checking procedures in the proof of Theorem 2, and we conclude: $\sigma_{\mu_1} \models \varphi$. By repeating these, the result of the second formula φ' is $\sigma_{\mu_1} \not\models \varphi'$.

8 Related Works

Agrawal *et al.* [2] introduced probabilistic linear-time temporal logic (PLTL) to reason about discrete-time Markov chains in the context of distribution transformers as we did for CTMCs in this paper. Interestingly, the Skolem Problem can be reduced to the model checking problem for the logic PLTL [3]. The Skolem Problem asks whether a given linear recurrence sequence has a zero term and plays a vital role in the reachability analysis of linear dynamical systems. Unfortunately, the decidability of the problem remains open [32]. Recently, the Continuous Skolem Problem has been proposed with good behavior (the problem is decidable) and forms a fundamental decision problem concerning reachability

in continuous-time linear dynamical systems [16]. Not surprisingly, the Continuous Skolem Problem can be reduced to model-checking CLL. The primary step of verifying CLL formulas is to find a real root isolation of a PEF in a given interval. Chonev, Ouaknine and Worrell reformulated the Continuous Skolem Problem in terms of whether a PEF has a root in a given interval, which is decidable subject to Schanuel's conjecture [16]. An algorithm for finding root isolation can also answer the problem of checking the existence of the roots of a PEF. However, the reverse does not work in general. Therefore, the decidability of the Continuous Skolem Problem cannot be applied to establish that of our CLL model checking.

Remark 1. By adopting the method in this paper, we established the decidability of model checking quantum CTMCs against signal temporal logic [40]. Again, we need Schanuel's conjecture to guarantee the correctness. A Lindblad's master equation governs a quantum CTMC and a more general real-time probabilistic Markov model than a CTMC, i.e., a CTMC is an instance of quantum CTMCs. We converted the evolution of Lindblad's master equation into a distribution transformer that preserves the laws of quantum mechanics. We reduced the model-checking problem of quantum CTMCs to the real root isolation problem, which we considered in this paper, and thus our method could be applied to it.

9 Conclusion

This paper revisited the study of temporal properties of finite-state CTMCs by symbolizing the probability value space $[0, 1]$ into a finite set of intervals. To specify relatively and absolutely temporal properties, we propose a probabilistic logic for CTMCs, namely continuous linear-time logic (CLL). We have considered the model checking problem in this setting. Our main result is that a state-of-the-art real root isolation algorithm over the field of algebraic numbers was proposed to establish the decidability of the model checking problem under the condition that Schanuel's conjecture holds.

This paper aims to show decidability in as simple a fashion as possible without paying much attention to complexity issues. Faster algorithms on our current constructions would significantly improve from a practical standpoint.

Acknowledgments

We want to thank Professor Joost-Pieter Katoen for his invaluable feedback and for pointing out the references [14,15,30]. This work is supported by the National Key R&D Program of China (Grant No: 2018YFA0306701), the National Natural Science Foundation of China (Grant No: 61832015), ARC Discovery Program (#DP210102449) and ARC DECRA (#DE180100156).

References

1. Achatz, M., McCallum, S., Weispfenning, V.: Deciding polynomial-exponential problems. In: Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation. pp. 215–222. ACM (2008)
2. Agrawal, M., Akshay, S., Genest, B., Thiagarajan, P.: Approximate verification of the symbolic dynamics of Markov chains. Journal of the ACM (JACM) **62**(1), 2 (2015)
3. Akshay, S., Antonopoulos, T., Ouaknine, J., Worrell, J.: Reachability problems for Markov chains. Information Processing Letters **115**(2), 155–158 (2015)
4. Almagor, S., Kelmendi, E., Ouaknine, J., Worrell, J.: Invariants for continuous linear dynamical systems. arXiv preprint arXiv:2004.11661 (2020)
5. Alur, R., Dill, D.L.: A theory of timed automata. Theoretical Computer Science **126**, 183–235 (1994)
6. Alur, R., Henzinger, T.A., Vardi, M.Y.: Parametric real-time reasoning. In: Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing. pp. 592–601 (1993)
7. Avellar, C.E., Hale, J.K.: On the zeros of exponential polynomials. Journal of Mathematical Analysis and Applications **73**(2), 434–452 (1980)
8. Aziz, A., Sanwal, K., Singhal, V., Brayton, R.: Model-checking continuous-time Markov chains. ACM Transactions on Computational Logic **1**(1), 162–170 (2000)
9. Baier, C., Haverkort, B., Hermanns, H., Katoen, J.P.: Model-checking algorithms for continuous-time Markov chains. IEEE Transactions on Software Engineering **29**(6), 524–541 (2003)
10. Baker, A.: Transcendental number theory. Cambridge university press (1990)
11. Barbot, B., Chen, T., Han, T., Katoen, J.P., Mereacre, A.: Efficient CTMC model checking of linear real-time objectives. In: International Conference on Tools and Algorithms for the Construction and Analysis of Systems. pp. 128–142. Springer (2011)
12. Chen, T., Diciolla, M., Kwiatkowska, M., Mereacre, A.: Time-bounded verification of CTMCs against real-time specifications. In: International Conference on Formal Modeling and Analysis of Timed Systems. pp. 26–42. Springer (2011)
13. Chen, T., Han, T., Katoen, J.P., Mereacre, A.: Quantitative model checking of continuous-time Markov chains against timed automata specifications. In: 2009 24th Annual IEEE Symposium on Logic In Computer Science. pp. 309–318. IEEE (2009)
14. Chen, T., Han, T., Katoen, J.P., Mereacre, A.: Model checking of continuous-time Markov chains against timed automata specifications. Logical Methods in Computer Science **7**(1) (Mar 2011)
15. Chen, T., Han, T., Katoen, J.P., Mereacre, A.: Observing continuous-time MDPs by 1-clock timed automata. In: International Workshop on Reachability Problems. pp. 2–25. Springer (2011)
16. Chonev, V., Ouaknine, J., Worrell, J.: On the skolem problem for continuous linear dynamical systems. In: Chatzigiannakis, I., Mitzenmacher, M., Rabani, Y., Sangiorgi, D. (eds.) 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016). Leibniz International Proceedings in Informatics (LIPIcs), vol. 55, pp. 100:1–100:13. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany (2016)
17. Cohen, H.: A course in computational algebraic number theory, vol. 138. Springer Science & Business Media (2013)

18. Dehnert, C., Junges, S., Katoen, J.P., Volk, M.: A STORM is coming: A modern probabilistic model checker. In: International Conference on Computer Aided Verification. pp. 592–600. Springer (2017)
19. Feng, Y., Katoen, J.P., Li, H., Xia, B., Zhan, N.: Monitoring CTMCs by multi-clock timed automata. In: International Conference on Computer Aided Verification. pp. 507–526. Springer (2018)
20. Gan, T., Chen, M., Li, Y., Xia, B., Zhan, N.: Reachability analysis for solvable dynamical systems. IEEE Transactions on Automatic Control **63**(7), 2003–2018 (2017)
21. Guan, J., Yu, N.: A probabilistic logic for verifying continuous-time markov chains. arXiv preprint arXiv:2004.08059 (2020)
22. Hansson, H., Jonsson, B.: A logic for reasoning about time and reliability. Formal Aspects of Computing **6**(5), 512–535 (1994)
23. Katoen, J.P.: The probabilistic model checking landscape. In: Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science. pp. 31–45. ACM (2016)
24. Katoen, J.P., Zapreev, I.S., Hahn, E.M., Hermanns, H., Jansen, D.N.: The ins and outs of the probabilistic model checker MRMC. Performance Evaluation **68**(2), 90–104 (2011)
25. Kolmogoroff, A.: Über die analytischen methoden in der wahrscheinlichkeitsrechnung. Mathematische Annalen **104**(1), 415–458 (1931)
26. Kwiatkowska, M., Norman, G., Parker, D.: PRISM: Probabilistic symbolic model checker. In: International Conference on Modelling Techniques and Tools for Computer Performance Evaluation. pp. 200–204. Springer (2002)
27. Lang, S.: Introduction to transcendental numbers. Addison-Wesley Pub. Co. (1966)
28. Li, J.C., Huang, C.C., Xu, M., Li, Z.B.: Positive root isolation for poly-powers. In: Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation. pp. 325–332. ACM (2016)
29. Macintyre, A., Wilkie, A.J.: On the decidability of the real exponential field (1996)
30. Majumdar, R., Salamati, M., Soudjani, S.: On decidability of time-bounded reachability in CTMDPs. In: Czumaj, A., Dawar, A., Merelli, E. (eds.) 47th International Colloquium on Automata, Languages, and Programming (ICALP 2020). Leibniz International Proceedings in Informatics (LIPIcs), vol. 168, pp. 133:1–133:19. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2020)
31. Nesterenko, Y.: Modular functions and transcendence problems. Comptes rendus de l'Académie des sciences. Série 1, Mathématique **322**(10), 909–914 (1996)
32. Ouaknine, J., Worrell, J.: Decision problems for linear recurrence sequences. In: International Workshop on Reachability Problems. pp. 21–28. Springer (2012)
33. Richardson, D.: How to recognize zero. Journal of Symbolic Computation **24**(6), 627–645 (1997)
34. Ritt, J.F.: On the zeros of exponential polynomials. Transactions of the American Mathematical Society **31**(4), 680–686 (1929)
35. Strzebonski, A.: Real root isolation for exp-log functions. In: Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation. pp. 303–314 (2008)
36. Strzebonski, A.: Real root isolation for tame elementary functions. In: Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation. pp. 341–350 (2009)
37. Terzo, G.: Some consequences of Schanuel's conjecture in exponential rings. Communications in Algebra® **36**(3), 1171–1189 (2008)

38. Tijdeman, R.: On the number of zeros of general exponential polynomials. In: Indagationes Mathematicae (Proceedings). vol. 74, pp. 1–7. North-Holland (1971)
39. Xu, M., Deng, Y.: Time-bounded termination analysis for probabilistic programs with delays. Information and Computation **275**, 104634 (2020)
40. Xu, M., Mei, J., Guan, J., Yu, N.: Model checking quantum continuous-time Markov chains. In: Haddad, S., Varacca, D. (eds.) 32nd International Conference on Concurrency Theory (CONCUR 2021). Leibniz International Proceedings in Informatics (LIPIcs), vol. 203, pp. 13:1–13:17. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2021)
41. Zhang, L., Jansen, D.N., Nielson, F., Hermanns, H.: Automata-based CSL model checking. In: International Colloquium on Automata, Languages, and Programming. pp. 271–282. Springer (2011)