Model checking conditional CSL for continuous-time Markov chains

Gao, Yang; Xu, Ming; Zhan, Naijun; Zhang, Lijun

Published in:
Information Processing Letters

Link to article, DOI:
10.1016/j.ipl.2012.09.009

Publication date:
2013

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Model checking conditional CSL for continuous-time Markov chains

Yang Gao\textsuperscript{a,1}, Ming Xu\textsuperscript{b,2}, Naijun Zhan\textsuperscript{a,1}, Lijun Zhang\textsuperscript{c,*,3}

\textsuperscript{a} State Key Lab. of Comp. Sci., Institute of Software, Chinese Academy of Sciences, China
\textsuperscript{b} Department of Computer Science and Technology, East China Normal University, China
\textsuperscript{c} Technical University of Denmark, DTU Informatics, Denmark

\textbf{A B S T R A C T}

In this paper, we consider the model-checking problem of continuous-time Markov chains (CTMCs) with respect to conditional logic. To the end, we extend Continuous Stochastic Logic introduced in Aziz et al. (2000)\cite{1} to Conditional Continuous Stochastic Logic (CCSL) by introducing a conditional probabilistic operator. CCSL allows us to express a richer class of properties for CTMCs. Based on a parameterized product obtained from the CTMC and an automaton extracted from a given CCSL formula, we propose an approximate model checking algorithm and analyse its complexity.

1. Introduction

Continuous-time Markov chains (CTMC) have received considerable attentions in network performance analysis, model checking, and system biology. In \cite{1}, Continuous Stochastic Logic (CSL) has been introduced, that has been widely used to specify properties over CTMCs.

In the paper \cite{1}, Aziz et al. focused on the decidability of the model-checking of CSL. Later, Baier et al. \cite{2} presented an \textit{approximate model checking algorithm} for the case restricted to binary until formulas. Recently, the approximate algorithm has been extended to handle nested until formulas in \cite{3}. The main idea is to exploit the notion of \textit{stratified CTMCs}, which are a subclass of CTMCs that have the nice feature allowing one to obtain the desired probability using a sequence of transient analysis. Then, the product of the CTMC and a deterministic finite automaton (DFA) obtained from the nested until formula is constructed, which is guaranteed to be stratified by construction. The product CTMC can then be analyzed efficiently, in a similar manner as the approach in \cite{2}.

In this paper, we propose the conditional continuous stochastic logic (CCSL), an extension of CSL with a conditional probabilistic operator. CCSL allows one to express a richer class of properties, such as:

\textit{The probability is at least 0.1, that the number of proteins is more than 5 and the gene becomes inactive within time interval [10, 20], under the condition that the proteins increasingly accumulated from 0 to k within the same time interval [10, 20].}

Such property can be expressed as a state formula of the form $\exists \mathcal{P}_{\geq 0.1}(\phi_{[10,20]} f \land g \mid f_1 U_{[10,20]} f_2 U_{[10,20]} \cdots f_k)$, where $f, g, f_1, \ldots, f_k$ are appropriate atomic propositions.

We believe that such conditional properties are an important extension because of the important role of conditional probabilities in stochastic models \cite{4}.

Essentially, the model checking for the conditional probabilistic operator deals with binary conjunction of CCSL path formulas, which is not allowed in the classical CSL, see \cite{1,2}. Thus, in this paper, we extend the logic CSL.
with binary conjunction and disjunction operators for the path formulas.

We discuss how to compute the probability of a conjunctive path formula, and then present an approximate model checking algorithm, following the approach in [3]. First, a DFA $A_{\psi}$ is constructed for a CCSL path formula $\psi$. The next step is to construct the DFA $A_{\psi_i}$ for the conjunction from the automata $A_{\psi_i}$. The first challenging step is to construct the product of the CTMC and the automaton $A_{\psi_i}$. A plain product construction turns out to be insufficient: We have to pay special attention to whether some conjuncts of the formula have been satisfied. We propose a notion of parameterized product construction. The probability is then computed on this product. The size of the automaton could be exponential in the number of binary operators in the path formulas, arising from the product construct, and the approximation calculation for the transient probability distributions is linear in the size of the product.

Related work. There is a rich literature on model checking techniques for CTMCs, see [1,2,5–8]. In [5,6], deterministic timed automata (DTA) are used for specifying path properties. As discussed in [9], nested until CSL path formulas can be expressed in DTA as well, however with a much larger number of states. Real-time is considered in [8], with exponential complexity both in the size of the formula and in the time bound appearing in it. In this paper, we extend CSL path formulas by allowing conjunction and disjunction, and then accordingly extend state formulas by introducing the conditional probabilistic operator.

The conditional probabilistic operator is directly inspired by the paper [10], in which the conditional probabilistic operator is introduced and analyzed for Markov decision processes (MDP). Path formulas considered there are restricted binary path operators, and the challenge for MDPs is to study the scheduler class guaranteeing the extreme (maximal or minimal) probabilities.

2. Preliminaries

In this section, we define some basic notions that will be used later. For details please refer to [2]. For convenience, we fix a set of propositions AP in the sequel, ranged by $f_1, f_2, g_1, g_2, \ldots$.

Definition 1. A labeled continuous-time Markov chain (CTMC) is a tuple $C = (S, R, L, \alpha)$ where $S$ is a finite set of states, $\alpha : S \to [0, 1]$ is the initial distribution satisfying $\sum_{s \in S} \alpha(s) = 1$, $R : S \times S \to \mathbb{R}_{\geq 0}$ is a rate matrix, and $L : S \to 2^{\text{AP}}$ is a labeling function.

For $A \subseteq S$, define $R(s, A) := \sum_{s' \in A} R(s, s')$. We denote the exit rate of state $s$ by $E(s) := R(s, S)$. A state $s$ is called absorbing if $E(s) = 0$. If $R(s, s') > 0$, we say that there is a transition from $s$ to $s'$.

Consider the CTMC in Fig. 1. If $s_1$ is the current state of the CTMC, the probability that some transition will be triggered within time $t$ is $1 - e^{-2t}$. Furthermore, there is a competition between the transitions to $s_2$ and $s_3$: the probability to take the transition to $s_2$ is $R(s_1, s_2) \cdot (1 - e^{-2t})$. The labeling function $L$ assigns to each state $s$ a set of atomic propositions $L(s) \subseteq \text{AP}$ which are valid in $s$.

Fig. 1. $C = (S, R, L, \alpha)$.

Transient probability. Starting with distribution $\alpha$ of $C$, the transient probability vector at time $t$, denoted by $\pi^c(\alpha, t)$, is the probability distribution over states at time $t$. If $t = 0$, we have $\pi^c(\alpha, 0)(s') = \alpha(s')$. For $t > 0$, the transient probability [11] is given by: $\pi^c(\alpha, t) = \pi^c(\alpha, 0)e^{Qt}$ where $Q := R - \text{diag}(E)$ is the generator matrix and $\text{diag}(E)$ denotes the diagonal matrix with $E$.

Paths and probabilistic measures. A right continuous step function $\rho : \mathbb{R}_{\geq 0} \to S$ is called a step function (or an infinite (sample) path), where $\rho(t)$ stands for the state at $t$. For a given step function $\rho$ and $i \in \mathbb{N}$, we denote by $\rho[i] = s_i$ the state at the $(i+1)$-th step, and by $\rho[I]$ the time spent at $\rho[i]$, i.e., the length of the step segment starting with $\rho[i]$. Let $P_C$ denote the set of all infinite paths, and $\text{Path}_C(s)$ denote the subset of those paths starting from $s$.

Let $I_0, \ldots, I_{k−1}$ be nonempty intervals in $\mathbb{R}_{\geq 0}$. The cylinder set $\text{Cyl}(s_0, I_0, s_1, I_1, \ldots, s_{k−1}, I_{k−1}, s_k)$ is defined by:

$$\{\rho \in \text{Path}_C \mid \forall 0 \leq i \leq k. \rho[i] = s_i \land 0 \leq i < k. \rho[I] \subseteq I_1\}.$$  

Let $F(\text{Path}_C)$ denote the smallest $\sigma$-algebra on $\text{Path}_C$ containing all cylinder sets. For initial distribution $\alpha : S \to [0, 1]$, a probability measure (denoted $\text{Pr}_{C}^\alpha$) on this $\sigma$-algebra is introduced as follows: $\text{Pr}_{C}^\alpha$ is the unique measure that satisfies: $\text{Pr}_{C}^\alpha(\text{Cyl}(s))$ equals $\alpha(s)$, and for $k > 0$, $\text{Pr}_{C}^\alpha(\text{Cyl}(s_0, I_0, \ldots, s_{k−1}))$ equals

$$\text{Pr}_{C}^\alpha(\text{Cyl}(s_0, I_0, \ldots, s_{k−1})). \frac{R(s_{k−1}, s_k)}{E(s_{k−1})}. \eta(I_{k−1}),$$

where $\eta(I_{k−1}) := e^{-E(s_{k−1})\inf I_{k−1}} - e^{-E(s_{k−1})\sup I_{k−1}}$ is the probability to take a transition during $I_{k−1}$. If $\alpha(s) = 1$ for some state $s \in S$, we sometimes simply write $\text{Pr}_{C}^\alpha$ instead of $\text{Pr}_{C}^\alpha$. We omit the superscript $C$ if it is clear from the context.

3. Conditional continuous stochastic logic (CCSL)

This section is devoted to introducing a conditional continuous stochastic logic (CCSL) by extending the Continuous Stochastic Logic (CSL) introduced by Aziz et al. [1] with a conditional probabilistic operator. Let $I_1$ be a nonempty left-closed and right-open interval on $\mathbb{R}_{\geq 0}$. Let $\alpha(\cdot) \in \{<, \leq, >, >\}, 0 < p \leq 1$, and $K > 1$. The syntax of CCSL is defined as:
$\Phi := f \mid \neg \Phi \mid \Phi \land \Phi \mid \mathcal{P}_{\text{sp}}(\varphi) \mid \mathcal{P}_{\text{op}}(\varphi \mid \varphi)$;

$\varphi := \varphi \land \varphi \mid \varphi \lor \varphi \mid \Phi_1 \ U_1, \Phi_2 \ U_2, \ldots \Phi_K$

where $f \in \mathcal{A}P$ is an atomic proposition. The syntax of CCSL consists of state formulas and path formulas. We use $\Phi, \Psi$ and their indexed versions for state formulas. The path formula $\Phi_1 \ U_1, \Phi_2 \ U_2, \ldots \Phi_K$ with $K > 1$ is referred to as the atomic path formula. Obviously, each path formula can be expressed into a disjunctive normal form (DNF) $\varphi = \bigvee_i \bigwedge_j \psi_i^j$ where $\psi_i^j$ are atomic path formulas. We use $\psi$ for atomic path formulas and $\Phi$ for general path formulas in DNF.

Let $C = (S, R, I, \alpha)$ be a CTMC with $s \in S$. The semantics of CCSL state formulas is standard: $s \models \text{true}$ for all $s \in S$, $s \models a$ iff $a \in L(s)$, $s \models \neg \Phi$ iff $s \not\models \Phi$, $s \models \Phi \land \Psi$ iff $s \models \Phi$ and $s \models \Psi$. For probabilistic formulas, we have:

$s \models \mathcal{P}_{\text{sp}}(\varphi)$ iff $\Pr_s(\{ \rho \in \text{Path} \mid \rho \models \varphi \}) = \rho$.

$s \models \mathcal{P}_{\text{op}}(\varphi_1 \mid \varphi_2)$ iff $\Pr_s(\{ \rho \in \text{Path} \mid \rho \models \varphi_1 \land \varphi_2 \}) = \rho$.

where $\Pr_s(\{ \rho \in \text{Path} \mid \rho \models \varphi \})$, or $\Pr_s(\varphi)$ for short, denotes the probability measure of the set of all paths which start from $s$ and satisfy $\varphi$. Similarly, $\Pr_s(\varphi_1 \mid \varphi_2)$ denotes the conditional probability $\frac{\Pr_s(\{ \rho \in \text{Path} \mid \rho \models \varphi \})}{\Pr_s(\{ \rho \in \text{Path} \mid \rho \models \varphi_2 \})}$ under the premise $\Pr_s(\varphi_2) \neq 0$.

The semantics for the Boolean operators is standard, and the semantics of the atomic path formula is given by [1,3]:

$\rho \models \varphi = \Phi_1 \ U_1, \Phi_2 \ U_2, \ldots \Phi_K$ iff there exist real numbers $0 \leq t_1 \leq t_2 \leq \ldots \leq t_{K-1}$ such that $\rho(t_{K-1}) = \Phi_K$, and for each integer $0 < i < K$ we have $(t_i, t_{i+1}) \cap (\forall t' \in [t_{i+1}, t_i), \rho(t') \models \Phi_i)$, where $t_0$ is defined to be 0 for notational convenience.

4. Model checking algorithm for CCSL

In this section, we present an algorithm for checking CCSL properties. We first recall the deterministic finite automaton (DFA) construction for the atomic path formula $\psi$. Then, we extend the construction to the conjunctive path formula by introducing the notion of a parameterized product construction for the given CTMC and the conjunctive path formula. This is the key for computing the probability of the set of paths satisfying the conjunctive path formula. We further show how to compute the probabilities of general path formulas. Finally, we describe an algorithm for model checking CCSL and analyze its complexity.

In the rest of the paper, let $\psi_i = f_1 \ U_1, f_2 \ U_2, \ldots f_k$ with $i = 1, \ldots, n$ be $n$ special atomic path formulas. For simplicity, as in [3,9] we assume that 1) $a_k^i \leq a_k^j$ and $b_k^i \leq b_k^j$ for any two intervals $f_k^i = [a_k^i, b_k^i]$ and $f_k^j = [a_k^j, b_k^j]$ with $k < i$; ii) all $f_k^i \in \mathcal{A}P$ are pairwise distinct for $i = 1, \ldots, n$ and $k = 1, \ldots, K$. We will drop the superscript in case $n = 1$.

4.1. Formula automata

In this subsection, we recall how to construct a deterministic finite automaton (DFA) for $\bigwedge_{i=1}^n \psi_i$. Firstly, we consider the simple case when $n = 1$. So, the atomic path formula $\psi_1$ describes the required order of $f_1^1, \ldots, f_k^1$-states.

Definition 2 (Atomic path formula automaton). (See [3]) The atomic path formula automaton $A_\psi = (\Sigma, q_0, q_s, \delta, F)$ is defined as follows:

- $\Sigma = 2\{f_1, \ldots, f_k\}$.
- $Q = \{q_1, \ldots, q_k, \bot\}$ with $q_0 = q_1$ and $F = \{q_1, \ldots, q_k\}$.
- For every $a \in \Sigma$, the transition relation $\delta$ is given by $\delta(q_k, a) = q_k$, $\delta(\bot, a) = \bot$, and for the rest $q_i \in Q \setminus \{q_k, \bot\}$.

Both $q_k$ and $\bot$ are absorbing states, i.e., with only transitions leading to themselves. The former state is referred to a good absorbing state, the latter a bad absorbing state.

The words accepted by $A_\psi$ are finite traces $w \in \Sigma^*$, such that they can be extended to a trace $w w' \in \Sigma^{\omega}$ that satisfies the time-abstract (LTL) formula of the form $f_1 \ U (f_2 \ U \cdots (f_{k-1} \ U f_k) \cdots)$.

Transitions in $A_\psi$ go always from lower goal states to higher goal states. The good state $q_k$ implies that any path traversing $q_k$ satisfies the atomic path formula $\psi$ under suitable timing constraint; while the bad state $\bot$ implies that any path traversing $\bot$ refutes the atomic path formula $\psi$.

Below we define the automaton for the conjunction of several atomic path formulas, which is essentially the product construction.

Definition 3 (Conjunctive path formula automaton). Let $\varphi = \bigwedge_{i=1}^n \psi_i$ and $A_\psi_i = (\Sigma, q_{i,0}, q_{i,s}, \delta_i, F_i)$ be the formula automaton for $\psi_i$ respectively for $i = 1, \ldots, n$. Then the conjunctive path formula automaton $A_\psi = (\Sigma, q_0, q_s, \delta, F)$ is defined as follows:

- $\Sigma = 2\bigwedge_{i=1}^n \{f_1^i, \ldots, f_k^i\}$.
- $Q = Q_1 \times \cdots \times Q^n$ with $q_{i,0} = (q_{1,i}^1, \ldots, q_{n,i}^n)$, and $F = F_1 \times \cdots \times F^n$.
- $\delta((q_{1,i}^1, \ldots, q_{n,i}^n), a) = (\delta^1(q_{1,i}^1, a^1), \ldots, \delta^n(q_{n,i}^n, a^n))$, where $a^i$ is the projection of $a$ onto $\Sigma^i$.

The state $(q_{1,i}^1, \ldots, q_{n,i}^n)$ is good if all elements $q_{k,i}^i$ are good; it is bad if at least one component $q_{k,i}^i$ is bad. Both good and bad states are absorbing.
4.2. Product construction

We have defined the conjunctive path formula automaton. Following the approach in [3], the next step would be to construct the product of the CTMC and the automaton. This step turns out to be more involved. Thus we first start with an example illustrating that the plain product does not work:

Example 2. Consider the CTMC in Fig. 1, and the conjunction $\psi^1 \land \psi^2$ with two atomic path formulas $\psi^1 = f_1 \cup f_2$ and $\psi^2 = g_1 \cup g_2$ (see Fig. 2). The initial state is $(q_1^1, q_1^2)$, final states are marked with a double circle. The transition labels indicate which subsets of $AP$ are acceptable. For example, we have $\delta((q_1^1, q_1^2), (f_2, g_1)) = (q_2^1, q_2^2)$, and $(q_2^1, q_2^2)$ is good. The node labeled with $\bot$ represents five bad absorbing states $(\bot, q_1^1), (\bot, q_2^2), (q_1^1, \bot), (q_2^2, \bot)$ and $(\bot, \bot)$. Transitions out of these two kinds of absorbing states are omitted.

In the product, each state is of the form $S_q = (\hat{S}, q)$ and its reachable part is $\hat{S} = S \times \{q\}$, where $S$ is the set of paths from the initial state $q_0$. The rate function $\hat{\mu}(\hat{S}, q)$ is defined in two steps:

1. For $i = 1, \ldots, n$, add the label $(f_i)^T$ to the state $(s, q)$ with $q_i = q_{k_i}$.
2. The labeling function $\hat{L}(s, q)$ is defined by:

   - $\hat{L}(s, q) = \emptyset$ if $s = (f_1, \ldots, f_n)$ and $\psi^i \in \Lambda$;
   - $\hat{L}(s, q) = q_{k_i}$ if $s = (f_1, \ldots, f_n)$ and $\psi^i \notin \Lambda$;
   - $\hat{L}(s, q) = \emptyset$ otherwise.

All other elements of $\hat{\mu}$ are zero.

In the product, each state is of the form $(s, (\ldots, q_{k_i}, \ldots))$, in which $q_{k_i}$ from the path formula automaton of $\psi_i$ is relevant to the atomic propositions in $\psi^i$ that $s$ satisfies. The parameter $\Lambda$ is a set of path formulas $\psi^i$. If a transition in the product leads to a state $s'$ which satisfies $f_{k_i}$ and $\Lambda$ contains $\psi^i$, the corresponding component of the state should be marked with the good absorbing state $q_{k_i}$ of $A_{\psi^i}$, i.e., $(s', (\ldots, q_{k_i}, \ldots))$. In what follows, we will show that the set $\Lambda$ plays an important role in keeping track of the path formulas which have been satisfied during the probability computation.

Example 3. The product $C_{\psi^1 \land \psi^2}$ is shown in Fig. 1. Since both $\psi^1$ and $\psi^2$ can be satisfied during $[2, 3]$ intervals, we need to construct $C_{\psi^1 \land \psi^2}$. Its reachable part is shown in Fig. 4. Note that the previous state $(s_1, q_2^1, q_3^1)$ is now renamed to $(s_1, q_2^1, q_3^2)$ according to the initial distribution. It is easy to
see that the path \( \rho = s_0, t_0, s_1, t_1, s_2, t_2, s_4, \ldots \), which was recognized as a bad path in Example 2, is captured by the new parameterized product CTMC during [2, 3] (assuming timing constraints are satisfied).

### 4.3. Probability computation

As in [3,9], the product CTMC stratifies the original CTMC in the sense that (time-abstract) bad paths will be uniformly directed towards the bad states. This allows us to reduce the computation by standard transient probability computation for CTMCs, which will be discussed in this section.

We fix a conjunctive path formula \( \psi = \bigwedge_{i=1}^{n} \psi^{i} \) together with a CTMC \( C = (S, R, \alpha, \psi) \). Now we focus on how to compute the probability of such a path formula starting from an arbitrary initial distribution \( \alpha \) in a forward way.

We first introduce some notation for convenience:

- For an interval \( I \) and a positive number \( h \), let \( I \uplus h \) denote the set \( \{ t - h | t \in I \cup \Lambda \geq h \} \), and let \( \psi \uplus h \) denote the formula \( f_1 U_{t \uplus h} f_2 U_{t \uplus h} \cdots f_K \).
- For \( 1 \leq i \leq j \leq K \), define \( f_{i \ldots j} := \bigvee_{k=i}^{j} f_k \).
- For \( 1 \leq i < K \), define \( f^{(i)} := f_{i+1} U_{t} f_{i+2} U_{t} \cdots f_{K} \).
- For a state formula \( \Phi \), let \( C(\Phi) \) be derived from \( C \) by making its states that satisfy \( \Phi \) absorbing.

**Definition 5 (Indicator matrix).** Given a state formula \( \Phi \) and a subset \( A \) of \( \{ \psi^i | i = 1, \ldots, n \} \), the indicator matrix \( I^\Phi_A \) is defined by:

- If \( (s, (q_{k_1}^1, \ldots, q_{k_l}^n)) \models \Phi \),
  \[ I^\Phi_A((s, (q_{k_1}^1, \ldots, q_{k_l}^n))) = 1, \]
- where \( q_{k_i}^i \) is \( q_{k_i}^i \), if \( \psi^i \in A \); \( q_{k_i}^i \) otherwise.
- All other entries of \( I^\Phi_A \) are zero.

Now we show how to compute the probability \( Pr^C_{\alpha}(\bigwedge_{i=1}^{n} \psi^i) \) in a forward way.

**Theorem 1 (Probability computation).** Given a conjunctive path formula \( \psi = \bigwedge_{i=1}^{n} \psi^i \) and a CTMC \( C = (S, R, \alpha, \psi) \) equipped with the following notations:

- Let \( h \) be the least nonzero endpoint of all intervals \( I^1_k \) occurring in \( \psi \), and let \( \Lambda \) be the set \( \{ \psi^i | h > a_{k_i}^i \} \).
- If \( h < \max_{i=1}^{n} b_{k_i}^i \), let \( h' \) be the least endpoint of all intervals \( I^1_k \) greater than \( h \), and let \( \Lambda' \) be the set \( \{ \psi^i | h' > a_{k_i}^i \} \).

- For \( i = 1, \ldots, n \), let \( a_{0}^i = 0 \), \( b_{0}^i = a_{1}^i \), \( a_{k_i}^i = b_{k_i}^i - 1 \), \( b_{k_i}^i = \infty \) and \( f^i_{k_i} = f^i_{k_i} \), and let \( k_i, h \) be the unique indices such that \( b_{k_i}^i - 1 \leq h < b_{k_i}^i \) and \( a_{k_i}^i - 1 < h < a_{k_i}^i \).

The probability \( Pr^C_{\alpha}(\psi) = Pr^C_{\alpha}(\psi^i) \) is computed as follows:

1. If \( h < \max_{i=1}^{n} b_{k_i}^i \), then
   \[
   Pr^C_{\alpha}(\psi) = \prod_{i=1}^{n} Pr^C_{\alpha}(\psi^i) \cdot \prod_{i=1}^{n} f^i_{k_i} (\Lambda' \cup 1, h),
   \] (1)
   where \( Pr^C_{\alpha}(\psi^i) \) stands for the vector \( (Pr^C_{\alpha}(\psi^i))_{i \in S} \).

2. Otherwise \( h = \max_{i=1}^{n} b_{k_i}^i \), then
   \[
   Pr^C_{\alpha}(\psi) = \prod_{i=1}^{n} Pr^C_{\alpha}(\psi^i) \cdot \prod_{i=1}^{n} f^i_{k_i} (1, \ldots, 1)^T.
   \] (2)

The proof is given in Appendix A for completeness, which follows the same idea as the proof in [9]. Intuitively, the computation is performed by traversing through the time intervals in a forward way in the product CTMC. The time is partitioned into finitely many intervals using endpoints appearing in the formula. With the initial distribution \( \bar{\alpha} \), we compute the probability distribution of all states at the time point \( h \) for the first interval \([0, h)\], which determines the parameter \( \Lambda \). The indicator matrix filters out all paths dissatisfying \( \psi \) at the time point \( h \). The parameter \( \Lambda' \) is determined by the next interval \([h, h')\). We recursively compute the probability distribution at the time point \( h' \), and repeat this until the last time point.

The parameter \( \Lambda \) will be repeatedly adjusted when we push the time forward. We illustrate the theorem by computing \( Pr^C_{\alpha}(\psi^1 \wedge \psi^2) \) in the following example.

**Example 4.** Let \( \psi^1 = f_1 U_{x(0,2)} f_2 U_{x(2,3)} f_3 \) and \( \psi^2 = g_1 U_{y(1,3)} g_2 \). We compute \( Pr^C_{\alpha}(\psi^1 \wedge \psi^2) \) in three phases.

Initially, \( a_{k_1}^1 = 2 \) and \( b_{k_1}^1 = 3 \) are the first two least nonzero endpoints, so \( h = 1 \) and \( h' = 2 \). Accordingly, \( \Lambda = \emptyset \) and \( \Lambda' = (\psi^2) \). By Theorem 1, \( k_1 = 1 \), \( l_1 = 2 \), \( k_2 = 3 \), and \( l_2 = 1 \), which means we should pick out the states satisfying \( f_1 \vee f_2 \) and \( g_1 \) at a given time point \( h \). Then, we compute

\[
\prod_{i=1}^{n} Pr^C_{\alpha}(\psi^i) \cdot \prod_{i=1}^{n} f^i_{k_i} (\Lambda' \cup 1, h),
\]
the probability distribution at time point \( h = 1 \) w.r.t. the product CTMC equipped with parameter \( \emptyset \) showed in Fig. 3. The indicator matrix has only two nonzero entries \( \prod_{i=1}^{n} f^i_{k_i} (1, \psi^1) \) and \( \prod_{i=1}^{n} f^i_{k_i} (1, \psi^2) \). After this step, we push forward the time, so \( \psi^1 \) and \( \psi^2 \) become \( f_1 U_{y(0,1)} f_2 U_{y(1,2)} f_3 \) and \( g_1 U_{y(0,2)} g_2 \), respectively.

In the next phase, \( h = 1, h' = 2 \), accordingly, \( \Lambda = (\psi^2) \), and \( \Lambda' = (\psi^1, \psi^2) \). Then, we compute the probability distribution at \( h = 1 \) w.r.t. the same CTMC in Fig. 3. At the next phase, \( \psi^1 \) and \( \psi^2 \) may be fully satisfied, so we should relocate the state \( (s_1, q_3^1, q_3^2) \) to \( (s_1, q_1^2, q_2^1) \), so the indicator matrix has only one nonzero entry.
1 | 2 | 3
---|---|---
(0, q₁₁, q₁₂) | 1 | e⁻² | 0 | 0
(1, q₁₂, q₁₃) | 0 | 2e⁻² | 0 | 0
(1, q₁₃, q₁₂) | 0 | 0 | 4e⁻⁴ | 0
(2, q₁₂, q₂₂) | 0 | 0 | 0 | 2²e⁻⁴ − 2e⁻⁵ − 2⁻⁴e⁻²
(4, q₁₂, q₂₂) | 0 | 0 | 0 | 2²e⁻⁴ − 2e⁻⁵ + 2⁻⁴e⁻²

Therefore, we have \( \Pr_{\hat{\sigma}}(\psi^1 \land \psi^2) = 4e^{-4} - 4e^{-5} \) by collecting all desired probabilities.

**Corollary 1.** Given a path formula \( \varphi = \bigwedge_{i=1}^{m} \psi^i \) in DNF and a CTMC \( C \), the probability \( \Pr_{\hat{\sigma}}^C(\varphi) \) can be computed by inclusion–exclusion principle.

**4.4. Model checking algorithm and its complexity**

Let \( C = (S, R, L, \alpha) \) be a CTMC, \( s \in S \), and \( \Phi \) be a CCSL state formula. The model checking problem is to check whether \( s \models \Phi \). The standard algorithm to solve CTL-like model checking problems recursively computes the sets of states satisfying \( \Psi \), denoted by \( \text{Sat}(\Psi) \), for all state subformulas \( \Psi \) of \( \Phi \). For CCSL, the cases where \( \Psi \) is an atomic proposition, a negation or a conjunction are standard as for CTL. The case when \( \Psi \) is a conditional probabilistic formula is the challenging part. The model checking algorithm for \( \Pr_{\hat{\sigma}}(\varphi) \) has been discussed in [19], thus we discuss the case of \( \Pr_{\hat{\sigma}}(\psi) \).

Let \( \varphi = \varphi_P \land \varphi \) with \( \varphi_P = \varphi_1 \land \ldots \land \varphi_k \) and \( \varphi = \bigwedge_{i=1}^{m} \psi^i \). By definition, checking \( \psi \) is equivalent to checking whether \( \Pr_{\hat{\sigma}}(\varphi \mid \psi) \sim \varphi \), i.e., whether the quotient of \( \Pr_{\hat{\sigma}}(\varphi \land \psi) \) and \( \Pr_{\hat{\sigma}}(\psi) \) meets the bound \( \sim \varphi \). Now we focus on the conjunction part. Assume that the sets \( \text{Sat}(\varphi_1) \) and \( \text{Sat}(\varphi_2) \) have been computed recursively. We replace \( \varphi_1, \ldots, \varphi_k \) and \( \varphi_1, \ldots, \varphi_l \) by fresh (pairwise disjoint) atomic propositions \( f_1, \ldots, f_k \) and \( g_1, \ldots, g_l \) and add the label \( f_1 \) (resp. \( g_j \)) to the state \( s \) if \( s \in \text{Sat}(\varphi_i) \) (resp. \( s \in \text{Sat}(\varphi_i) \)). Thus, after applying Theorem 1 and Corollary 1 a finite number of times, \( \Pr_{\hat{\sigma}}(\varphi \mid \psi) \) reduces to a product of transient probabilities. We can now apply the results in [11] as follows: By definition, \( \Pr_{\hat{\sigma}}(\rho \mid \psi) \) can be expressed as a quotient of finite sum of the form \( \sum \eta_j \), with algebraic \( \eta_j \). Aziz et al. proved that it is decidable whether such an expression is

5 If any state subformula is undefined, our algorithm will then report undefined.
Again, in the stratified product it can be shown that

$$Pr_{\mathcal{Z}}(\sigma) = \sum_{s' \in S} \mathcal{Z}(s) \cdot \Pr_C(s', \sigma) \cdot \Pr_{\mathcal{Z}}(s')$$

Thus, 

$$Pr_{\mathcal{Z}}(\sigma) = \sum_{s' \in S} \mathcal{Z}(s') \cdot \Pr_C(s', \sigma) \cdot \Pr_{\mathcal{Z}}(s').$$

Hence Eq. (1) holds by $Pr_{\mathcal{Z}}(\sigma) = \sum_{s \in S} \mathcal{Z}(s) Pr_C(\sigma)$.

At last, we prove Eq. (2). For $s' \in S$, define the event $Z(s') := \{ \sigma \mid \sigma @ h = s' \land \forall t \in [0, h), \sigma \rightarrow t = \bigwedge_{i=1}^{n} f_{i_{k_i}} \}$. Again, in the stratified product it can be shown that $\{ \sigma \mid \sigma \models \psi \} \subseteq \bigcup_{s \in S} \mathcal{Z}(s')$. Fix first $\mathcal{G}_\sigma$ as an initial distribution with $\mathcal{G}_\sigma = 1$ and $s \models \bigwedge_{i=1}^{n} f_{i_{k_i}}$. By the law of total probability, we have

$$Pr_C^\sigma(\psi) = \sum_{s' \models \bigwedge_{i=1}^{n} f_{i_{k_i}}} Pr_C(s, h)(s') \cdot \Pr_{\mathcal{Z}}^\psi(s').$$

By definition of $Z(s')$, $Pr_C^\sigma(\psi \models Z(s')) = \pi_C^\sigma(s, h)(s')$ holds. Thus,

$$Pr_C^\sigma(\psi) = \sum_{s' \models \bigwedge_{i=1}^{n} f_{i_{k_i}}} \pi_C^\sigma(s, h)(s') \cdot \Pr_{\mathcal{Z}}^\psi(s').$$

Now let $\sigma \models Z(s')$. We consider the two following cases.

- If $h = \max_{i \in N} |b_{i_{k_i}-1}| < \infty$, then $\sigma \models \psi$ implies that at time $h$, $\sigma$ has reached a state labeled with $f_{1_{k_1}}, \ldots, f_{n_{k_n}}$. This state is good in the product CTMC. So

$$Pr_C^\sigma(\psi) = \sum_{s' \models \bigwedge_{i=1}^{n} f_{i_{k_i}}} \pi_C^\sigma(s, h)(s').$$

It requires that the probability on the states labeled with $f_{1_{k_1}}, \ldots, f_{n_{k_n}}$ should be added. So

$$Pr_C^\sigma(\psi) = \sum_{s' \models \bigwedge_{i=1}^{n} f_{i_{k_i}}} \pi_C^\sigma(s, h)(s') \cdot \mathbf{1}_{s' = \bigwedge_{i=1}^{n} f_{i_{k_i}}}. 1.$$

Eq. (2) for general initial distribution $\mathcal{Z}$ follows as the step 2 of this proof.

- Otherwise $h = \max_{i \in N} |b_{i_{k_i}-1}| = \infty$, then $Pr_C^\sigma(\psi)$ is the probability to reach the states labeled with $f_{1_{k_1}}, f_{2_{k_2}}, \ldots, f_{N_{k_N}}$. Eventually, we just need to pass the $h$ to $\infty$ to obtain the probability. □

References


