2016 IEEE 55th Conference on Decision and Control (CDC)
ARIA Resort & Casino
December 12-14, 2016, Las Vegas, USA

Verifying Continuous-time Stochastic Hybrid Systems via Mori-Zwanzig Model Reduction

Yu Wang, Nima Roohi, Matthew West, Mahesh Viswanathan and Geir E. Dullerud

Abstract— **In this work, we develop a method for verifying Continuous-time Stochastic Hybrid Systems (CTSHSs) using the Mori-Zwanzig model reduction method, whose behaviors are specified by Metric Interval Temporal Logic (MITL) formulas. By partitioning the state space of the CTSHS and computing the optimal transition rates between partitions, we provide a procedure to both reduce a CTSHS to a Continuous-Time Markov Chain (CTMC), and the associated MITL formulas defined on the CTSHS to MITL specifications on the CTMC. We prove that an MITL formula on the CTSHS is true (or false) if the corresponding MITL formula on the CTMC is robustly true (or false) under certain perturbations. In addition, we propose a stochastic algorithm to complete the verification. Finally, as an example, we implement the method in a Billiard Problem.**

I. Introduction

In this work, we study the problem of verifying Metric Interval Temporal Logic (MITL) [1] on continuous-time stochastic hybrid systems (CTSHS) [2]. MITL is a powerful tool to describe both the transient and asymptotic behaviors of various kinds of continuous-time dynamical systems, and to specify design goals in synthesis and verification problems [3]. On finite-state systems, verifying MITL formulas is decidable; however, on infinite-state systems, checking the formulas directly is always beyond the computational capacity of computers.

One possible solution is the abstraction-based method, that is, to find a finite-state system whose behavior simulates perfectly or approximately the infinite-state system. It has been shown that finite state transition systems can be used to simulate linear or piecewise affine systems [4], [5], [6] and certain classes of nonlinear systems [7], [8], [9], [10]; and discrete-time Markov chains can be used to simulate CTSHS [12], [13], [14] and hybrid automata [15], [16], [17], [18]. In those works, continuous-time dynamics are simulated by discrete-time dynamics, and accordingly the properties of the systems are described by discrete-time types of temporal logic.

In this work, we propose an approach of using the Mori-Zwanzig model reduction method [19], [20] to reduce the continuous-time stochastic hybrid systems to continuous-time Markov chains (CTMC) with finite state spaces. This gives us the power of studying directly on the behaviors of the system over continuous time.

This work can be viewed as the hybrid and continuous-time extension of our previous works [21], [22]. Specifically, we find a CTMC that approximates the CTSHS and prove that, to verify an MITL formula on the CTSHS, it is sufficient to check a slightly stronger MITL formula on the CTMC, which can be done by a statistical model checker [23]. we choose the statistical approach since they usually scale better when the number of states increase [24].

The rest of the paper is organized as follows. In Section II, we introduce the general setup of the problem including the definition of continuous-time stochastic hybrid system and the syntax and semantics of metric interval temporal logic. In Section III, we use the Mori-Zwanzig method to reduce the CTSHS to a CTMC, and prove that the MITL formulas on the CTSHS can be verified by checking slightly stronger formulas on the CTMC. Finally, we conclude the main contributions in this work in Section V.

II. Problem Formulation

A. Notations

We denote the set of *natural*, *rational*, *non-negative rational*, *real*, *positive real*, and *non-negative real* numbers, respectively by $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{Q}_{\geq 0}$, $\mathbb{R}$, $\mathbb{R}_+$ and $\mathbb{R}_{\geq 0}$. For any set A, the cardinality is denoted by $|A|$ and the power set is denoted by 2^A. The empty set is denoted by $\emptyset$. For a set $S \subseteq \mathbb{R}^d$, we denote the boundary of S by ∂S.

B. Continuous-time Stochastic Hybrid Systems

In this work, we follow the definition of state-driven continuous-time stochastic hybrid systems in [11]. The *configuration space* is given by $Q \times \Omega$, where $Q = \{q_1, \ldots, q_n\}$ is a finite set of *locations* and $\Omega = \mathbb{R}^d$ is the *continuous state space*. In a location $q_i \in Q$, the continuous state $x \in \Omega$ evolves by a stochastic differential equation

$$\mathrm{d}x(t) = f(q_i,x)\mathrm{d}t + g(q_i,x)\mathrm{d}w_t, \tag{1}$$

where w_t is the standard Brownian motion. It reduces to an ordinary differential equation when $g(q_i,x) = 0$. Meanwhile, the system may switch to another location q_j and reset the continuous state to z by

$$(q_j,z) = h_j(q_i,x) \tag{2}$$

and the transition intensity is given by $r_j(q_i,x)$.

Yu Wang and Geir E. Dullerud are with the Coordinated Science Laboratory and the Department of Mechanical Science and Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA. {yuwang8, dullerud}@illinois.edu

Nima Roohi and Mahesh Viswanathan are with the Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA. {roohi2, vmahesh}@illinois.edu

Matthew West is with the Department of Mechanical Science and Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA. mwest@illinois.edu

a) Evolution of distributions on the system: Give the initial configuration $(q(0),x(0))$ of the system that obeys the distribution $F(0,q,x)$, we can derive a stochastic *trajectory* $\mathscr{T}(t) = (q(t),x(t))$ of the system by solving (1)-(2). The distribution $F(t,q,x)$ of $(q(t),x(t))$ satisfies the Fokker-Planck equation

$$\begin{aligned}\frac{\partial F(t,q_i,x)}{\partial t} &= L(F(t,q_i,x)) \\ &= -\sum_{a=1}^{d}\frac{\partial}{\partial x_a}(f_a(q_i,x)F(t,q_i,x)) \\ &\quad+\sum_{a=1}^{d}\sum_{b=1}^{d}\frac{\partial^2}{\partial x_a\partial x_b}\frac{g_a(q_i,x)g_b(q_i,x)F(t,q_i,x)}{2} \\ &\quad-\sum_{j=1}^{n} r_j(q_i,x)F(t,q_i,x) \\ &\quad+\sum_{h_i(q_j,y)=(q_i,x)} r_i(q_j,y)F(t,q_j,y)\end{aligned} \tag{3}$$

where L is the Fokker-Planck operator for the system. We may write symbolically that $F(t,q,x) = e^{tL}F(0,q,x)$.

Remark 1. (3) *resembles the Fokker-Planck equation for jump-diffusion process where the four terms on the right hand side describes "drift", "diffusion", "jump-out" and "jump-in", respectively.*

C. Timed Automata

In Section IV, we will use the following concept of timed automata to reduce our model checking problem to an emptiness problem.

Definition 1 (Timed Automata)**.** *A timed automaton A is a tuple* $(\mathtt{Q},\mathtt{X},\Sigma,\mathtt{L},\mathtt{I},\mathtt{E},\mathtt{Q}^{\mathtt{init}},\mathtt{Q}^{\mathtt{final}})$ *such that:*

- $\mathtt{Q}$ *is a finite non-empty set of* locations*,*
- $\mathtt{X}$ *is a finite non-empty set of* clocks*,*
- Σ *is a finite non-empty set of* labels*,*
- $\mathtt{L} \in \mathtt{Q} \to \Sigma$ *maps each location to the* label *of that location,*
- $\mathtt{I} \in \mathtt{Q} \to \mathscr{I}^{\mathtt{X}}_{\geq 0}$ *maps each location to its* invariant *which is the set of possible values of variables in that location.*
- $\mathtt{E} \subseteq \mathtt{Q}\times\mathtt{Q}\times 2^{\mathtt{X}}$ *is a finite set of* edges *of the form* (s,d,j)*, where 1) s is the* source*, 2) d is* destination*, and 3) j is the set of clocks that are reset by the edge. Given an edge e, we denote the components by* $\mathtt{Se}$*,* $\mathtt{De}$*, and* $\mathtt{Je}$*.*
- $\mathtt{Q}^{\mathtt{init}} \subseteq \mathtt{Q}$ *is a set of* initial locations*.*
- $\mathtt{Q}^{\mathtt{final}} \subseteq \mathtt{Q}$ *is a set of* final locations*.*

A configuration of a timed automaton A at every time instance is completely determined by its control location and valuation of variables at that time. Each clock takes values in $\mathbb{R}_{\geq 0}$. The set of all possible valuations is $\mathbb{R}^{\mathtt{X}}_{\geq 0}$ which we denote it by $\mathtt{V}$. Also for any $t \in \mathbb{R}_{\geq 0}$, $\nu \in \mathtt{V}$, and $j \subseteq \mathtt{X}$, we define 1) $(\nu+t)(x)$ to be $\nu(x)+t$, and 2) $\nu[j:=0](x)$ to be 0 if $x \in j$ and $\nu(x)$ otherwise.

D. Metric Interval Temporal Logic

We can use the Metric Interval Temporal Logic (MITL) to describe various behaviors of a continuous-time stochastic hybrid system. The advantage of MITL is twofold: it can describe both the transient and asymptotic behaviors, and we can write arbitrarily long logic formulas from some simple rules.

The *atomic propositions* of the logic, which serve as the basic building blocks, depend on a set of *observables* of the system.

Definition 2. *Let $\gamma(q,x)$ be an L_1 function on the configuration space $Q\times\Omega$ and $\mathscr{T}(t) = (q(t),x(t))$ be a trajectory of the continuous-time stochastic hybrid system that obeys the time-evolving distribution $F(t,q,x)$. We define an* observable *y of the system as a map from the set of trajectories of the system to real functions of time by*

$$[y(\mathscr{T})](t) = \mathbb{E}\left[\gamma(q(t),x(t))\right] = \sum_{q\in Q}\int_{\Omega}\gamma(q,x)F(t,q,x)\mathrm{d}x, \tag{4}$$

where $\gamma(q,x)$ is called the weight function*. We refer to the function $[y(\mathscr{T})](t)$ as an* observation *and write it as $y(t)$ when $\mathscr{T}$ is clear from the context.*

The basic building blocks of MITL formulas are simple inequalities on a set of observables. They can be used to reason about the observations of a trajectory.

Definition 3. *Given a set of observables $\{y_1,\ldots,y_m\}$, we define MITL formulas recursively by*

$$\phi ::= \mathtt{F} \mid \mathtt{T} \mid y_i \sim c \mid \neg\phi \mid \phi\wedge\phi \mid \phi\vee\phi \mid \phi\mathscr{U}_{(a,b)}\phi \mid \phi\mathscr{R}_{(a,b)}\phi$$

where $\mathtt{T}$ *stands for "true",* $\mathtt{F}$ *stands for "false", $y_i \sim c$ for $i = 1,\ldots,m$ and $\sim \in \{<,>,\leq,\geq\}$ is an* atomic proposition*, and (a,b) with $a < b$ and $a,b \in \mathbb{Q}_{\geq 0}$ is an interval over rationals. We denote the set of atomic propositions of ϕ by $\mathtt{AP}_\phi$, and may drop the subscript if it is clear from the context.*

The interpretation of an MITL formula depends on an trajectory $\mathscr{T}(t) = (q(t),x(t))$ of the system.

Definition 4. *Let $\mathscr{T}(t) = (q(t),x(t))$ be a trajectory of the continuous-time stochastic hybrid system. We denote $(\mathscr{T},t)(s) = \mathscr{T}(s-t)$ by the suffix of $\mathscr{T}$ starting from t. Given an MITL formula ϕ, the satisfaction relation $\mathscr{T} \vDash \phi$ is interpreted inductively by*

$$\begin{aligned}
&\mathscr{T} \vDash \mathtt{T} && \text{always true}\\
&\mathscr{T} \vDash \mathtt{F} && \text{always false}\\
&\mathscr{T} \vDash y_i \sim c && \Leftrightarrow\ y_i(0) \sim c \text{ in } \mathscr{T} \text{ for } \sim\in\{<,>,\leq,\geq\}\\
&\mathscr{T} \vDash \neg\phi && \Leftrightarrow\ \mathscr{T} \nvDash \phi\\
&\mathscr{T} \vDash \phi_1\wedge\phi_2 && \Leftrightarrow\ \mathscr{T} \vDash \phi_1 \text{ and } \mathscr{T} \vDash \phi_2\\
&\mathscr{T} \vDash \phi_1\vee\phi_2 && \Leftrightarrow\ \mathscr{T} \vDash \phi_1 \text{ or } \mathscr{T} \vDash \phi_2\\
&\mathscr{T} \vDash \phi_1\mathscr{U}_{(a,b)}\phi_2 && \Leftrightarrow\ \exists t \in (a,b)\cdot\ (\mathscr{T},t) \vDash \phi_2\wedge\ \forall t' \in (0,t)\cdot\ (\mathscr{T},t') \vDash \phi_1.\\
&\mathscr{T} \vDash \phi_1\mathscr{R}_{(a,b)}\phi_2 && \Leftrightarrow\ \forall t \in (a,b)\cdot(\mathscr{T},t) \vDash \phi_1 \text{ or } \exists t\cdot(\mathscr{T},t) \vDash \phi_2\wedge\forall t' \in [0,t]\cap(a,b)\cdot(\mathscr{T},t') \vDash \phi_1
\end{aligned}$$

Finally, we define $[\![\phi]\!]$ to be the set of signals that satisfy ϕ.

Remark 2. *It is enough to only considers formulas in negated normal form. Since the atomic propositions are inequalities, it is also enough to restrict attention to $>$ and*

$\geq$. *Finally, since we are using statistical methods to check MITL formulas, we do not distinguish strict and non-string inequalities.*

Here is an example of how to use MITL formulas to specify the behavior of the system.

Example 1. *Consider an observable y whose weight function is*

$$\gamma(q,x) = \begin{cases} 1, & \text{if } q = q_i \text{ and } x \in A, \\ 0, & \text{otherwise}, \end{cases} \tag{5}$$

where $A \subseteq \Omega$. Then the MITL formula $\mathtt{T}\mathscr{U}_{(0,1)}(y > 0.5)$ means that there is a time $t < 1$ such that the probability of being in $q_i \times A$ is above 0.5.

E. A fundamental algorithm

In [25], an statistical algorithm $\mathtt{Close}(y, y', \alpha, \delta)$ has been proposed to check whether $\|y - y'\| < \delta$, for any two probability distributions y and y' on the same finite states. This algorithm is sub-linear and provides the following guarantee.

Theorem 1. *[25] For any α and δ, and distributions y and y' over the same n states, there is a test which runs in time $O\big(n^{2/3}(2\delta)^{-8/3}\log(n/\alpha)\big)$ such that if $\|y - y'\| \leq \max\Big(\frac{\delta^{4/3}}{2^{14/3}\sqrt[3]{n}}, \frac{\delta}{4\sqrt{n}}\Big)$ then the test accepts with probability at least $1-\alpha$, and if $\|y - y'\| > \delta$ then the test rejects with probability at least $1-\alpha$.*

III. Model Reduction

A. Reducing the Dynamics

To implement the Mori-Zwanzig model reduction method to CTSHS, we first divide the state space into finitely many partitions, and treat each of them as a discrete state.

Definition 5. *$S = \{s_1, s_2, \ldots, s_l\}$ is called a measurable partition of the continuous state space Ω, if for $i, j = 1, \ldots, l$ and $i \neq j$,*

1) *s_i is nonempty, open and simply-connected,*
2) *$\mu(\Omega \backslash \bigcup_{i=1}^{l} s_i) = 0$,*
3) *$s_i \cap s_j = \emptyset$ for any $i \neq j$,*

where μ is the Borel measure on S.

We assume the partitions to be open and simply-connected to rule out wired-shaped ones. Given a partition of the continuous state space Ω, we will construct the reduced system as a Continuous-time Markov Chain (CTMC). Let $m(\Omega)$ and $m(S)$ be set of probability distribution functions on Ω and S, respectively. First, we can define a projection $P : m(\Omega) \to m(S)$ and an injection $R : m(S) \to m(\Omega)$ between $m(\Omega)$ and $m(S)$ by

$$p_j = Pf(x) = \int_{s_j} f(x)\mathrm{d}x, \tag{6}$$

where p_j is the jth element of p, and

$$f(x) = Rp = \sum_{j=1}^{l} p_j \mathbf{U}_{s_j}, \tag{7}$$

where $\mathbf{U}_{s_j}$ is the uniform distribution on s_j

$$\mathbf{U}_{s_j}(x) = \begin{cases} \frac{1}{\mu(s_j)}, & \text{if } x \in s_j \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

Remark 3. *Here the projection P and the injection R are defined for probability distributions. But they extend naturally to L_1 functions on Ω and S respectively.*

Remark 4. *The projection P is the left inverse of the injection R but not* vice versa*, namely $PR = I$ but $RP \neq I$.*

Obviously, the partition of the continuous state space Ω induces a discretization of the configuration space Q by $Q \times S$. Let $p = [p_{ij}]_{nl}$ be a probability distribution on $Q \times S$ and $F(q,x)$ be a probability distribution on $Q \times \Omega$. Then the projection and injection defined above extends to $m(Q \times \Omega)$ and $m(Q \times S)$ by acting on the second argument, namely

$$p_{ij} = PF(q_i, x) = \int_{s_j} F(q_i, x)\mathrm{d}x, \tag{9}$$

and

$$F(q_i, x) = Rp = \sum_{j=1}^{l} p_{ij} \mathbf{U}_{s_j}. \tag{10}$$

In particular, given an initial distribution $F(0,q,x)$ on the CTSHS, we can derive an initial distribution $p(0)$ on the CTMC by the projection P.

This projection P and injection R can reduce the Fokker-Planck operator to a transition rate matrix on $Q \times S$, hence reduce the continuous-time stochastic hybrid system into a continuous-time Markov chain.

Theorem 2. *Let $S = \{s_1, s_2, \ldots, s_l\}$ be a partition of the continuous state space Ω and P, R be the corresponding projection and injection defined in* (9)-(10)*. The Fokker-Planck operator given in* (3) *reduces to the transition rate matrix A of a continuous-time Markov chain on $Q \times S$ by*

$$A = PLR \tag{11}$$

where the transition rate from state ij to ab at time t is given by

$$A_{abij}(t) = \begin{cases} \int_{\partial s_j \cap \partial s_b} f(t, q_i, x)\mathrm{d}x, & \text{if } a = i, \\ \frac{1}{\mu(s_j)} \int_{s_j} r_a(t, q_i, x)\mathbf{I}_{h_a(t,q_i,x) \in s_b}(x)\mathrm{d}x, & \text{otherwise.} \end{cases} \tag{12}$$

for $i, a = 1, \ldots, n$ and $j, b = 1, \ldots, l$, where $\mathbf{I}_{h_a(t,q_i,x) \in s_b}(x) = 1$ when $h_a(t, q_i, x) \in s_b$, and 0 *otherwise.*

Proof. Plug the Fokker Planck equation (3) and the definition of projection (9) and injection (10) into (11). □

Roughly speaking, the transition rate between two partitions in the same location is the flux of $f(t,q,x)$ across the boundary and the transition rate between two different locations is the flux of $r(t,q,x)$.

Remark 5. *Previously, we assumed that the partition of the continuous state space Ω is identical for every location $q \in Q$. But, the above statements can be easily extended to the case of partitioning Ω differently for each location.*

B. Reducing MITL Formulas

The observables on the continuous-time stochastic hybrid systems (see Definition 2) extend to the corresponding continuous-time Markov chains by using the injection R. For the time-evolving distribution $p(t)$ on the CTMC that derives from the model reduction procedure, we can define the observable on the CTMC by plugging Rp into (4).

Definition 6. *Let y be an observable on the continuous-time stochastic hybrid system with weight function $\gamma(q,x)$. We define a corresponding observable y' on the continuous-time Markov chain that derives from the model reduction procedure by*

$$[y'(\mathscr{S})](t) = \sum_{q\in Q}\int_{\Omega}\gamma(q,x)Rp(t)\mathrm{d}x, \tag{13}$$

where $\mathscr{S}$ is a trajectory of the continuous-time Markov chain that obeys the distribution $p(t)$.

Throughout the section, to facilitate further discussion, we will always denote the corresponding observable on the CTMC by y' for any observable y on the CTSHS.

For a given observable y with weight function $\gamma(q,x)$, the error of the projection P with respect to the observable y is defined by the maximal possible difference between y and y',

$$\begin{aligned}\Delta_y &= |y-y'|\\ &= |\sum_{q\in Q}\int_{\Omega}\gamma(q,x)(F(0,q,x)-RPF(0,q,x))\mathrm{d}x|.\end{aligned} \tag{14}$$

Remark 6. *When refining the partition of Ω, the operator $QP\to I$ in the weak operator topology, thus $\Delta_y\to 0$ for any given y.*

By the definition of Δ_y, we know that, at the initial time, the atomic propositions on the CTSHS and the CTMC has the following relations

$$y(0) > c \Longrightarrow y'(0) > c-\Delta_y, \tag{15}$$
$$y(0) < c \Longrightarrow y'(0) < c+\Delta_y, \tag{16}$$

and similarly,

$$y'(0) > c+\Delta_y \Longrightarrow y(0) > c, \tag{17}$$
$$y'(0) < c-\Delta_y \Longrightarrow y(0) < c. \tag{18}$$

To derive the relations of the observations between the CTSHS and the CTMC at any time, we define the reduction error of the observation y at time t due to the model reduction process by

$$\begin{aligned}\Theta_y(t) &= |y(t)-y'(t)|\\ &= |\sum_{q\in Q}\int_{\Omega}\gamma(q,x)(e^{Lt}-Re^{At}P)F(0,q,x)\mathrm{d}x|,\end{aligned} \tag{19}$$

where $F(0,q,x)$ is an initial distribution of the CTSHS and $y'(t)$ is the corresponding observation of $y(t)$ on the CTMC (see Definition 6). This reduction error is illustrated in Figure 1. Note that the diagram is not commutative;

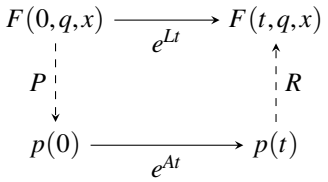

Fig. 1. Diagram for reduction error.

actually the difference between going along the two paths is related to the reduction error.

In general, the reduction error $\Theta(t)$ may not be bounded as $t\to\infty$. To find a sufficient condition, we define the reduction error of the Fokker-Planck operator L by

$$\delta(t,q,x) = (L-RPL)e^{tRPL}F(0,q,x). \tag{20}$$

Accordingly, we define the integration of $\delta(t,q,x)$ with respect to the weight function $\gamma(q,x)$ by

$$\begin{aligned}\Lambda_y &= \sup_{t\geq 0}|\frac{\mathrm{d}y(t)}{\mathrm{d}t}-\frac{\mathrm{d}y'(t)}{\mathrm{d}t}|\\ &= \sup_{t\geq 0}|\sum_{q\in Q}\int_{\Omega}\gamma(q,x)\delta(t,q,x)\mathrm{d}x|,\end{aligned} \tag{21}$$

which captures the maximal change of the time derivative of observation y.

A sufficient condition to find a uniform bound over time is that the reduction error of the Fokker-Planck operator $\delta(f(q,x))$ converges exponentially in time for any $f(q,x)\in m(Q\times\Omega)$.

Definition 7. *For $\alpha>0$, $\beta\geq 1$ and a given observable y, the continuous-time stochastic hybrid system is α-contractive with respect to y, if for any initial distribution function $F(0,q,x)$ on the configuration space, we have*

$$\begin{aligned}&|\sum_{q\in Q}\int_{\Omega}\gamma(q,x)e^{tL}\delta(t,q,x)\mathrm{d}x|\\ &\quad\leq \beta e^{-\alpha t}|\sum_{q\in Q}\int_{\Omega}\gamma(q,x)\delta(t,q,x)\mathrm{d}x|.\end{aligned} \tag{22}$$

where $\delta(t,q,x)$ is given by (20)

This contractivity condition, though seems restrictive, is valid for a relatively wide range of systems including asymptotically stable systems. It is a commonly used sufficient condition to guarantee the existence and uniqueness of invariant measure of general dynamical systems, and the contractivity factor α is usually derived case-by-case. Using Definition 7, we derive the following theorem.

Theorem 3. *If the continuous-time stochastic hybrid system is α-contractive, then for any $t\geq 0$, the reduction error $\Theta_y(t)$ for an observable y satisfies*

$$\Theta_y(t) \leq \frac{\beta\Lambda_y}{\alpha}+\Delta_y. \tag{23}$$

Proof. By Dyson's formula, we can decompose the exponential of L by

$$e^{tL} = e^{tRPL} + \int_{[0,t]} e^{(t-s)L}(L - RPL)e^{sRPL}\mathrm{d}s. \tag{24}$$

This formula, sometimes referred to as Duhamel's principle, can be verified by taking time derivatives on both sides. Plugging (24) into (19) gives

$$\begin{aligned}\Theta_y(t) \le & |\sum_{q\in Q}\int_\Omega \gamma(q,x)(e^{tRPL} - Re^{tA}P)F(0,q,x)\mathrm{d}x| \\ & + |\sum_{q\in Q}\int_\Omega\int_{[0,t]} \gamma(q,x)e^{(t-s)L}(L-RPL)e^{sRPL}F(0,q,x)\mathrm{d}s\mathrm{d}x|\end{aligned} \tag{25}$$

Since the projection P and the injection R preserve L_1 norm, RPL is also a Fokker-Planck operator. Noting $Re^{tA}PF(0,q,x) = e^{tRPL}PF(0,q,x)$, by (14), we obtain that the first term on the right hand side of (25) is less than Δ_y.

For the second term on the right hand side of (25), by (21)-(22), we have

$$\begin{aligned}\Theta_y(t) &\le \Delta_y + |\sum_{q\in Q}\int_\Omega\int_{[0,t]} \gamma(q,x)e^{(t-s)L}\delta(s,q,x)\mathrm{d}s\mathrm{d}x| \\ &\le \Delta_y + |\sum_{q\in Q}\int_\Omega\int_{[0,t]} \beta e^{-\alpha(t-s)}\gamma(q,x)\delta(s,q,x)\mathrm{d}s\mathrm{d}x| \\ &\le \frac{\beta\Lambda_y}{\alpha} + \Delta_y.\end{aligned} \tag{26}$$

□

Theorem 3 implies the following relations between the atomic propositions on the CTSHS and the CTMC.

Theorem 4. *If the continuous-time stochastic hybrid system is α-contractive, then we have*

$$y(t) > c \Longrightarrow y'(t) > c - (\frac{\beta\Lambda_y}{\alpha} + \Delta_y), \tag{27}$$

$$y(t) < c \Longrightarrow y'(t) < c + (\frac{\beta\Lambda_y}{\alpha} + \Delta_y), \tag{28}$$

and similarly,

$$y'(t) > c + (\frac{\beta\Lambda_y}{\alpha} + \Delta_y) \Longrightarrow y(t) > c, \tag{29}$$

$$y'(t) < c - (\frac{\beta\Lambda_y}{\alpha} + \Delta_y) \Longrightarrow y(t) < c. \tag{30}$$

The above theorem gives the following result.

Theorem 5. *Given a MITL formula ϕ on the CTSHS that is α-contractive, it can be strengthened to ψ by replacing the atomic propositions according to* (29)-(30)*. If ψ is true on the corresponding CTMC, then ϕ is true on the CTSHS.*

Example 2. *Recall Example 1. The MITL formula $\mathtt{T}\mathscr{U}_{(0,1)}(y > 0.5)$ is true on the CTSHS if $\mathtt{T}\mathscr{U}_{(0,1)}(y > 0.5 + (\frac{\beta\Lambda_y}{\alpha} + \Delta_y))$ is true on the CTMC. It is false on the CTSHS if $\mathtt{T}\mathscr{U}_{[0,1]}(y < 0.5 - (\frac{\beta\Lambda_y}{\alpha} + \Delta_y))$ is true on the CTMC.*

IV. Statistical Model Checking of MITL

In this section we show that for a CTMC C and a MITL formula ϕ with atomic propositions $\{P_i\}$, we can construct statistically a timed automaton $T_{C,\mathtt{AP}_\phi}$ (see Section II-C) such that reachable locations of this automaton at time t are labeled by the subset of atomic propositions in ϕ that are true in C at that time. By $[\![C,\mathtt{AP}_\phi]\!]$ we denote the singleton set containing the unique signal induced by C and ϕ. For simplicity, we assume $\mathtt{AP}_\phi$ is singleton and focus only on constructing $T_{C,\{P\}}$ for an atomic formula $P := y_i > c$. Let $f(t)$ be the set of atomic formulas that y satisfies at time t. Formally $(y_i, c) \in f(t)$ iff $y_i(t) > c$. Also, let $T_{C,\{P\}}(t)$ be the set of reachable locations of $T_{C,\{P\}}$ at time t.

We have assumed that the reduced model is contractive and hence the function $y(t)$ converges to a *known* invariant y^{inv}. Therefore, there is a time T, which can be found by Figure 2, such that $\|y(t) - y^{\mathrm{inv}}\| < \delta_2$ for $t \ge T$.

1: $t \leftarrow 1$
2: **while** $\mathtt{Close}\big(y(t), y^{\mathrm{inv}}, \frac{3\alpha}{4}, \delta_2\big) \neq \mathtt{yes}$ **do** $t \leftarrow t+1$
3: **return** t

Fig. 2. Finding the time for being close to invariant distribution

For some given $\delta_1 > 0$, let $\Delta = \frac{\delta_1}{3\max\{|\dot{y}_i(t)| \mid t\in[0,T]\}}$. Then, for any $t \in [0,T]$ and $t' \in [t-\Delta, t+\Delta] \cap [0,T]$, we have

1. if $y_i(t) - c > \frac{\delta_1}{3}$ then $y_i(t') - c > 0$,
2. if $y_i(t) - c < -\frac{\delta_1}{3}$ then $y_i(t') - c < 0$,
3. if $|y_i(t) - c| \le \frac{2\delta_1}{3}$ then $|y_i(t') - c| \le \delta_1$.

We can partition $[0,T)$ into $\lceil T/\Delta \rceil + 1$ intervals of size smaller than Δ, and run (recall Section II-E)

$$res_1 = \mathscr{A}_1^{\delta_1/3}(y_i(t), c + \delta_1/3, \alpha', \beta')$$
$$res_2 = \mathscr{A}_1^{\delta_1/3}(y_i(t), c - \delta_1/3, \alpha', \beta')$$

for each interval. If $res_1 = \mathtt{yes}$, then for any time t' in the interval, $y_i(t') > c$ with bounded error α', hence we set $T_{C,\{P\}}(t) = \{P\}$. If $res_2 = \mathtt{no}$, then for any time t' in the interval, $y_i(t') < c$ with bounded error α', hence we set $T_{C,\{P\}}(t) = \{\emptyset\}$. Otherwise, for any time t' in the interval, $|y_i(t) - c| \le \frac{2\delta_1}{3}$ with bounded error $\max(2\alpha', \beta')$. In this case, we set 1) $T_{C,\{P\}}(t) = \{q, q'\}$, 2) $\mathtt{L}(q) = \{P\}$ and $\mathtt{L}(q') = \emptyset$, 3) entry to q or q', and 4) switches between q and q' for arbitrary number of times, while their common invariant permits.

The above procedure is formally given in Figure 3. This algorithm terminates and the output $res = \mathscr{A}^{\delta_1,\delta_2}(C, y_0, \phi, \alpha, \beta)$ satisfies

$$\mathbb{P}[res = \mathtt{no} \mid C \vDash \phi] \le \alpha \tag{31a}$$
$$\mathbb{P}[res = \mathtt{yes} \mid C \nvDash \phi] \le \alpha \tag{31b}$$

As for the `unknown` output, let $B^{\delta_1}(y)$ be the δ_1-ball centered at y in L_∞ norm. The algorithm guarantees that

$$\mathbb{P}[res = \mathtt{unknown}] \le \alpha + \beta \tag{32}$$

when $y' \vDash \phi$, or $y' \nvDash \phi$, for all $y' \in B^{\delta_1}(y)$.

$h \leftarrow \max\{|\dot{y}_i(t)| \mid t \in [0,T]\}$
$\Delta \leftarrow \frac{\delta_1}{3h}$, $n \leftarrow |\mathtt{AP}|\left\lceil \frac{T}{\Delta} \right\rceil$
$T_{C,\{P\}} \leftarrow$ an empty automaton
$\mathtt{X} \leftarrow \{t\}$, $q_{\mathsf{last}} \leftarrow \perp$
for $i \leftarrow 0$ to $\left\lfloor \frac{T}{\Delta} \right\rfloor$ **do**
    $\alpha' \leftarrow \min(\frac{\alpha}{4n}, \frac{\beta}{2n})$, $\beta' \leftarrow \frac{\beta}{n}$
    $res_1 \leftarrow \mathscr{A}_1^{\delta_1/3}\left(y_i\left((i+\frac{1}{2})\Delta\right), c+\frac{\delta_1}{3}, \alpha', \beta'\right)$
    $res_2 \leftarrow \mathscr{A}_1^{\delta_1/3}\left(y_i\left((i+\frac{1}{2})\Delta\right), c-\frac{\delta_1}{3}, \alpha', \beta'\right)$
    add a new location q to $\mathtt{Q}$
    if $res_1 = \mathtt{yes}$ **then** $\mathtt{L}(q) \leftarrow \{P\}$
    else if $res_2 = \mathtt{no}$ **then** $\mathtt{L}(q) \leftarrow \emptyset$
    else $\mathtt{L}(q) \leftarrow \mathtt{unknown}$
    $\mathtt{I}(q) \leftarrow 2i\Delta \le t < 2(i+1)\Delta$
    if $q_{\mathsf{last}} \neq \perp$ **then** $\mathtt{E} \leftarrow \mathtt{E} \cup \{(q_{last}, q, \emptyset)\}$
    else $\mathtt{Q}^{\mathsf{init}} \leftarrow \{q\}$
    $q_{\mathsf{last}} = q$
add a new location q to $\mathtt{Q}$
$\mathtt{I}(q) \leftarrow true$, $\mathtt{Q}^{\mathtt{final}} \leftarrow \{q\}$
$\mathtt{E} \leftarrow \mathtt{E} \cup \{(q_{last}, q, \emptyset), (q, q, \emptyset)\}$
if $y^{\mathrm{inv}} > c$ **then** $\mathtt{L}(q) \leftarrow \{P\}$
else $\mathtt{L}(q) \leftarrow \emptyset$
$T_{C,\{P\}} \leftarrow$ replace any `unknown` location in $\mathtt{Q}$ with q and q' labeled $\{P\}$ and $\emptyset$. Duplicate edges from/to q and q' accordingly.
Add $(q, q', \emptyset)$ and $(q', q, \emptyset)$ to $\mathtt{E}$ for every split locations in the previous step.
return $T_{C,\{P\}}$

Fig. 3. Constructing the signal for atomic proposition P

Remark 7. *For any CTMC C and MITL formula ϕ, if C is robust on ϕ, iteratively reducing δ_1 in our algorithm guarantees that it will eventually return an answer which is not* `unknown` *while satisfying conditions 31a and 31b.*

V. Conclusion

In this work, we proposed a framework of using metric interval temporal logic formulas to describe the behavior of continuous-time stochastic hybrid systems and a method of using the Mori-Zwanzig model reduction method to verify the temporal logic formulas. Specifically, we discretized the system by partitioning the configuration space and derived a continuous-time Markov chains that optimally approximates the original system. We proved that the problem of verifying the temporal logic formulas on the CTSHS can be transformed to the problem of verifying a slightly stronger formulas on the CTMC and used a sampling-based method to finish the verification.

References

[1] R. Alur, T. Feder, and T. A. Henzinger, "The benefits of relaxing punctuality," *J. ACM*, vol. 43, no. 1, pp. 116–146, Jan. 1996.

[2] A. R. Teel, A. Subbaraman, and A. Sferlazza, "Stability analysis for stochastic hybrid systems: A survey," *Automatica*, vol. 50, no. 10, pp. 2435 – 2456, 2014.

[3] E. M. Clarke and P. Zuliani, "Statistical model checking for cyber-physical systems," in *Automated Technology for Verification and Analysis*, ser. LNCS, 2011, pp. 1–12.

[4] P. Tabuada and G. Pappas, "Linear time logic control of discrete-time linear systems," *IEEE Transactions on Automatic Control*, vol. 51, no. 12, pp. 1862–1877, Dec. 2006.

[5] M. Kloetzer and C. Belta, "A fully automated framework for control of linear systems from temporal logic specifications," *IEEE Transactions on Automatic Control*, vol. 53, no. 1, pp. 287–297, Feb. 2008.

[6] T. Wongpiromsarn, U. Topcu, and R. M. Murray, "Receding horizon control for temporal logic specifications," in *HSCC*, 2010, pp. 101–110.

[7] G. Pola, A. Girard, and P. Tabuada, "Approximately bisimilar symbolic models for nonlinear control systems," *Automatica*, vol. 44, no. 10, pp. 2508 – 2516, 2008.

[8] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 116–126, 2010.

[9] M. Zamani, G. Pola, M. Mazo, and P. Tabuada, "Symbolic models for nonlinear control systems without stability assumptions," *IEEE Transactions on Automatic Control*, vol. 57, no. 7, pp. 1804–1809, 2012.

[10] J. Liu, N. Ozay, U. Topcu, and R. M. Murray, "Synthesis of reactive switching protocols from temporal logic specifications," *IEEE Transactions on Automatic Control*, vol. 58, no. 7, pp. 1771–1785, 2013.

[11] J. P. Hespanha, "Modeling and analysis of networked control systems using stochastic hybrid systems," *Annual Reviews in Control*, vol. 38, no. 2, pp. 155 – 170, 2014.

[12] I. Tkachev and A. Abate, "Formula-free finite abstractions for linear temporal verification of stochastic hybrid systems," in *Proceedings of the 16th international conference on Hybrid Systems: Computation and Control*. ACM, 2013, pp. 283–292.

[13] I. Tkachev, A. Mereacre, J.-P. Katoen, and A. Abate, "Quantitative automata-based controller synthesis for non-autonomous stochastic hybrid systems," in *Proceedings of the 16th international conference on Hybrid Systems: Computation and Control*. ACM, 2013, pp. 293–302.

[14] M. Zamani, P. M. Esfahani, R. Majumdar, A. Abate, and J. Lygeros, "Symbolic control of stochastic systems via approximately bisimilar finite abstractions," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3135–3150, 2014.

[15] B. Liu, D. Hsu, and P. S. Thiagarajan, "Probabilistic approximations of ODEs based bio-pathway dynamics," *Theoretical Computer Science*, vol. 412, no. 21, pp. 2188–2206, May 2011.

[16] B. Liu, A. Hagiescu, S. K. Palaniappan, B. Chattopadhyay, Z. Cui, W.-F. Wong, and P. S. Thiagarajan, "Approximate probabilistic analysis of biopathway dynamics," *Bioinformatics*, vol. 28, no. 11, pp. 1508–1516, Jun. 2012.

[17] P. Zuliani, "Statistical model checking for biological applications," *STTT*, pp. 1–10, Aug. 2014.

[18] B. M. Gyori, B. Liu, S. Paul, R. Ramanathan, and P. Thiagarajan, "Approximate probabilistic verification of hybrid systems," in *Hybrid Systems Biology*. Springer, 2015, pp. 96–116.

[19] A. J. Chorin, O. H. Hald, and R. Kupferman, "Optimal prediction and the Mori-Zwanzig representation of irreversible processes," *Proceedings of the National Academy of Sciences*, vol. 97, no. 7, pp. 2968–2973, Mar. 2000.

[20] C. Beck, S. Lall, T. Liang, and M. West, "Model reduction, optimal prediction, and the Mori-Zwanzig representation of markov chains," in *CDC/CCC*, 2009, pp. 3282–3287.

[21] Y. Wang, N. Roohi, M. West, M. Viswanathan, and G. E. Dullerud, "Statistical verification of dynamical systems using set oriented methods," in *HSCC*, 2015, pp. 169–178.

[22] ——, "A Mori-Zwanzig and MITL based approach to statistical verification of continuous-time dynamical systems," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 267 – 273, 2015, ADHS.

[23] N. Roohi and M. Viswanathan, "Statistical model checking for unbounded until formulas," *STTT*, vol. 17, no. 4, pp. 417–427, 2015.

[24] H. L. S. Younes and R. G. Simmons, "Statistical probabilistic model checking with a focus on time-bounded properties," *Information and Computation*, vol. 204, no. 9, pp. 1368–1409, Sep. 2006.

[25] T. Batu, L. Fortnow, R. Rubinfeld, W. D. Smith, and P. White, "Testing closeness of discrete distributions," *J. ACM*, vol. 60, no. 1, pp. 4:1–4:25, Feb. 2013.