Quantitative Automata Model Checking of Autonomous Stochastic Hybrid Systems*

Alessandro Abate
Delft Center for Systems & Control
Mekelweg 2, 2628 CD Delft
The Netherlands
a.abate@tudelft.nl

Joost-Pieter Katoen
Software Modeling and Verification Group
Ahornstraße 55
D-52056 Aachen, Germany
katoen@cs.rwth-aachen.de

Alexandru Mereacre
Software Modeling and Verification Group
Ahornstraße 55
D-52056 Aachen, Germany
mereacre@cs.rwth-aachen.de

ABSTRACT

This paper considers the quantitative verification of discrete-time stochastic hybrid systems (DTSHS) against linear time objectives. The central question is to determine the likelihood of all the trajectories in a DTSHS that are accepted by an automaton on finite or infinite words. This verification covers regular and ω-regular properties, and thus comprises the linear temporal logic LTL. This work shows that these quantitative verification problems can be reduced to computing reachability probabilities over the product of an automaton and the DTSHS under study. The computation of reachability probabilities can be performed in a backward-recursive manner, and quantitatively approximated by procedures over discrete-time Markov chains. A case study shows the feasibility of the approach.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous

General Terms

Theory

Keywords

Stochastic hybrid systems, finite state automata, LTL

1. INTRODUCTION

Stochastic hybrid systems (SHS, for short) are pivotal in application areas such as systems biology, air traffic control, finance, and telecommunication systems [6]. Their main analytical challenge is to treat the intricate intertwining of discrete dynamics, continuous phenomena, and randomness. An important class of properties for such systems are probabilistic invariance (i.e., what is the likelihood to stay in a set of "safe" states for some period of time?) and reachability (i.e., what is the likelihood to reach a certain set of "goal" states within a number of steps?). Variants thereof, such as reach-avoid objectives, have also been considered [18]. A broad palette of techniques has been developed to compute these quantities, e.g., measure-theoretical approaches [5], Monte Carlo simulations [14], coupled Hamilton Jacobi Bellman equations [13], approximation methods that turn an infinite-state problem into a finite-state one [15], and dynamic programming [3]. These approaches exist for controllable as well as autonomous models (i.e. "deterministic" SHS), where in the former case maximal – or dually minimal – probabilities are determined [3].

On the other hand, probabilistic reachability, invariance, and reach-avoid measures have been studied extensively in the field of probabilistic model checking. In fact, these properties can all naturally be expressed in PCTL [11], the probabilistic variant of the branching-time temporal logic CTL. Thanks to the effective support of powerful software tools such as PRISM [1] and MRMC [12], the verification of this class of properties has been successfully applied to numerous models for systems biology, security protocols, hardware circuits and reliability analysis. This insight has recently culminated into the generalization of CTL model checking to continuous state space [7], the application of PCTL model checking to discrete-time SHS (DTSHS) [2], and a study on the relationship between PCTL and dynamic programming for SHS models [17].

The use of PCTL allows for the expression of a significant class of properties that can be analyzed over SHS. This paper takes a somewhat orthogonal direction by considering probabilistic *linear-time* objectives. An example of such an objective is a more advanced reach-avoid property, such as the following: determine the likelihood, starting from some initial point, to reach a set of "goal" states, while avoiding "bad" states, but conditional on visiting some "trigger" states prior to reaching the goal states. Other examples include repeated reachability objectives (certain goal states must be visited repeatedly), conjuncted with a persistence property – from some point on, the system should only obey goal states. Such objectives can naturally be provided as finite-

*This research is funded by the DFG research training group 1295 AlgoSyn, by the European Commission under the MoVeS project, FP7-ICT-2009-257005, by the European Commission under Marie Curie grant MANTRAS 249295, and by NWO under VENI grant 016.103.020.

HSCC'11, April 12–14, 2011, Chicago, Illinois, USA.

state automata, either on finite or on infinite words. This includes regular and ω-regular properties, and thus covers the linear temporal logic LTL and several properties that cannot be expressed in PCTL (like the ones above).

The central question that we address in this paper is how to determine the probability that a given discrete-time SHS satisfies an automaton. Stated differently, we investigate what is the likelihood of the trajectories in the DTSHS that are accepted by the automaton. In order to cope with the quantitative verification of DTSHS against automata objectives, we resort to a well-known technique from model checking: product construction. We consider the synchronous product of a DTSHS $\mathcal{H}$ and a (Büchi) automaton $\mathcal{A}$. Technically this is achieved by adopting deterministic finite-state automata (for finite words) and separated generalized Büchi automata [8] (for infinite words). The key result is that the probability of all paths in $\mathcal{H}$ that are accepted by $\mathcal{A}$ can be reduced to computing reachability probabilities in the product $\mathcal{H} \otimes \mathcal{A}$. These reachability probabilities can in principle be determined by any available technique for DTSHS. We then consider a finite abstraction of the DTSHS as a discrete-time Markov chain (DTMC), and provide an approximation (with explicit errors) of the time-bounded or -unbounded reachability objectives. Aa a numerical case study, a two-room heating benchmark [2] is used to illustrate the application and feasibility of our approach.

Automated verification of stochastic hybrid systems is *en vogue*, and several quite recent works have appeared focusing on safety properties. Zhang *et al.* [20] propose a technique for verifying probabilistic safety problems by adopting abstraction techniques from the verification of hybrid systems. Fränzle *et al.* apply stochastic satisfiability modulo theory (SSMT) to the symbolic analysis of probabilistic bounded reachability problems of probabilistic hybrid automata. This SSMT-approach has recently been extended to computing expected values of probabilistic hybrid systems, for instance mean-times to failure [10]. This paper complements the verification techniques using PCTL [2, 17], and includes safety as well as liveness properties.

2. PRELIMINARIES

We consider the model of discrete time stochastic hybrid systems (DTSHS) from [2], which is an autonomous (uncontrolled) version of that in [3]. A DTSHS is a stochastic model with a hybrid state space $\mathbb{S} = \cup_{\ell \in Loc}\{\ell\} \times S_\ell, S_\ell \subseteq \mathbb{R}^{d(\ell)}$, given by the disjoint union of continuous domains S_ℓ (each of which with its own dimension, specified by $d : Loc \to \mathbb{N}$) associated to discrete locations *Loc*, also referred to as the "modes". A point in the hybrid state space $s = (\ell, x)$ is thus made up of two components: a discrete one $\ell \in Loc$ and a continuous one $x \in \mathbb{R}^{d(\ell)}$. Unlike [2, 3], here discrete labels are associated with locations via a function L. Let $\mathcal{B}(\mathbb{S})$ denote the σ-algebra generated by the subsets A of $\mathbb{S}$ of the form $A = \cup_{\ell \in Loc}\{\ell\} \times A_\ell$, where $A_\ell \in \mathcal{B}(\mathbb{R}^{d(\ell)})$ is a Borel set in $\mathbb{R}^{d(\ell)}$. We use the notation $\mathbf{dom}(\ell)$ to denote the domain associated to location ℓ.

Definition 1. *[DTSHS] A* DTSHS *is a structure* $\mathcal{H} = (Loc, \mathrm{AP}, L, d, \alpha, T_x, T_\ell, T_r)$*, where:*

- Loc *- is a finite set of locations;*
- AP *- is a finite set of atomic propositions;*
- $L : Loc \to 2^{\mathrm{AP}}$ *- is the labeling function, which acts on the discrete locations;*
- $d : Loc \to \mathbb{N}$ *- is the dimension assigned to the continuous domain* $\mathbb{R}^{d(\ell)}$ *of each location* $\ell \in Loc$*;*
- $\alpha : \mathcal{B}(\mathbb{S}) \to [0, 1]$ *- is the initial probability distribution;*
- $T_\ell : Loc \times \mathbb{S} \to [0, 1]$ *- is a conditional discrete stochastic kernel, which assigns to each* $s \in \mathbb{S}$ *a probability distribution,* $T_\ell(\cdot|s)$*, over Loc;*
- $T_x : \mathcal{B}(\mathbb{R}^{d(\cdot)}) \times \mathbb{S} \to [0, 1]$ *- is a continuous stochastic kernel on* $\mathbb{R}^{d(\cdot)}$*, conditional on* $\mathbb{S}$*. It assigns to each* $s = (\ell, x) \in \mathbb{S}$ *a probability measure,* $T_x(\cdot|s)$*, on the Borel space* $(\mathbb{R}^{d(\ell)}, \mathcal{B}(\mathbb{R}^{d(\ell)}))$*. The function* $T_x(A_\ell|(\ell, \cdot))$ *is assumed to be Borel measurable, for all* $\ell \in Loc$ *and all* $A_\ell \in \mathcal{B}(\mathbb{R}^{d(\ell)})$*;*
- $T_r : \mathcal{B}(\mathbb{R}^{d(\cdot)}) \times \mathbb{S} \times Loc \to [0, 1]$ *- is a stochastic kernel on* $\mathbb{R}^{d(\cdot)}$*, conditional on* $\mathbb{S} \times Loc$*. It assigns to each* $s \in \mathbb{S}$ *and* $\ell' \in Loc$*, a probability measure,* $T_r(\cdot|s, \ell')$*, on the Borel space* $(\mathbb{R}^{d(\ell')}, \mathcal{B}(\mathbb{R}^{d(\ell')}))$*. The function* $T_r(A_{\ell'}|(\ell, \cdot), \ell')$ *is assumed to be Borel measurable for all* $\ell, \ell' \in Loc, \ell \neq \ell'$*, and all* $A_{\ell'} \in \mathcal{B}(\mathbb{R}^{d(\ell')})$*.*

Example 1. *Fig. 1 depicts the* DTSHS $\mathcal{H}_1$ *with the set of locations* $Loc = \{\ell_0, \ell_1, \ell_2, \ell_3\}$ *and the set of atomic propositions* $\mathrm{AP} = \{\texttt{ON}_1, \texttt{ON}_2, \texttt{OFF}_1, \texttt{OFF}_2\}$*. Each location* ℓ_i *is associated with a continuous two-dimensional bounded rectangular domain* $S_{\ell_i} = [0, x_1'] \times [0, x_2'] \subset \mathbb{R}^2$ *(thus* $d(l_i) = 2$*), and is labeled with an element from* 2^{AP}*, for instance* $L(\ell_0) = \{\texttt{ON}_1, \texttt{ON}_2\}$*. The initial distribution is* $\alpha(\cdot) = \delta_{(\ell_0,0)}(\cdot)$*. Here* $\delta_{(\ell_0,0)}(\cdot)$ *is the Dirac delta function. Each continuous domain* S_{ℓ_i} *is partitioned into (the same) four non-overlapping sub-regions* G_0*,* G_1*,* G_2 *and* G_3 *(see Fig. 2). The conditional discrete stochastic kernel* T_ℓ *is given by* $T_\ell(\ell_i|(\ell, x)) = \frac{Leb(G_i)}{Leb(S_\ell)}$*, where Leb is the Lebesgue measure. The discrete graphical structure of* $\mathcal{H}_1$ *is represented in Fig. 1. An edge represents a positive transition probability between pairs of modes. In particular, each self-loop denotes the likelihood of dwelling within* G_i*, for any location* ℓ_i*. The conditional stochastic kernel* T_x *corresponds to a Gaussian distribution* $T_x(\cdot|(\ell, x)) = \mathcal{N}(\cdot; \mu(\ell, x), \Sigma(\ell, x))$*, where* $\mu(\ell, x)$ *and* $\Sigma(\ell, x)$ *are the mean and the covariance, respectively, and are functions of the hybrid state* (ℓ, x)*. For* $\ell \neq \ell'$ *the stochastic kernel* T_r*, conditional on a point* (ℓ, x)*, is given by* $T_r(\cdot|(\ell, x), \ell') = \delta_{(\ell,x)}(\cdot)$*, which denotes a (deterministic) identity map.* □

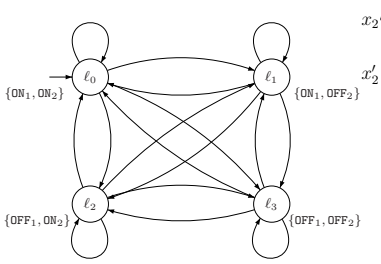

Figure 1: The discrete structure of $\mathcal{H}_1$.

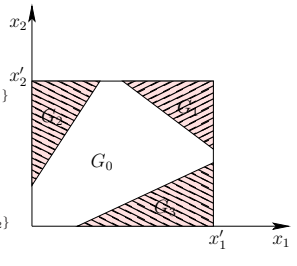

Figure 2: The (partitioned) continuous domains S_{ℓ_i} of $\mathcal{H}_1$.

Semantics.

To simplify the notation, let us introduce a conditional stochastic kernel $T : \mathcal{B}(\mathbb{S}) \times \mathbb{S} \to [0,1]$ defined by

$$T(\{\ell'\}\times A_{\ell'}\,|(\ell,x))=\begin{cases} T_x(A_{\ell'}|(\ell,x))T_\ell(\ell'|(\ell,x)), & \text{if } \ell'=\ell \\ T_r(A_{\ell'}|(\ell,x),\ell')T_\ell(\ell'|(\ell,x)), & \text{if } \ell'\neq\ell, \end{cases} \tag{1}$$

for all sets $A_{\ell'} \in \mathcal{B}(\mathbb{R}^{d(\ell')})$, $\ell' \in Loc$, and $(\ell, x) \in \mathbb{S}$. We consider the evolution of the DTSHS either over a finite time horizon $\mathbb{T} \subset \mathbb{N}$, or over an infinite one $\mathbb{T} = \mathbb{N}$. The underlying stochastic process of a DTSHS is $\{\mathbf{s}(k),\, k \in \mathbb{T}\}$, where $\mathbf{s}(k) = (\mathbf{l}(k), \mathbf{x}(k))$ represents the process at step $k \in \mathbb{T}$ (we denote processes with bold font, in order to emphasize the difference from sample points over the state space). The executions of $\{\mathbf{s}(k),\, k \in \mathbb{T}\}$ are obtained according to the following procedure [3, Definition 3]: the conditional discrete stochastic kernel T_ℓ gives the probability to jump to any location ℓ', given the current state (ℓ, x). If T_ℓ samples location $\ell' = \ell$, the conditional stochastic kernel T_x characterizes the probability for the next point inside the continuous domain S_ℓ of ℓ. If instead T_ℓ samples location $\ell' \neq \ell$, the conditional stochastic kernel T_r induces a probability distribution for the process over domain $S_{\ell'}$ for location ℓ'.

Definition 2. *[Paths] Let $\mathcal{H}$ be a* DTSHS*. An infinite path starting at state (ℓ_0, x_0) is a sequence $\rho = (\ell_0, x_0) \to (\ell_1, x_1) \to (\ell_2, x_2) \cdots$, such that for every $k \in \mathbb{N}$, $s_k = (\ell_k, x_k) \in \mathbb{S}$. A finite path is a prefix (ending in a state) of an infinite path.*

We define $Paths^{\mathcal{H}}_*$ and $Paths^{\mathcal{H}}_\omega$ as the set of all finite paths and infinite paths in $\mathcal{H}$, respectively. Let also the sets $Paths^{\mathcal{H}}$ and $Paths^{\mathcal{H}}(\ell, x)$ denote all finite and infinite paths in $\mathcal{H}$ and those starting from state (ℓ, x), respectively. For any k less than the length of path ρ, let $\rho[k] := (\ell_k, x_k)$ be the k-th state of ρ. Given a path ρ, the function $\mathbf{lab}(\rho)$ returns the word $w = a_1 a_2 a_3 \ldots$ (sequence of state labels corresponding to path ρ) such that $a_k = L(\rho[k](1))$.

A DTSHS $\mathcal{H}$ with initial probability distribution α is associated to a probability measure $\Pr^{\mathcal{H}}_\alpha$ on paths over a time horizon $[0, k], k \in \mathbb{N}$, as follows. Consider the canonical sample space $\Omega = \mathbb{S}^{k+1}$, endowed with its product topology. Let $C(G(0), G(1), \ldots, G(k))$ denote the cylinder set consisting of all paths $\rho \in Paths^{\mathcal{H}}$ such that $\rho[i] = s_i$, where $G(i) \in \mathcal{B}(\mathbb{S})$, $s_i \in G(i)$ for any $i \leq k$. The probability measure $\Pr^{\mathcal{H}}_\alpha$ on $\mathcal{B}(Paths^{\mathcal{H}})$ is the unique measure defined as: $\Pr^{\mathcal{H}}_\alpha(C(G(0), G(1), \ldots, G(k))) =$

$$\int_{G(0)} \int_{G(1)} \cdots \int_{G(k)} T(da_k|a_{k-1}) \cdots T(da_1|a_0)\alpha(da_0).$$

Notice that $\Pr^{\mathcal{H}}_\alpha(C(G(0))) = \int_{G(0)} \alpha(da_0)$. Further details on the topological and semantical properties of the DTSHS model can be found in [3].

Automata and LTL specifications.

Here we will distinguish two types of specifications: finite state automata and linear temporal logic (LTL) specifications.

Definition 3. *[*DFA*] A deterministic finite state automaton (*DFA*) is a structure $\mathcal{A} = (Q, q_0, \Sigma, F, \Delta)$, where: Q - is a finite set of locations; $q_0 \in Q$ - is the initial location; Σ - is a finite alphabet; $F \subseteq Q$ - is a set of accept locations; $\Delta : Q \times \Sigma \to Q$ - is a transition function.*

From here on we assume that $\Sigma = 2^{\mathrm{AP}}$, and let Σ^* and Σ^ω denote the set of all finite and infinite words over Σ, respectively. A finite word $w \in \Sigma^*$ is accepted by a DFA $\mathcal{A}$, if there exists a finite *run* (or a path) $\theta \in Q^*$ such that $\theta[0] = q_0$, $\Delta(\theta[i], w[i]) = \theta[i+1]$ for $i \geqslant 0$ and there exists a $j \in \mathbb{N}, j < \infty$, such that $\theta[j] \in F$. Note that $w[i]$ (resp. $\theta[i]$) denotes the i-th letter (resp. state) on w (resp. θ). The accepted language of $\mathcal{A}$, denoted $\mathcal{L}_*(\mathcal{A})$, is the set of all words accepted by $\mathcal{A}$. Notice that one could define Δ as a transition relation (as opposed to a function), which results in a nondeterministic finite state automaton (NFA). It is well known that DFAs are equally expressive as NFA and that for any NFA a canonical minimal DFA exists [16].

Definition 4. *[*GBA*] A generalized Büchi automaton (GBA) is a structure $\mathcal{A} = (Q, Q_0, \Sigma, \mathcal{F}, \Delta)$, where Q - is a finite set of locations; $Q_0 \subseteq Q$ - is a set of initial locations; Σ - is a finite alphabet; $\mathcal{F} \subseteq 2^Q$ - is a set of acceptance sets; $\Delta \subseteq Q \times \Sigma \times Q$ - is a transition relation.*

We sometimes write $q \xrightarrow{\sigma} q'$ if $(q, \sigma, q') \in \Delta$ for simplicity. An infinite *word* $w \in \Sigma^\omega$ is accepted by $\mathcal{A}$, if there exists an infinite *run* $\theta \in Q^\omega$ such that $\theta[0] \in Q_0$, $(\theta[i], w[i], \theta[i+1]) \in \Delta$ for all $i \geqslant 0$ and for each $F \in \mathcal{F}$, there exist infinitely many indices $j \in \mathbb{N}$ such that $\theta[j] \in F$. The accepted language of $\mathcal{A}$, denoted $\mathcal{L}_\omega(\mathcal{A})$, is the set of all infinite words accepted by $\mathcal{A}$. Given a GBA $\mathcal{A}$ and location q, we denote by $\mathcal{A}[q]$ the GBA $\mathcal{A}$ with q as the unique initial location. Note that $\mathcal{L}_\omega(\mathcal{A}) = \bigcup_{q \in Q_0} \mathcal{L}_\omega(\mathcal{A}[q])$.

Definition 5. *[Separated* GBA*] A* GBA $\mathcal{A}$ *is separated if, for any locations $q, q' \in Q$, $\mathcal{L}_\omega(\mathcal{A}[q']) \cap \mathcal{L}_\omega(\mathcal{A}[q'']) = \emptyset$.*

The set of LTL formulae over the set AP of atomic propositions is defined as follows:

$$\varphi ::= a \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathsf{X}\,\varphi \mid \varphi\,\mathsf{U}\,\varphi,$$

where $a \in \mathrm{AP}$. We interpret LTL formulae over DTSHS $\mathcal{H}$.

Definition 6. *[*LTL *semantics] For an* LTL *formula φ, a path $\rho \in Paths^{\mathcal{H}}$, and a step $i \in \mathbb{N}$, the satisfaction relation $\models$ is defined by:*

$$\begin{array}{lcl} (\rho,i) \models a & \iff & a \in L(\rho[i](1)) \\ (\rho,i) \models \varphi_1 \wedge \varphi_2 & \iff & (\rho,i) \models \varphi_1 \text{ and } (\rho,i) \models \varphi_2 \\ (\rho,i) \models \neg\varphi & \iff & \text{not } (\rho,i) \models \varphi \\ (\rho,i) \models \mathsf{X}\varphi & \iff & (\rho,i+1) \models \varphi \\ (\rho,i) \models \varphi_1\,\mathsf{U}\,\varphi_2 & \iff & \exists j \in \mathbb{N}.\infty > j \geq i,\ (\rho,j) \models \varphi_2 \text{ and} \\ & & \forall k \in \mathbb{N}.i \leqslant k < j,\ (\rho,k) \models \varphi_1 \end{array}$$

An example LTL formula is $a\,\mathsf{U}\,(\neg b \wedge (c\,\mathsf{U}\,d))$. Using the until operator we can define the temporal modalities $\Diamond$ and $\Box$ as $\Diamond\varphi := \mathit{true}\,\mathsf{U}\,\varphi$ and $\Box\varphi := \neg\Diamond\neg\varphi$. The operator $\Diamond\varphi$ is satisfied on all paths where eventually in the future φ holds. The operator $\Box\varphi$ characterizes all the paths that only contain states satisfying φ. The formula $\Box\Diamond\varphi$ means that φ holds infinitely often, whereas $\Diamond\Box\varphi$ means that from some moment on the formula φ will always hold.

Given a DTSHS $\mathcal{H}$, let $\mathcal{L}_\omega(\varphi) = \{\rho \in Paths^{\mathcal{H}} \mid (\rho, 0) \models \varphi\}$ be the *language* of φ in $\mathcal{H}$. The measurability of $\mathcal{L}_\omega(\varphi)$ can be proven in a similar way as in [9].

THEOREM 1. *[[8]] For any* LTL *formula* φ *over* AP*, there exists a* separated GBA $\mathcal{A}_\varphi = (Q, Q_0, \Sigma, \mathcal{F}, \Delta)$*, where* $\Sigma = 2^{\text{AP}}$ *and* $|Q| \leqslant 2^{\mathcal{O}(|\varphi|)}$*, such that* $\mathcal{L}_\omega(\mathcal{A}_\varphi)$ *is the set of computations satisfying the formula* φ*.*

Here $|\varphi|$ denotes the length of the LTL formula φ in terms of the number of operators in φ.

3. REACHABILITY ANALYSIS

This section formally introduces the following problem over a DTSHS $\mathcal{H}$: determine the probability of reaching a certain "goal" or "target" set within a given time horizon, starting from any state in $\mathbb{S}$. More precisely, select any compact Borel set $G \in \mathcal{B}(\mathbb{S})$, representing the goal set. We are interested in determining the probability that the execution associated with the initial condition $s_0 \in \mathbb{S}$ will intersect G within the time horizon $\mathbb{T}$:

$$\mathrm{p}_{s_0}(\Diamond G) := P_{s_0}\{\mathbf{s}(k) \in G \text{ for some } k \in \mathbb{T}\}, \tag{2}$$

where P_{s_0} denotes the probability measure for an event over the solution of $\mathcal{H}$, conditional on $\mathbf{s}(0) = s_0$: the value of $\mathrm{p}_{s_0}(\Diamond G)$ depends on the initial state s_0. (Notice that the measure P_{s_0} can also be expressed by $\Pr^{\mathcal{H}}$, where $G(0) = s_0$.) If $\mathrm{p}_{s_0}(\Diamond G) \geq \epsilon$, $\epsilon \in (0, 1]$, we say that the system initialized at s_0 reaches G with an ϵ probabilistic guarantee (the case $\epsilon = 0$ is trivially satisfied by all states in $\mathbb{S}$). For a given $\epsilon \in (0, 1]$, we define the *ϵ-probabilistic reachability set* by

$$R(\epsilon, G) = \{s_0 \in \mathbb{S} : \mathrm{p}_{s_0}(\Diamond G) \geq \epsilon\} \tag{3}$$

of those initial states s_0 that are associated with a process that reaches set G with an ϵ probabilistic guarantee. We show that the problem of computing $\mathrm{p}_{s_0}(\Diamond G)$ can be solved through a backward iterative procedure by representing $\mathrm{p}_{s_0}(\Diamond G)$ as a max function.

3.1 Characterizing Probabilistic Reachability

Step-bounded reachability probability.

Let us consider $\mathbb{T} = [0, N] \subset \mathbb{N}$. Let $1_C : \mathbb{S} \to \{0, 1\}$ denote the indicator function of the set $C \subseteq \mathbb{S}$: $1_C(s) = 1$ if and only if $s \in C$. Observe that $\max_{k\in[0,N]} 1_G(s_k) = 1$, if $\exists k \in [0, N] : s_k \in G$, and 0 otherwise, where $s_k \in \mathbb{S}$. Then, the quantity $\mathrm{p}_{s_0}(\Diamond G)$ in (2) can be expressed as the expectation with respect to the probability measure P_{s_0} of the Bernoulli random variable $\max_{k\in\mathbb{T}} 1_G(\mathbf{s}(k))$, conditional on $\mathbf{s}(0) = s_0$ [3]:

$$\mathrm{p}_{s_0}(\Diamond G) = E_{s_0}\left[\max_{k\in[0,N]} 1_G(\mathbf{s}(k))\right]. \tag{4}$$

Denote with $\overline{G} = \mathbb{S} \setminus G$, the complement of G over $\mathbb{S}$. Consider the sequence of functions $W_k : \mathbb{S} \times \mathcal{B}(\mathbb{S}) \to [0, 1]$, $k \in [0, N]$, defined for $s \in \mathbb{S}$ and $G \in \mathcal{B}(\mathbb{S})$ by $W_N(s, G) = 1_G(s)$, and for $k < N$:

$$\begin{aligned} W_k(s, G) \;=\; & 1_G(s) + 1_{\overline{G}}(s) \int_{\mathbb{S}^{N-k}} \max_{n=k+1,\ldots,N} 1_G(s_n) \cdot \\ & \prod_{m=k+1}^{N-1} T(ds_{m+1}|s_m) T(ds_{k+1}|s). \end{aligned} \tag{5}$$

It is easily seen that for any $k \in [0, N]$, $W_k(s, G)$ represents the probability that an execution of the DTSHS enters the target set G over the residual time horizon $[k, N]$, starting from s at time instant k [3]: we name $W_k(s, G)$ the value function at time k. In particular, $W_0(s, G) = E_s[\max_{k\in[0,N]} 1_G(\mathbf{s}(k))]$, evaluated at $s = s_0 \in \mathbb{S}$ returns the quantity of interest $\mathrm{p}_{s_0}(\Diamond G)$, and the ϵ-probabilistic reachability set defined in (3): $R(\epsilon, G) = \{s_0 \in \mathbb{S} : W_0(s_0, G) \geq \epsilon\}$.

The following result states that the value functions can be determined through a backward-recursive procedure.

THEOREM 2. *[[3], Lemma 2] The value functions* $W_k : \mathbb{S} \times \mathcal{B}(\mathbb{S}) \to [0, 1]$*, defined in* (5) *can be computed for* $s \in \mathbb{S}$ *through the following backward recursion for* $k < N$*:*

$$W_k(s, G) = 1_G(s) + 1_{\overline{G}}(s) \int_{\mathbb{S}} W_{k+1}(s_{k+1}, G) T(ds_{k+1}|s) \tag{6}$$

initialized with $W_N(s, G) = 1_G(s)$*.*

In conclusion, given an initial distribution α, the related step-bounded rechability probability is simply $\int_{\mathbb{S}} \alpha(ds) p_s(\Diamond G)$.

Step-unbounded reachability probability.

Let us consider now the case $\mathbb{T} = \mathbb{N}$. We denote by

$$\mathrm{p}^\infty_{s_0}(\Diamond G) := P_{s_0}\{\mathbf{s}(k) \in G \text{ for some } k \geq 0\} \tag{7}$$

the step-unbounded reachability probability. It can be computed as the fixpoint $W(s, G)$ of the following system of integral equations:

$$W(s, G) = 1_G(s) + 1_{\overline{G}}(s) \int_{\mathbb{S}} W(s', G) T(ds'|s). \tag{8}$$

In this case $\mathrm{p}^\infty_{s_0}(\Diamond G) = W(s_0, G)$. Notice that the map $W : \mathbb{S} \times \mathcal{B}(\mathbb{S}) \to [0, 1]$ is related to W_k as follows $W(s, G) = \lim_{k\to\infty} W_k(s, G)$, for any $s \in \mathbb{S}$.

3.2 Discretization

In most cases, the solution of Equations (6) or (8) is not analytic. In this paper we will use discretization techniques in order to approximate the solution for the time-bounded and time-unbounded reachability probability.

Consider $\mathbb{S} = \bigcup_{\ell\in Loc}\{\ell\} \times S_\ell$ and assume each S_ℓ is compact. We introduce a finite partition for each domain $S_\ell \subset \mathbb{R}^{d(\ell)}$, $\ell \in Loc$, by taking $S_\ell = \bigcup_{i=1}^{m_\ell} S_{\ell,i}$, where $S_{\ell,i} \in \mathcal{B}(\mathbb{R}^{d(\ell)})$ with $S_{\ell,i} \cap S_{\ell,j} = \emptyset$, for all $i \neq j$. Here m_ℓ represents the finite number of partitions for the domain in location ℓ. Denote by $h_{\ell,i}$ the diameter of the set $S_{\ell,i}$ as $h_{\ell,i} = \sup\{||x - x'|| : x, x' \in S_{\ell,i}\}$ (here we are using the Euclidean norm), and define the grid size parameter by $h := \max_{i=1,\ldots,m_\ell;\ell\in Loc} h_{\ell,i}$. Let us additionally introduce a function $r_\ell : \mathcal{B}(\mathbb{R}^{d(\ell)}) \to \mathbb{R}^{d(\ell)}$ which, given a partition set $S_{\ell,i} \in \mathcal{B}(\mathbb{R}^{d(\ell)})$ and location $\ell \in Loc$, returns a randomly chosen point in $S_{\ell,i}$, denoted with $r_\ell(S_{\ell,i})$, which is also named the "representative point" of the partition set $S_{\ell,i}$. Notice that the discretization can in general be tailored to the target set G, so that $G = \bigcup_{i=1}^{m^g_\ell} S^g_{\ell,i}$, where $\forall \ell \in Loc, m^g_\ell \leq m_\ell$. Using the grid size parameter h we can define the discretized DTMC of a DTSHS as follows:

DEFINITION 7. *[DTMC approximation of DTSHS] For the* DTSHS $\mathcal{H} = (Loc, \text{AP}, L, d, \alpha, T_x, T_\ell, T_r)$*, the* DTMC $\mathcal{D}_h = (\mathbb{S}_h, \text{AP}, L_h, \alpha_h, P_h)$ *is defined as follows:* $\mathbb{S}_h = \{(\ell, i)|\ell \in Loc, i \in \{1, \ldots, m_\ell\}\}$ *- is the state space;* $L_h(\ell, i) = L(\ell)$ *- is the labeling function;* $\alpha_h(\ell, i) = \int_{S_{\ell,i}} \alpha(\ell, x)dx$ *- is the*

initial probability distribution; $P_h((\ell,i),(\ell',i')) = T(\ell' \times S_{\ell',i'}|(\ell, r_\ell(S_{\ell,i})))$ *- is the transition probability matrix.*

Notice that the state space $\mathbb{S}_h$ of the discretized DTMC $\mathcal{D}_h$ is given by pairs (location, partition index). The probability $P_h((\ell,i),(\ell',i'))$ to jump from state (ℓ,i) to state (ℓ',i') is the probability to jump from $r_\ell(S_{\ell,i})$, the representative point of partition $S_{\ell,i}$, to the partition set $S_{\ell',i'}$ in location ℓ'.

Let us denote with $G_h \in \mathbb{S}_h$ the set of states of $\mathcal{D}_h$ corresponding to partitions of $\mathbb{S}$ overlapping with the original target set G of $\mathcal{H}$. Similarly, $\overline{G_h} = \mathbb{S}_h \setminus G_h$. We define the step-bounded and step-unbounded reachability probabilities by introducing functions W_k^h and W^h respectively, both of which are defined on $\mathbb{S}_h \times \mathcal{B}(\mathbb{S}_h)$ and take value in $[0,1]$:

$$W_k^h(v,G_h)=1_{G_h}(v)+1_{\overline{G_h}}(v)\sum_{v_{k+1}\in\mathbb{S}_h} W_{k+1}^h(v_{k+1},G_h)P_h(v,v_{k+1}), \tag{9}$$

for $k < N$, initialized with $W_N^h(v,G_h) = 1_{G_h}(v)$ and

$$W^h(v,G_h) = 1_{G_h}(v) + 1_{\overline{G_h}}(v)\sum_{v'\in\mathbb{S}_h} W^h(v',G_h)P_h(v,v'). \tag{10}$$

W_k^h and W^h approximate the original functions W_k and W – in the next Section we derive explicit approximation bounds.

Notice that step-bounded and step-unbounded reachability probability is given by a system of linear equations for which solutions can be computed efficiently. If $\alpha_h(v_0) = 1$, the solutions to Eq. (9) and (10) will be denoted as $\widehat{p}_{v_0}(\Diamond G_h)$ and $\widehat{p}^{\infty}_{v_0}(\Diamond G_h)$, respectively, whereas for an arbitrary initial distribution α_h we get $\sum_{v\in\mathbb{S}_h}\alpha_h(v)\widehat{p}_v(\Diamond G_h)$ and $\sum_{v\in\mathbb{S}_h}\alpha_h(v)\widehat{p}^{\infty}_v(\Diamond G_h)$, respectively.

3.3 Error Bounds

The quantities $W_k^h(v,G_h), W^h(v,G_h), \widehat{p}_v(\Diamond G_h)$, and $\widehat{p}^{\infty}_v(\Diamond G_h)$ are all defined on $\mathbb{S}_h$. We can extend them over $\mathbb{S}$ by piecewise constant interpolation – for instance, $W_k^h(s,G_h) = W_k^h(r_\ell(S_{\ell,i}),G_h), \forall s \in S_{\ell,i}, i = 1,\ldots,m_\ell, \ell \in Loc$. In the remaining of this section, we shall refer to the quantities extended over $\mathbb{S}$. We now derive explicit error bounds between the quantities in Equations (6)-(8) and the corresponding quantities in Equations (9)-(10) (again, extended over $\mathbb{S}$).

We assume that the kernels T_ℓ, as well as the densities t_x and t_r of T_x and T_r, satisfy the following Lipschitz continuity assumptions:

Assumption 1. *For any* $(\ell,x),(\ell,x'),(\ell,x''),(\ell',x'') \in \mathbb{S}$*:*

$$|T_\ell(\ell'|(\ell,x)) - T_\ell(\ell'|(\ell,x'))| \le h_1||x-x'||,$$
$$|t_x(x''|(\ell,x)) - t_x(x''|(\ell,x'))| \le h_2||x-x'||,$$
$$|t_r(x''|(\ell,x),\ell') - t_r(x''|(\ell,x'),\ell')| \le h_3||x-x'||,\ \ell \neq \ell',$$

where h_1*,* h_2 *and* h_3 *are finite Lipschitz constants.*

We define $\mathcal{K} \doteq |Loc|h_1 + \lambda(\overline{G})\cdot(h_2 + (|Loc|-1)h_3)$, where $\lambda(\overline{G})$ is the Lebesgue measure of the set $\overline{G}$ and $|Loc|$ is the number of discrete locations.

Theorem 3. *Given a* DTSHS $\mathcal{H}$*, the* DTMC $\mathcal{D}_h$ *obtained with discretization step* h*, a finite time horizon* N *and a target set* $G \in \mathcal{B}(\mathbb{S})$*, the following holds:*

1) $|p_{s_0}(\Diamond G) - \widehat{p}_{v_0}(\Diamond G_h)| \le N\mathcal{K}h$,

2) $|p^{\infty}_{s_0}(\Diamond G) - \widehat{p}^{\infty}_{v_0}(\Diamond G_h)| \le 2\mathcal{K}h$,

where $v_0 = (\ell,i)$ *and* $s_0 \in G_{\ell,i}$.

4. AUTOMATA MODEL CHECKING

In this section we study the problem of model checking a property specified as a DFA or as a separated GBA against a DTSHS. Recall that the main difference between a DFA-property and a separated GBA-property is that the former reasons over the finite paths whereas the latter reasons over infinite paths. Since every LTL-formula φ can be expressed as a separated GBA (see Section 2), LTL model checking boils down to automata model checking. Let the quantity $\Pr^{\mathcal{H}}(\mathcal{L}(\mathcal{A})) := \Pr^{\mathcal{H}}(\rho \in Paths^{\mathcal{H}}_f | \mathbf{lab}(\rho) \in \mathcal{L}(\mathcal{A}))$ (and $\Pr^{\mathcal{H}}(\mathcal{L}_\omega(\mathcal{B})) := \Pr^{\mathcal{H}}(\rho \in Paths^{\mathcal{H}}_\omega | \mathbf{lab}(\rho) \in \mathcal{L}_\omega(\mathcal{B}))$) denote the probability that the DTSHS $\mathcal{H}$ satisfies the DFA $\mathcal{A}$ (and GBA $\mathcal{B}$, respectively). The measurability of the sets $\{\rho \in Paths^{\mathcal{H}}_f | \mathbf{lab}(\rho) \in \mathcal{L}(\mathcal{A})\}$ and $\{\rho \in Paths^{\mathcal{H}}_\omega | \mathbf{lab}(\rho) \in \mathcal{L}_\omega(\mathcal{B})\}$ can be shown as in [19]. We will show that the probability of these events can be computed over the product between $\mathcal{H}$ and $\mathcal{A}$ (and $\mathcal{B}$).

DFA Specifications.

We start considering properties expressed as DFA.

Definition 8. *[Product between* DTSHS *and* DFA*] Consider a* DTSHS $\mathcal{H} = (Loc, \mathrm{AP}, L, d, \alpha, T_x, T_\ell, T_r)$ *and a* DFA $\mathcal{A} = (Q, q_0, \Sigma, F, \Delta)$*. Let* $\mathcal{H}\otimes\mathcal{A} = (V, \mathrm{AP}, \widehat{L}, \widehat{\alpha}, \widehat{d}, \widehat{T}_x, \widehat{T}_\ell, \widehat{T}_r)$ *be the product* DTSHS*, where* $V := Loc \times Q$*,* $\widehat{L}(\langle\ell,q_0\rangle) = L(\ell)$*,* $\widehat{\alpha}(\langle\ell,q_0\rangle,x) := \alpha(\ell,x)$*,* $\widehat{d}(\langle\ell,q\rangle) := d(\ell)$ *and the kernels are defined by:*

$$\frac{T_\ell(\ell'|(\ell,x)) = p \ \wedge\ \Delta(q,L(\ell)) = q'}{\widehat{T}_\ell(\langle\ell',q'\rangle|(\langle\ell,q\rangle,x)) = p},$$

$$\frac{T_x(A_\ell|(\ell,x)) = p \ \wedge\ \Delta(q,L(\ell)) = q'}{\widehat{T}_x(A_{\langle\ell,q'\rangle}|(\langle\ell,q\rangle,x)) = p},$$

$$\frac{T_r(A_{\ell'}|(\ell,x),\ell') = p \ \wedge\ \Delta(q,L(\ell)) = q'}{\widehat{T}_r(A_{\langle\ell',q'\rangle}|(\langle\ell,q\rangle,x),\langle\ell',q'\rangle) = p}(\ell \neq \ell').$$

Here $A_{\langle\ell,q'\rangle}$ and $A_{\langle\ell',q'\rangle}$ denote the Borel-measurable sets in $S_{\langle\ell,q'\rangle}$ and $S_{\langle\ell',q'\rangle}$, respectively. The definition of the conditional stochastic kernel $\widehat{T}$ for the product $\mathcal{H}\otimes\mathcal{A}$ is the same as in Eq. (1). We define the set of final locations of $\mathcal{H}\otimes\mathcal{A}$ as $V_F := Loc \times F$.

Theorem 4. *For any* DTSHS $\mathcal{H}$ *and* DFA $\mathcal{A}$*,*

$$\Pr^{\mathcal{H}}(\mathcal{L}(\mathcal{A})) = \Pr^{\mathcal{H}\otimes\mathcal{A}}(\Diamond V_F),$$

where $\Pr^{\mathcal{H}\otimes\mathcal{A}}(\Diamond V_F)$ *is the probability to reach the set of final locations* V_F *in the product* $\mathcal{H}\otimes\mathcal{A}$*.*

Given the fact that $\mathcal{H}\otimes\mathcal{A}$ is a DTSHS, the probability $\Pr^{\mathcal{H}\otimes\mathcal{A}}(\Diamond V_F)$ can be computed via Eq. (6). In this case, $\Pr^{\mathcal{H}\otimes\mathcal{A}}(\Diamond V_F)$ is the fixpoint of Eq. (8). Notice that in order to make the computation of $\Pr^{\mathcal{H}\otimes\mathcal{A}}(\Diamond V_F)$ more efficient we can make all the states corresponding to the set of locations V_F absorbing.

GBA Specifications.

In order to compute the probability that a DTSHS $\mathcal{H}$ satisfies a separated GBA-property $\mathcal{A}$ we consider two steps. First, we construct the product between $\mathcal{H}$ and the separated GBA $\mathcal{A}$. Second, in the product $\mathcal{H}\otimes\mathcal{A}$ we compute the probability $\Pr^{\mathcal{H}}(\mathcal{L}_\omega(\mathcal{A}))$.

Definition 9. *[Product between* DTSHS *and* GBA*] Consider a* DTSHS $\mathcal{H} = (Loc, \mathrm{AP}, L, d, \alpha, T_x, T_\ell, T_r)$ *and a* GBA $\mathcal{A} = (Q, Q_0, \Sigma, \mathcal{F}, \Delta)$*. Their product is defined as* $\mathcal{H} \otimes \mathcal{A} = (V, \mathrm{AP}, \widehat{L}, \widehat{\alpha}, \widehat{d}, \widehat{T}_x, \widehat{T}_\ell, \widehat{T}_r)$ *and is constructed as in Definition 8, except that* $\widehat{\alpha}(\langle \ell, q_0 \rangle, x) := \alpha(\ell, x)$ *for all* $q_0 \in Q_0$*.*

In general when one takes the product between a generalized *deterministic* Büchi automaton (GDBA) and a DTSHS, the resulting product is a DTSHS. The product between a generalized (nondeterministic) Büchi automaton (GBA) and a DTSHS is not always a DTSHS. This can be seen from the fact that for a location q in $\mathcal{A}$ and a symbol $\sigma \in \Sigma$, $\{(q, \sigma, q'), (q, \sigma, q'')\} \subseteq \Delta$ for $q' \neq q''$, it follows that for a transition $\ell \to \ell'$ in $\mathcal{H}$ with $T_\ell(\ell' | (\ell, x)) = 1$ the product will contain two transitions: $\langle \ell, q \rangle \to \langle \ell', q' \rangle$ and $\langle \ell, q \rangle \to \langle \ell', q'' \rangle$. In this case we get that $\widehat{T}_\ell(\langle \ell', q' \rangle | (\langle \ell, q \rangle, x)) + \widehat{T}_\ell(\langle \ell', q'' \rangle | (\langle \ell, q \rangle, x)) = 2$. In this paper we consider GBA, which are strictly more expressive than GDBA [4]. The separability property will give us the possibility to transform the product into a DTSHS.

Example 2. *Fig. 5 shows the product* $\mathcal{H} \otimes \mathcal{A}$ *between the* DTSHS $\mathcal{H}$ *of Fig. 3 and the separated* GBA $\mathcal{A}$ *of Fig. 4. (For each location of the* DTSHS $\mathcal{H}$ *we pick a continuous kernel* T_x *and kernel* T_r *– they can for instance be a conditional exponential or Gaussian distribution.) Notice that the product in its original form does not define a* DTSHS *as the automaton* $\mathcal{A}$ *is nondeterministic (all dashed transitions in Fig. 5 are nondeterministic). For instance in the product location* v_0 *there are two transitions to the dashed product locations* v_1 *and* v_2*. To each product locations* v_1 *and* v_2 *corresponds the location* ℓ_0 *from the* DTSHS $\mathcal{H}$*.*

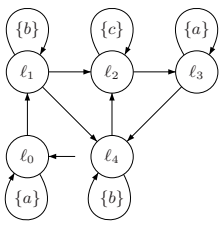

Figure 3: DTSHS $\mathcal{H}$ for Example 2.

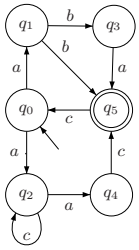

Figure 4: Separated GBA $\mathcal{A}$ for Ex. 2.

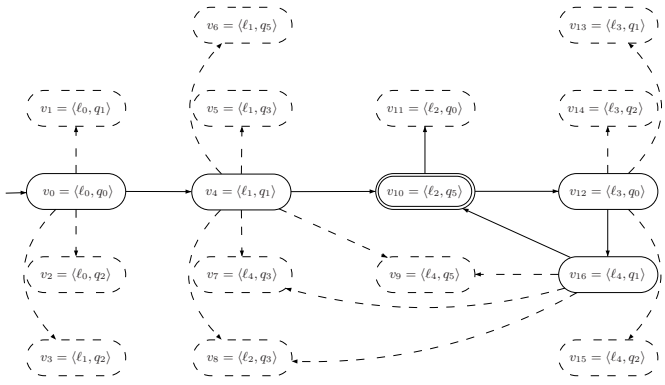

Figure 5: Product $\mathcal{H} \otimes \mathcal{A}$ for Example 2.

In order to compute the probability $\Pr^{\mathcal{H}}(\mathcal{L}_\omega(\mathcal{A}))$, we consider the probability to reach an *accepting bottom strongly connected component* (aBSCC) in the product $\mathcal{H} \otimes \mathcal{A}$. A *strongly connected component* (SCC) is a strongly connected set of discrete locations such that no proper superset is strongly connected.(The notion of SCC is related to that of irreducible class for classical Markov chains.) A *bottom strongly connected component* (BSCC) is an SCC from which no location outside the SCC is reachable.

Definition 10. *[a*BSCC*] Given the product* $\mathcal{H} \otimes \mathcal{A}$*, a* BSCC $B \subseteq V = Loc \times Q$ *is accepting if for all* $F \in \mathcal{F}$ *of* $\mathcal{A}$*, there exists some* $\langle \ell, q \rangle \in B$ *such that* $q \in F$*.*

Let the set of final locations be $V_F^\omega = \{v \in B \mid B \text{ in the set of all } a\text{BSCC in } \mathcal{H} \otimes \mathcal{A}\}$.

Now the task is to compute $\Pr^{\mathcal{H}}(\mathcal{L}_\omega(\mathcal{A}))$. Using the separability property of GBA $\mathcal{A}$ we obtain a DTSHS out of $\mathcal{H} \otimes \mathcal{A}$. The following lemma asserts that for each accepted word of the separated GBA $\mathcal{A}$ there exists a single accepting path in $\mathcal{H} \otimes \mathcal{A}$.

We say that from location $\langle \ell, q \rangle$ there is a path leading to a aBSCC B, if there is a sequence $\langle \ell_0, q_0 \rangle, \langle \ell_1, q_1 \rangle, \ldots, \langle \ell_n, q_n \rangle$ such that $\langle \ell, q \rangle = \langle \ell_0, q_0 \rangle$, $\langle \ell_i, q_i \rangle$ and $\langle \ell_{i+1}, q_{i+1} \rangle$ are connected (if there exists $G' \subseteq \mathbf{dom}(\langle \ell_i, q_i \rangle) \backslash \{\emptyset\}$ such that for all $x \in G'$, $\widehat{T}((\langle \ell_{i+1}, q_{i+1} \rangle, \cdot) | (\langle \ell_i, q_i \rangle, x)) > 0$) for $0 \leqslant i < n$ and $\langle \ell_n, q_n \rangle \in B$.

Lemma 1. *Consider the product* $\mathcal{H} \otimes \mathcal{A}$*, where* $\mathcal{A}$ *is a separated* GBA*. For any a*BSCC B *of the product* $\mathcal{H} \otimes \mathcal{A}$*, it holds that*

1. $\langle \ell, q \rangle \to \langle \ell', q' \rangle$ *and* $\langle \ell, q \rangle \to \langle \ell', q'' \rangle$ *implies* $q' = q''$*, for any* $\langle \ell, q \rangle, \langle \ell', q' \rangle, \langle \ell', q'' \rangle$ *in* B*;*
2. *if* $\langle \ell, q \rangle$ *and* $\langle \ell, q' \rangle$ *with* $q \neq q'$ *have a path leading to* B *then* $q = q'$*.*

Using the above lemmas we can conclude that each location of $\mathcal{H} \otimes \mathcal{A}$ that does not lead to an aBSCC can be safely removed. The resulting product is denoted $\mathcal{H} \underline{\otimes} \mathcal{A}$. With reference to Example 2, by removing all dashed transitions and dashed locations in Fig. 5 we obtain the DTSHS $\mathcal{H} \underline{\otimes} \mathcal{A}$.

In general, when searching for an aBSCC one relies on the topological discrete structure (which hinges on the conditional discrete stochastic kernels) of $\mathcal{H} \underline{\otimes} \mathcal{A}$. Still, an aBSCC in $\mathcal{H} \underline{\otimes} \mathcal{A}$ might not be accepting. To illustrate this fact, consider the product $\mathcal{H} \underline{\otimes} \mathcal{A}$ from Fig. 6 and the set of accepting conditions $\mathcal{F} = \{\{q_0\}, \{q_1\}\}$. It is easy to see that when the conditions $\widehat{T}((v_1, \cdot) | (v_0, x)) > 0$ and $\widehat{T}((v_0, \cdot) | (v_1, y)) > 0$ are satisfied for every $x \in \mathbb{R}^{d(v_0)}$ and $y \in \mathbb{R}^{d(v_1)}$ then the set $B = \{v_0, v_1\}$ is an aBSCC. However, let us now assume that the domain S_0 from Fig. 7 is associated to location v_0. The domain S_0 contains two subdomains G_1 and G_2, which are such that $\widehat{T}(v_0 \times S | (v_0, x)) = 0$ and $\widehat{T}((v_1, \cdot) | (v_0, x)) = 0$, for all $x \in G_1 \cup G_2$ and $S \subseteq S_0 \backslash (G_1 \cup G_2)$. This means that when we are in the subdomain G_1 or G_2 there is no way to jump back to $S_0 \backslash (G_1 \cup G_2)$, nor to jump to location v_1. As a result we get that the aBSCC B is not accepting. This example suggests that when searching for accepting BSCCs it is not enough to look at the conditional discrete stochastic kernels — one has to consider also the continuous stochastic kernels.

Given an aBSCC B in $\mathcal{H} \underline{\otimes} \mathcal{A}$ and a set of accepting conditions $\mathcal{F}$ we introduce $acc(B) = \{\langle \ell, q \rangle \in B | , q \in F \in \mathcal{F}\}$,

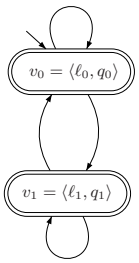

Figure 6: Product $\mathcal{H} \underline{\otimes} \mathcal{A}$ with aBSCC.

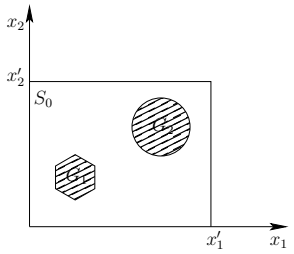

Figure 7: Domain with two absorbing subregions: the aBSCC may not be accepting.

the function returning the set of accepting locations in the aBSCC B. For a given set of states $G \subseteq \mathbb{S}$ we define the random variable $\eta(G) = \sum_{k=0}^{\infty} 1_G(\mathbf{s}(k))$, where $\mathbf{s}(k)$ is the stochastic process associated with $\mathcal{H} \underline{\otimes} \mathcal{A}$, and $\mathbb{E}_s(\eta(G))$ is the expected value of $\eta(G)$ over all executions of $\mathbf{s}(k)$ starting from $\mathbf{s}(0) = s$.

DEFINITION 11. *[Recurrent aBSCC] An aBSCC B is recurrent if for the set $G = \{v \times G' | v \in acc(B), G' \subseteq \mathbf{dom}(v)\}$, $\mathbb{E}_s(\eta(G)) = \infty$, for all $s \in G$.*

Here recall that $\mathbf{dom}(v)$ denotes the domain associated to location v. The above definition says that every state from G can reach all other states in G infinitely often.

In order to check whether an aBSCC is recurrent one has to look at the conditional stochastic kernel $\widehat{T}$. For instance, in Fig. 7 one has to find all possible subsets G_i, $i > 0$, of the domain S_0, such that $\widehat{T}(v_0 \times S_0 \backslash (\cup_{i>0} G_i) | (v_0, x)) = 0$, $x \in G_i$. This is equivalent to searching for all absorbing regions S' of the domain S_0. In case one such region S' does exist, one can assign a new location v' to the absorbing region S' and a transition $v \to v'$, such that v' has the domain S' and v has the new absorbing domain $S_0 \backslash S'$. In general searching for absorbing regions is hard as one has to analyse the kernel $\widehat{T}$ for every x (uncountable many) in a continuous domain S. We propose to solve the problem of absorbing regions by discretizing the aBSCC into a DTMC and then searching for absorbing states. Notice that the discretization approach will not guarantee the absence of absorbing states as it relies on the size of the discretization step.

THEOREM 5. *For any separated* GBA $\mathcal{A}$ *and* DTSHS $\mathcal{H}$*:*

$$\Pr^{\mathcal{H}}(\mathcal{L}_\omega(\mathcal{A})) = \Pr^{\mathcal{H} \underline{\otimes} \mathcal{A}}(\Diamond V_F^\omega).$$

Notice that for the above theorem we only need to compute the probability to reach a set of absorbing final locations V_F^ω. This is enough due to the fact that as long as we are in an aBSCC the DTSHS $\mathcal{H}$ satisfies the GBA-property $\mathcal{A}$ with probability one.

5. CASE STUDY

In this section, we will show the applicability of our theoretical results to a case study.

5.1 Model Description

The following computational study [2] considers a model for the temperature evolution in a building with two rooms. Both rooms are equipped with a heater and each heater switches between the `ON` and `OFF` conditions depending on the temperature in the corresponding room. The state of the system is hybrid, with the discrete state component representing the status of the two heaters and the continuous state component representing the temperature in each of the two rooms. The discrete state space is given by $Loc = \{\texttt{ON}, \texttt{OFF}\}^2$. The allowed transitions between the locations are depicted in Fig. 1. The continuous state space is $\mathbb{R}^2$, irrespectively of the discrete state value (that is, $d(\ell) = 2, \forall \ell \in Loc$).

We suppose that the temperature of each room, say room i, evolves according to the following stochastic difference equation (SDE):

$$\begin{aligned} \mathbf{x}_i(k+1) \;=\; & \mathbf{x}_i(k) + b_i(x_a - \mathbf{x}_i(k)) + a_{ij, j \neq i}(\mathbf{x}_j(k) - \mathbf{x}_i(k)) \\ & + c_i 1_{Loc_i}(\ell(k)) + \mathbf{w}_i(k), \end{aligned}$$

where x_a represents the ambient temperature (assumed to be constant and equal for both rooms) and $1_{Loc_i}(\cdot)$ is the indicator function of set $Loc_i = \{(\ell_1, \ell_2) \in Loc : \ell_i = \texttt{ON}\}$. The quantities b_i, a_{ij}, and c_i are non-negative real constants representing the heat transfer rate from room i to the ambient (b_i) and to room $j \neq i$ (a_{ij}), and the heat rate supplied to room i by the heater in room i (c_i). The disturbance $\{\mathbf{w}_i(k),\, k = 0, \ldots, N\}$ affecting the temperature evolution in room i is assumed to be a sequence of independent identically distributed Gaussian random variables with zero mean and variance ν^2. Furthermore, with no loss of generality we suppose that the disturbances $\mathbf{w}_i$ and $\mathbf{w}_j$ affecting the temperature of different rooms ($i \neq j$) are independent.

The continuous transition kernel T_x describing the evolution of the continuous state $x = (x_1; x_2)$ can be easily derived from the SDE above. $T_x : \mathcal{B}(\mathbb{R}^2) \times \mathcal{S} \to [0, 1]$ can be expressed as

$$T_x(\cdot \,|(\ell, x)) = \mathcal{N}(\cdot; x + Zx + \Gamma(\ell), \nu^2 I), \tag{11}$$

where $Z \in \mathbb{R}^{2 \times 2}$, $\Gamma(\ell) \in \mathbb{R}^2$, and $I \in \mathbb{R}^{2 \times 2}$ is the identity matrix. For $i = 1, 2$, the element in row i and column j of matrix Z is given by $[Z]_{ij} = a_{ij}$, if $j \neq i$, and $[Z]_{ij} = -(b_i + \sum_{k \neq i, k \in Loc} a_{ik})$, if $j = i$. For $i = 1, 2$, the i^{th} element of vector $\Gamma(\ell)$, $\ell = (\ell_1, \ell_2) \in Loc$, is given by $[\Gamma(\ell)]_i = b_i x_a + c_i$, if $\ell_i = \texttt{ON}$, and $[\Gamma(\ell)]_i = b_i x_a$, if $\ell_i = \texttt{OFF}$. The reset kernel is set to coincide with the transition kernel in the current mode, irrespectively of the status to which the heaters possibly switch: $T_r(\cdot \,|(\ell, x), \ell') = T_x(\cdot \,|(\ell, x))$, for any $\ell, \ell' \in Loc$, and any $x \in \mathbb{R}^2$.

As for the discrete state evolution, we suppose that each heater switches status based on the temperature of the corresponding room, and independently of the other heater. This is modeled taking the discrete transition kernel $T_\ell : Loc \times \mathcal{S} \to [0, 1]$ as the product of two conditional stochastic kernels $T_{\ell,i} : \{\texttt{ON}, \texttt{OFF}\} \times (\{\texttt{ON}, \texttt{OFF}\} \times \mathbb{R}) \to [0, 1]$ governing the switching of each heater i. More precisely, we set

$$T_\ell(\ell' | (\ell, x)) = \prod_{i=1}^{2} T_{\ell,i}(\ell_i' | (\ell_i, x_i)), \tag{12}$$

$\ell = (\ell_1, \ell_2)$, $\ell' = (\ell_1', \ell_2') \in Loc$, $x = (x_1, x_2) \in \mathbb{R}^2$, where

$$T_{\ell,i}(\ell_i' | (\ell_i, x_i)) = \begin{cases} \sigma_i(x_i), & \ell_i' = \texttt{OFF}, \\ 1 - \sigma_i(x_i), & \ell_i' = \texttt{ON} \end{cases} \tag{13}$$

with $\sigma_i : \mathbb{R} \to [0,1]$ a sigmoidal function given by

$$\sigma_i(y) = \frac{y^{d_i}}{\alpha_i^{d_i} + y^{d_i}},\ y \in \mathbb{R}. \tag{14}$$

Function $\sigma_i(y)$, $y \in \mathbb{R}$, is parameterized by a "threshold" parameter α_i and a "steepness" parameter $d_i > 0$. α_i is the value of y at which the probability of the heater changing status becomes equal to 0.5, whereas d_i is related to the slope of the sigmoidal function at $y = \alpha_i$ (which amounts to $d_i/(4\alpha_i)$). We shall refer to the three possible values for the steepness parameter d_i respectively as $d_i = 1$ (*flat*), $d_i = 10$ (*gradual*), and $d_i = 100$ (*steep*), in increasing order. The values for the threshold α_i are determined as a convex combination of the temperatures x_i^l and x_i^u, $x_i^l < x_i^u$, defining the desired temperature range $[x_i^l, x_i^u]$ in room i.

5.2 Property Specification

We will consider two properties. The first one is a DFA and the second one is an LTL-formula expressed as a GBA. Recall that the difference between a DFA property and an LTL-formula is that the former reasons over the finite paths whereas the latter reasons over the infinite paths.

DFA property.

The property specified as a DFA $\mathcal{A}$ is depicted in Fig. 8.

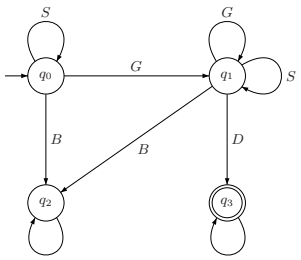

Figure 8: DFA $\mathcal{A}$.

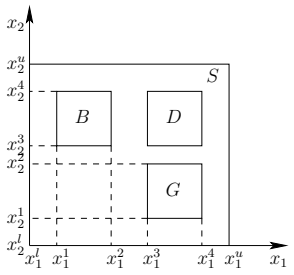

Figure 9: Domains for DFA $\mathcal{A}$ of Fig. 8.

Intuitively, $\mathcal{A}$ describes all the paths, the continuous part of which can reach the region labeled with D (see Fig. 9) by first visiting the region labeled with G while avoiding the regions labeled with B. Region S is given by $([x_1^l, x_1^u] \times [x_2^l, x_2^u]) \backslash (G \cup B \cup D)$. Notice that no equivalent CTL formula can be formulated for property $\mathcal{A}$.

We specify the heating system as a DTSHS $\mathcal{H}$ with 16 locations: to every subset S, G, D and B of each continuous domain we assign a location, each of which has the conditional discrete stochastic kernel T_ℓ specified as in Fig. 1 and Eq. (13). The parameter d_i is taken to be equal to 10 (gradual) and the parameter α_i is equal to $\frac{1}{4}x_i^l + \frac{3}{4}x_i^u$ for $i \in \{1,2\}$. The regions within the continuous domains are specified by the parameters from Table 1. The set of atomic propositions is $\mathrm{AP} = \{S, G, D, B\}$. Every location is labeled with a single element from the set AP. The continuous transition kernels T_x and R are given by Eq. (11), and depend on the parameters $a_{12} = a_{21} = 0.25$, $b_1 = b_2 = 0.1$, $c_1 = 2.6$, $c_2 = 2.4$, $x_a = 6$ and $\nu = 0.5$. We partition the continuous domains $[x_1^l, x_1^u] \times [x_2^l, x_2^u]$ into square regions, uniformly dividing each interval $[x_1^l, x_1^u]$ into l slots. We leverage the discretization technique from Section 3.2 in order to obtain the discretized DTMC from the product $\mathcal{H} \otimes \mathcal{A}$. The DTMC

$x_1^l \backslash x_2^l$	$x_1^1 \backslash x_2^1$	$x_1^2 \backslash x_2^2$	$x_1^3 \backslash x_2^3$	$x_1^4 \backslash x_2^4$	$x_1^u \backslash x_2^u$
10\10	15\15	20\20	25\25	30\30	35\35

Table 1: Parameters characterizing continuous domains.

is highly connected, namely most of the transition probabilites are non zero. The results reported in this section refer to computations performed on a AMD Athlon 64 Dual Core Processor with 2GB RAM. The product construction and the discretization algorithm were implemented in MATLAB. Table 2 shows the verification time and the DTMC

Slots l	5	10	20
DTMC states	400	1600	6400
Time (sec)	29.5	466.7	5694.6

Table 2: Verification time for the DFA $\mathcal{A}$ in (Fig. 8) over the DTMC obtained from the DTSHS $\mathcal{H}$.

size for different number of slots. The obtained verification times critically depend on the discretization procedure, rather than the model checking algorithms: the time spent on the product construction and solving the system of linear equations is much smaller compared to the time spent for the generation of the DTMC. Fig. 10 displays the probability that the two-room DTSHS satisfies the DFA property $\mathcal{A}$ given that the initial location is $(\texttt{OFF}, \texttt{OFF})$ and the continuous state is chosen in any of the 4 domains S, G, B and D. (The surface is obtained at the representative points.) The number of discretization slots l is 10. A similar plot is reported on Fig. 11 in 2D for a parameter choice of d_i of 100 (steep) and of α_i of $\frac{1}{2}x_i^l + \frac{1}{2}x_i^u$, respectively — all other parameters are as before. Here warmer colors denote higher probabilities. In both the described instances, the probability is higher for all the states starting from the domain G or nearby. This is due to the fact that the property $\mathcal{A}$ is satisfied only for the paths of DTSHS that reach D by starting anywhere in G or S and having crossed G.

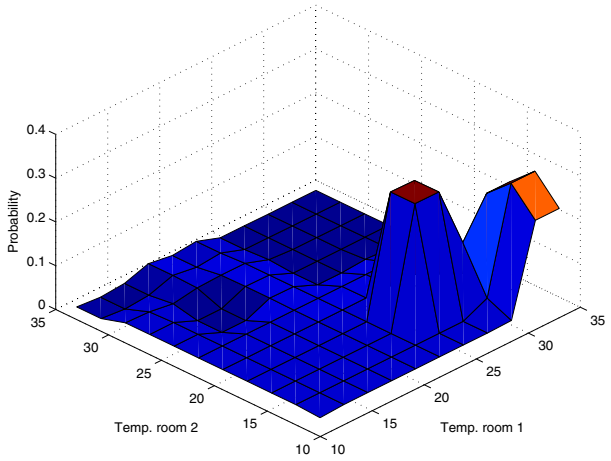

Figure 10: Satisfiability probability for the DFA $\mathcal{A}$ over the DTSHS $\mathcal{H}$ (through its DTMC discretization), with the first set of parameters.

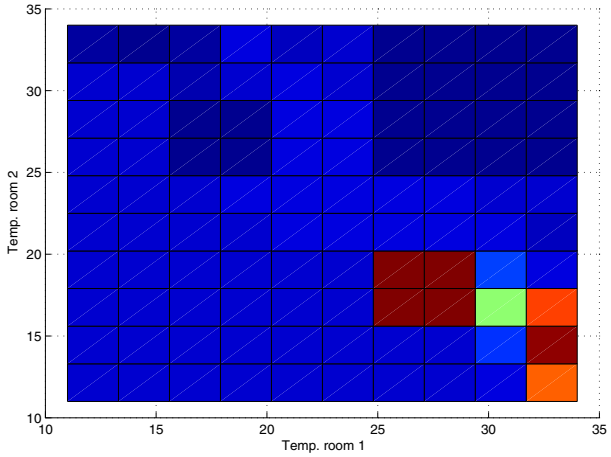

Figure 11: 2D plot for the satisfiability probability for the DFA $\mathcal{A}$ over the DTSHS $\mathcal{H}$ (through its DTMC discretization), with the second set of parameters.

LTL - formula.

We consider the formula $\varphi = \Diamond\Box(D \wedge \neg S \wedge \neg F)$ on the set of atomic propositons AP $= \{S, D, F\}$ and sets $S = [x_1^l, x_1^u] \times [x_2^l, x_2^u]$ and $D = [x_1^l, x_1^m] \times [x_2^l, x_2^m]$, where $x_i^m = \frac{x_i^u + x_i^l}{2}$, $i \in \{1, 2\}$. The formula signifies that all paths should eventually reach domain D and then stay there forever.

We compute the satisfiability probability of the formula φ on the DTSHS $\mathcal{H}_2$ modeling the two-room heating benchmark, where we consider a slightly different discrete structure, as specified in Fig. 12. For all locations Loc of the

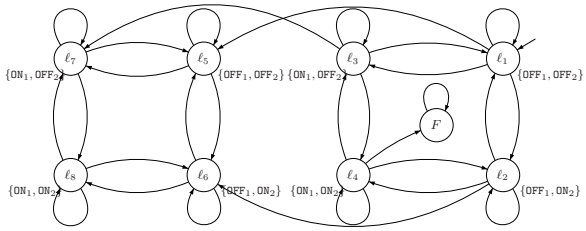

Figure 12: Discrete structure of the DTSHS $\mathcal{H}_2$.

DTSHS $\mathcal{H}_2$, the behavior of the discrete stochastic kernel T_ℓ is defined in Eq. (12). The kernels T_ℓ, T_x and T_r for locations $Loc \backslash \{\ell_4\}$ are normalized, whereas in ℓ_4 we introduce a new location F: this location models a failure mode, which is possibly attained when both heaters in the two rooms are switched on. F is an abstract locations containg four sublocations F_1, F_2, F_3 and F_4 denoting the following hybrid set of states $\{\mathtt{ON}_1, \mathtt{ON}_2\} \times D$, $\{\mathtt{ON}_1, \mathtt{OFF}_2\} \times D$, $\{\mathtt{OFF}_1, \mathtt{ON}_2\} \times D$ and $\{\mathtt{OFF}_1, \mathtt{OFF}_2\} \times (S \cup D)$. The transitions kernels T_ℓ and T_x to the four sublocations are defined accordingly to Eq. (11) and (12), as in $T_\ell(F_i|(\ell_4, x))$ for $F_i \in \{\{\mathtt{ON}_1, \mathtt{ON}_2\}, \{\mathtt{ON}_1, \mathtt{OFF}_2\}, \{\mathtt{OFF}_1, \mathtt{ON}_2\}, \{\mathtt{OFF}_1, \mathtt{OFF}_2\}\}$. The reset transition kernel is defined as $T_r(x'|(\ell_4, x), F_i) = T_x(x'|(\ell_4, x))$ for two cases $F_i \in \{F_1, F_2, F_3\}$ and $x' \in D$, or $F_i = F_4$ and $x' \in S \cup D$. All locations ℓ_1, ℓ_2, ℓ_3 and ℓ_4 are labeled with S (domain S), locations ℓ_5, ℓ_6, ℓ_7 and ℓ_8 are labeled with D (domain D) and locations F_i are labeled with F. We select the boundary for the continuous domains as $x_1^l = x_2^l = 5$ and $x_1^u = x_2^u = 45$. Table 3 displays the

Slots l	4	8	16
DTMC states	49	193	769
Time (sec)	66.4	142.4	1723.8

Table 3: Verification time for the LTL-formula φ over the DTMC obtained from the DTSHS $\mathcal{H}_2$.

verification time and the DTMC size for different choices of partitioning slots l. Fig. 13 depicts the probability that the

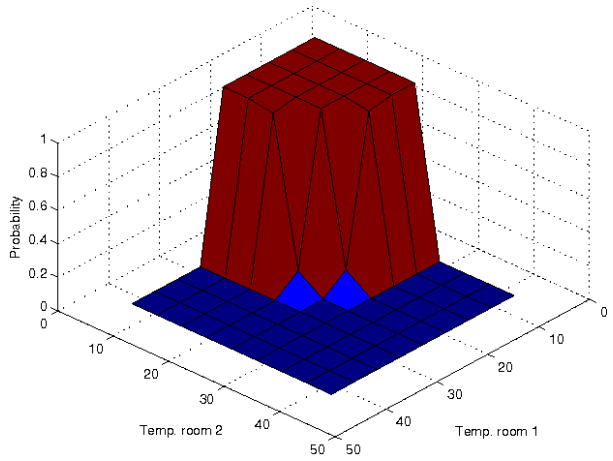

Figure 13: Satisfiability probability for the LTL-formula φ over the DTSHS $\mathcal{H}_2$ (through its DTMC discretization).

DTSHS $\mathcal{H}_2$ satisfies the LTL-formula φ given that the initial location is $\{\mathtt{OFF}, \mathtt{OFF}\}$ and the continuous state is chosen anywhere within the sets S, D of the continuous domains. Notice that the probability is higher for continuous states that are closer to the domain D. All continuous states in domain D satisfy the formula φ with probability one.

6. CONCLUSIONS

In this paper, we have considered the quantitative verification of DTSHS against linear time objectives, specified either as a DFA or as an LTL-formula (Büchi automaton). We have shown that the probability that a DTSHS satisfies a linear time property can be reduced to computing reachability probabilities in the product of the DFA (or the Büchi automaton) and the DTSHS. Future work will include verification of nonautonomous DTSHS and the development of more efficient techniques for the general verification of DTSHS.

7. REFERENCES

[1] PRISM website. http://www.prismmodelchecker.org.

[2] A. Abate, J.-P. Katoen, J. Lygeros, and M. Prandini. Approximate model checking of stochastic hybrid systems. *European Journal of Control*, 16(6):1–18, 2010.

[3] A. Abate, M. Prandini, J. Lygeros, and S. Sastry. Probabilistic reachability and safety for controlled

discrete time stochastic hybrid systems. *Automatica*, 44(11):2724–2734, 2008.

[4] C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, 2008.

[5] M. Bujorianu and J. Lygeros. Reachability questions in piecewise deterministic Markov processes. In O. Maler and A. Pnueli, editors, *HSCC*, volume 2623 of *LNCS*, pages 126–140. Springer-Verlag, 2003.

[6] C. Cassandras and J. Lygeros, editors. *Stochastic Hybrid Systems*. CRC Press, 2007.

[7] P. Collins and I. S. Zapreev. Computable CTL* for discrete-time and continuous-space dynamic systems. In *RP '09: Proceedings of the 3rd International Workshop on Reachability Problems*, pages 107–119, Berlin, Heidelberg, 2009. Springer-Verlag.

[8] J.-M. Couvreur, N. Saheb, and G. Sutre. An optimal automata approach to LTL model checking of probabilistic systems. In *LPAR*, volume 2850 of *LNCS*, pages 361–375, 2003.

[9] J. Desharnais and P. Panangaden. Continuous stochastic logic characterizes bisimulation of continuous-time Markov processes. *J. Log. Algebr. Program.*, 56(1-2):99–115, 2003.

[10] M. Fränzle, T. Teige, and A. Eggers. Satisfaction meets expectations - computing expected values of probabilistic hybrid systems with SMT. In *IFM*, pages 168–182, 2010.

[11] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6:512–535, 1994. 10.1007/BF01211866.

[12] J.-P. Katoen, E. M. Hahn, H. Hermanns, D. N. Jansen, and I. Zapreev. The ins and outs of the probabilistic model checker MRMC. In *QEST*, pages 167–176, 2009.

[13] X. D. Koutsoukos and D. Riley. Computational methods for verification of stochastic hybrid systems. *IEEE Trans. on Systems, Man, and Cybernetics, Part A*, 38(2):385–396, 2008.

[14] A. Lecchini, W. Glover, J. Lygeros, and J. Maciejowski. Monte Carlo optimization for conict resolution in air traffic control. *IEEE Transactions on Intelligent Transportation Systems*, 7:470–482, 2006.

[15] M. Prandini and J. Hu. Stochastic reachability: Theory and numerical approximation. In C. Cassandras and J. Lygeros, editors, *Stochastic hybrid systems*, Automation and Control Engineering Series, pages 107–138. Taylor & Francis Group/CRC Press, 2006.

[16] M. O. Rabin and D. Scott. Finite automata and their decision problems. *IBM Journal of Research and Development*, 3(2):114 –125, 1959.

[17] F. Ramponi, D. Chatterjee, S. Summers, and J. Lygeros. On the connections between PCTL and dynamic programming. In *HSCC*, pages 253–262. ACM, 2010.

[18] S. Summers and J. Lygeros. Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem. *Automatica*, 46(12):1951–1961, 2010.

[19] M. Y. Vardi and P. Wolper. An automata-theoretic approach to automatic program verification. In *LICS*, pages 332–344, 1986.

[20] L. Zhang, Z. She, S. Ratschan, H. Hermanns, and E. M. Hahn. Safety verification for probabilistic hybrid systems. In *CAV*, volume 6174 of *LNCS*, pages 196–211. Springer Verlag, 2010.