Approximate probabilistic verification of hybrid systems

Benjamin M. Gyori∗, Bing Liu†, Soumya Paul, R. Ramanathan, P.S. Thiagarajan‡

ABSTRACT
Hybrid systems whose mode dynamics are governed by nonlinear ordinary differential equations (ODEs) are difficult to analyze. To address this, we develop an approximate probabilistic analysis method. We do so by approximating the mode transitions as stochastic events. More precisely, we assume that the probability of making a mode transition is proportional to the measure of the set of pairs of time points and value states at which the mode transition is enabled. To ensure a sound mathematical basis, we impose a natural continuity property on the non-linear ODEs. We also assume that the states of the system are observed at discrete time points but that the mode transitions may take place at any time between two successive discrete time points. This leads to a discrete time Markov chain as a probabilistic approximation of the hybrid system. We then show that for BLTL (bounded linear time temporal logic) specifications the hybrid system meets a specification iff its Markov chain approximation meets the same specification with probability 1. Based on this, we formulate a sequential hypothesis testing procedure for verifying -approximately- that the Markov chain meets a BLTL specification almost certainly. Our two case studies indicate that our scheme can be applied in a number of realistic settings.

Keywords
hybrid systems, Markov chains, dynamical systems, statistical model checking

1. INTRODUCTION
The analysis of hybrid systems is difficult. The high expressive power of the mixed dynamics renders even basic reachability questions undecidable [18]. Various lines of work have explored ways to mitigate this problem [15, 13, 9, 3, 2, 19]. A common technique is to restrict the continuous dynamics. However, for many of the models arising in the domains of cyber physical systems and systems biology the mode dynamics will be governed by a system of (non-linear) ordinary differential equations (ODEs). To analyze such systems, we develop here a probabilistic scheme under which a rich class of hybrid systems with non-linear dynamics can be approximated as a discrete time Markov chain.

A key difficulty in analyzing a hybrid system’s behavior arises from the interaction between the continuous mode dynamics and the discrete mode transitions governed by the guards. Specifically, the time points and value states at which a trajectory meets a guard will depend on the solutions to the ODE systems associated with the modes. For high-dimensional systems these solutions will not be available in closed form. To get around this, we assume that the mode transitions are stochastic events and that the probability of a mode transition is proportional to the measure of the value state and time point pairs at which this transition is enabled. More sophisticated hypotheses could be considered. For instance one could tie the mode transition probability to how long the guard has been continuously enabled or how deeply within a guard region the current state is. It could also be the case that some of the mode transitions are controllable, say, by a digital controller. This will, however, entail MDPs (Markov decision processes) based approximations, and we postpone the study of this more complex setting to the future.

To secure a sound mathematical basis for our approximation, we further assume: (i) The vector fields associated with the ODEs are C1 functions.(ii) The states of the hybrid system are observable only at discrete time points. (iii) The set of initial states and the guard sets are bounded open sets.(iv) The hybrid dynamics is strictly non-Zeno in the sense there is uniform upper bound on the number of transitions that can take place in a unit time interval. For technical convenience we in fact assume that time discretization is so chosen that at most one mode transition takes place between two successive discrete time points. A rich class of engineered systems and biological processes can be modeled under these restrictions.
In this setting, we construct a Markov chain $M$ as an approximation of the hybrid system $H$. To relate the behaviors of $M$ and $H$, we use BLTL (bounded linear-time temporal logic) to specify time bounded dynamic properties of $H$. We then show that $H$ meets the specification $\psi$—i.e. every trajectory of $H$ is a model of $\psi$—if $M$ meets the specification $\psi$ with probability 1. This allows us to approximately verify interesting properties of the hybrid system using its Markov chain approximation. However, the transition probabilities of the Markov chain will depend on the solutions to the ODEs associated with the modes, which will not be available in a closed form. To cope with this, we design a statistical model checking procedure to approximately verify that the chain almost certainly meets the specification. We do so by randomly generating trajectories of $H$ through numerical simulations in a way that corresponds to randomly sampling the paths of the Markov chain according to its underlying transition probabilities.

In establishing these results, we first assume that the atomic propositions in the specification are interpreted over the modes of the hybrid system. Consequently one can specify patterns of mode visitations while quantitative properties can be inferred only indirectly and in a limited fashion. As an extension we then introduce quantitative atomic propositions ("the current velocity of the vehicle is greater than 40 miles/hour") and show that our results go through—with a more refined construction—provided the dynamics is restricted to robust trajectories. Informally, under a natural topology, a robust trajectory is one that is contained in an open neighborhood of trajectories which satisfy the same specification. The procedure for sampling trajectories can be easily modified to sample for robust trajectories. Finally, we demonstrate the applicability of our method using a room heating system and a model of the activation dynamics of cardiac muscle cells.

Due to space limitations we present only proof sketches for a number of the results. More details can be found in the appendix.

1.1 Related work

Mode transitions have been approximated as random events in the literature. In [1] the dynamics of a hybrid system is approximated by substituting the guards with probabilistic barrier functions. Our transition probabilities are constructed using similar but simpler considerations. We have done so in order to be able to carry out temporal logic based verification based on simulations. Another related work is [11], which studies a network of hybrid automata that communicate with each other through input/output actions. Translated into our setting, the main idea roughly boils down to this: the time point in $(0,1)$, at which the decision about what the mode should be up to the next discrete time point, is determined by the uniform distribution over $(0,1)$. In our setting this probability is determined by the continuous mode dynamics and the guard sets.

An alternative approach to approximately verifying nonlinear hybrid systems is one based on $\delta$-reals [14]. Here one verifies bounded reachability properties that are robust under small perturbations of the numerical values mentioned in the specification. Since the approximation involved is of a very different kind, it is difficult to compare this line of work with ours. However, it may be fruitful to combine the two approaches to verify a richer set of reachability properties.

The present work may be viewed as an extension of [23] where a single system of ODEs is considered. This method, however, breaks down in the multi-mode hybrid setting and one needs to construct—as we do here—an entirely new machinery. Finally, a wealth of literature is available on the analysis of stochastic automata [8], [6], [21], [4]. It will be interesting to explore if these methods can be transported to our setting.

2. HYBRID AUTOMATA

As usual we will use hybrid automata as a model of hybrid systems. Accordingly, we fix $n$ real-valued variables $\{x_i\}_{i=1}^n$ viewed as functions of time $x_i(t)$ with $t \in \mathbb{R}_+$, the set of non-negative reals. A valuation of $\{x_i\}_{i=1}^n$ is $v \in \mathbb{R}^n$ with $v(i) \in \mathbb{R}$ representing the value of $x_i$. The language of guards is given by: (i) $a < x_i$ and $x_i < b$ are guards where $a, b$ are rationals and $i \in \{1, 2, \ldots, n\}$. (ii) If $g$ and $g'$ are guards then so are $g \land g'$ and $g \lor g'$.

$G$ denotes the set of guards. We define $v \models g$ (i.e. $v$ satisfies the guard $g$) via: $v \models g \iff a < x_i$ if $x_i < b$ and similarly for $x_i < b$. The clauses for conjunction and disjunction are standard. We let $\|g\| = \{v \models g\}$. We note that $\|g\|$ is an open subset of $\mathbb{R}^n$ for every guard $g$. We will abbreviate $\|g\|$ as $g$.

Definition 1 A hybrid automaton is a tuple $H = (Q, q_0, \{F_i(x)\}_{x \in Q}, G, \rightarrow, \text{INIT})$, where

- $Q$ is a finite set of modes and $q_0 \in Q$ is the initial mode.
- For each $g \in G$, $dx/dt = F_i(x)$ is a system of ODEs, where $x = (x_1, x_2, \ldots, x_n)$ and $F_i = (f_1^i(x), f_2^i(x), \ldots, f_n^i(x))$. Further, $f_i^j$ is a $C^1$ (continuously differentiable) function for each $i$.
- $\rightarrow \subseteq (Q, G, Q)$ is the mode transition relation.
- INIT = $(L_1, U_1) \times (L_2, U_2) \times \ldots \times (L_n, U_n)$ is the set of initial states where $L_i < U_i$ and $L_i, U_i$ are rationals.

We have not associated invariant conditions with the modes or reset conditions with the mode transitions. They can be introduced with some additional work.

Fixing a suitable unit time interval $\Delta$, we discretize the time domain as $t = 0, \Delta, 2\Delta, \ldots$. We assume the states of the system are observed only at these discrete time points. Furthermore, we shall assume that only a bounded number of mode changes may take place between successive discrete time points. Both in engineered and biological processes this is a reasonable assumption. Given this, we shall in fact assume that $\Delta$ is such that at most one mode change takes place within a $\Delta$ time interval. We note that there can be multiple choices for $\Delta$ that meet this requirement and in practice one must choose this parameter carefully. (Our
method can be extended to handle a bounded number of mode transitions in a unit time interval but this will entail notational complications that will obscure the main ideas.

In what follows, for technical convenience we also assume the time scale has been normalized so that \( \Delta = 1 \). As a result, the discretized set of time points will be \( \{0, 1, 2, \ldots\} \).

2.1 Trajectories

In what follows, we fix a hybrid automaton \( H \) as defined above. The behavior of \( H \) will consist of its trajectories. To define this notion and for later use, we start with some preliminaries. We recall that a function \( f : \mathbb{R} \to \mathbb{R} \) is \( C^1 \) if \( f' \), the derivative of \( f \), exists everywhere and is continuous. This notion extends to \( \mathbb{R}^n \) in the obvious way. Next, the function \( F : \mathbb{R}^n \to \mathbb{R}^n \) is Lipschitz if there exists a \( c \in \mathbb{R}, c > 0 \), such that for all \( v_1, v_2 \in \mathbb{R}^n \), \( |F(v_1) - F(v_2)| \leq c|v_1 - v_2| \), where \( |\cdot| \) is the standard Euclidean norm on \( \mathbb{R}^n \).

We have assumed that for every mode \( q \), the right hand side of the ODEs, \( F_q(x) \), is \( C^1 \) for each component. As a result, for each value \( v \in \mathbb{R}^n \) and in each mode \( q \), the system of ODEs \( dx/dt = F_q(x) \) will have a unique solution \( Z_{q,v}(t) \) [20] satisfying \( Z_{q,v}(0) = v \) and \( dZ_{q,v}(t)/dt = F(Z_{q,v}(t)) \). We are also guaranteed that \( Z_{q,v}(t) \) is Lipschitz and hence measurable [20]. This fact will play a crucial role in what follows. It will be convenient to work with two sets of functions derived from solutions to the ODE systems.

The (unit interval) flow \( \Phi_q : (0,1) \times \mathbb{R}^n \to \mathbb{R}^n \) is given by \( \Phi_q(t,v) = Z_{q,v}(t) \). \( \Phi_q \) will also be Lipschitz. Next we define the parametrized family of functions \( \Phi_{q,t} : \mathbb{R}^n \to \mathbb{R}^n \) given by \( \Phi_{q,t}(v) = \Phi_q(t,v) \). In addition to being Lipschitz, these functions will be bijective as well. Further, their inverses will also be bijective and Lipschitz.

A (finite) trajectory is a sequence

\[
\tau = (q_0, v_0) (q_1, v_1) \ldots (q_k, v_k)
\]

such that for \( 0 \leq j < k \) the following conditions are satisfied: (i) For \( 0 \leq j < k \), \( q_j \xrightarrow{g_j} q_{j+1} \) for some guard \( g_j \); (ii) there exists \( t \in (0,1) \) such that \( \Phi_{q_j,t}(v_j) \in g \). Furthermore \( v_{j+1} = \Phi_{q_{j+1}-1}^{-1}(\Phi_{q_j,t}(v_j)) \).

We say that the trajectory \( \tau \) as defined above starts from \( q_0 \) and ends in \( q_k \). Further, its initial value state is \( v_0 \) and its final value state is \( v_k \). We let \( TRJ \) denote the set of all finite trajectories that start from the initial mode \( q_0 \) and with an initial value state in INIT.

3. THE MARKOV CHAIN APPROXIMATION

A (finite) path in \( H \) is a sequence \( \rho = q_0 q_1 \ldots q_k \) such that for \( 0 \leq j < k \), there exists a guard \( g_j \) such that \( q_j \xrightarrow{g_j} q_{j+1} \). We say that this path starts from \( q_0 \), ends at \( q_k \) and of length \( k+1 \). We let \( paths_H \) denote the set of all finite paths that start from \( q_0 \).

In what follows \( \mu \) will denote the standard Lebesgue measure over finite dimensional Euclidean spaces. We will construct \( M_H = (\mathcal{Y}, \Rightarrow) \), the Markov chain approximation of \( H \) inductively. Each state in \( \mathcal{Y} \) will be of the form \((\rho, X, \mu_X)\) with \( \rho \in paths_H \). \( X \) an open subset of \( \mathbb{R}^n \) of non-zero, finite measure and \( \mu_X \) a probability distribution over \( SA(X) \), the \( \sigma \)-algebra generated by \( X \).

We start with \((q_0, \text{INIT}, \mu_{\text{INIT}}) \in \mathcal{Y} \). Clearly, INIT is an open set and it is of non-zero, finite measure since \( \mu(\text{INIT}) = \prod_i (U_i - L_i) \). For technical convenience we shall assume \( \mu_{\text{INIT}} \) to be the uniform probability distribution. This reflects the assumption that each member of INIT is an equally likely initial value state. However we can handle other distributions over INIT as well.

Assume inductively that \((\rho, X, \mu_X) \) is in \( \mathcal{Y} \) with \( X \) an open subset of \( \mathbb{R}^n \) of non-zero, finite measure and \( \mu_X \) a probability distribution over \( SA(X) \). Suppose \( \rho \) ends in \( q \) and there are \( m \) outgoing transitions \( q \xrightarrow{g_1} q_1, \ldots, q \xrightarrow{g_m} q_m \) from \( q \) in \( H \) (Fig. 1 illustrates this inductive step). Then for \( 1 \leq j \leq m \) we define the triples \((pq_j, X_j, \mu_{X_j})\) as follows. In doing so we will assume the required properties of the objects involved in this construction. We will then establish these properties and thus the soundness of the construction. For convenience, through the remaining parts of this section \( j \) will range over \( \{1, 2, \ldots, m\} \).

For each \( v \in X \) and each \( j \) we first define the set of time points \( T_j(v) \subseteq (0,1) \) via

\[
T_j(v) = \{ t | \Phi_q(t,v) \in g_j \}.
\]

Thus \( T_j(v) \) is the set of time points in \((0,1)\) at which the guard \( g_j \) is satisfied if the system starts from \( v \) in mode \( q \) at time \( k \) and evolves according to dynamics of mode \( q \) up to time \( k + t \). We next define \( X_j \) for each \( j \) as

\[
X_j = \bigcup_{v \in X} \{ \Phi_q(1-t, \Phi_q(t,v)) | t \in T_j(v) \}.
\]

Thus \( X_j \) is the set of all value states obtained by starting from some \( v \in X \) at time \( k \), evolving up to \( k + t \) according to the dynamics \( q \), making an instantaneous mode switch to \( q_j \) at this time point, and evolving up to time \( k + 1 \) according to dynamics of mode \( q_j \).

To complete the definition of the triples \((pq_j, X_j, \mu_{X_j})\), we first denote by \( \mu_{X_j} \) the uniform probability distribution over \( T_j(v) \). Our construction can be easily extended to handle other kinds of distributions as well. We now define the probability distributions \( \mu_{X_j} \) over \( SA(X_j) \) as follows. Suppose \( Y \) is a measurable subset of \( X_j \). Then

\[
\mu_{X_j}(Y) = \int_{v \in X} \int_{t \in T_j(v)} 1(\Phi_q(1-t, \Phi_q(t,v)) \in Y) dP_{T_j(v)} d\mu_X.
\]

As usual \( 1_Z \) is the indicator function of the set \( Z \) while \( dP_{T_j(v)} \) indicates that the inner integration over \( T_j(v) \) is w.r.t. the (uniform) probability measure \( P_{T_j(v)} \) and \( d\mu_X \) indicates that the outer integration over \( X \) is w.r.t. the probability measure \( \mu_X \). Thus \( \mu_{X_j}(Y) \) captures the probability that the value state \( \Phi_q(1-t, \Phi_q(t,v)) \) lands in \( Y \subseteq X_j \) by taking the transition \( q \xrightarrow{g_j} q_j \) at some time point in \( T_j(v) \) given that one started with some value state in \( X \).

Next we define the triples \( ((\rho, X, \mu_X), p_j, (pq_j, X_j, \mu_{X_j})) \), where \( p_j \) is given by
\[ p_j = \int_{v \in X} \frac{\mu(T_j(v))}{\sum_{\ell=1}^m \mu(T_\ell(v))} d\mathcal{P}_X. \]  

(4)

Thus \( p_j \) captures the probability of taking the mode transition \( q \xrightarrow{a} q \) when starting from the value states in \( X \) and mode \( q \). For every \( j \) we add the state \((p_j, X_j, \mathcal{P}_{X_j})\) to \( \Upsilon \) and the triple \((\rho, X, \mathcal{P}_X), p_j, (p_j, X_j, \mathcal{P}_{X_j})\) to \( \Rightarrow \) iff \( \mu(X_j) > 0 \).

Finally, \((q_{ini}, \text{INIT}, \mathcal{P}_{\text{INIT}})\) is the initial state of \( M_H \). We can summarize the key properties of our construction as follows (while assuming the associated terminology and notations).

**Theorem 1**

1. \( T_j(v) \) is an open set of finite measure for each \( v \in X \) and each \( j \).
2. \( X_j \) is open and is of finite measure for each \( j \).
3. If \((p_j, X_j, \mathcal{P}_{X_j}) \in \Upsilon \) then \( \mu(X_j) > 0 \).
4. \( \mathcal{P}_{X_j} \) is a probability distribution for each \( j \).
5. \( M_H = (\Upsilon, \Rightarrow) \) is an infinite state Markov chain whose underlying graph is a finitely branching tree.

**Proof.** To prove the first part, suppose \( t \in T_j(v) \). Then \( \Phi_q(t, v) = v' \in g_j \) and \( g_j \) is open. Hence \( v' \) will be contained in an open neighborhood \( U \) contained in \( g_j \). Since \( \Phi_q \) is Lipschitz we can pick \( U \) such that \( Y' = \Phi_{q^{-1}}(U) \) is an open set containing \((v, t)\) with \( Y' \subseteq (0, 1) \times X \). Thus every element of \( T_j(v) \) is contained in an open neighborhood in \((0, 1)\) and hence \( T_j(v) \) is open.

Using the definition of \( X_j \), the fact that \( X \) and \( T_j(v) \) are open, and the continuity of the inverses of the flow functions it is easy to observe that \( X_j \) is open. To see that it is of finite measure, by the induction hypothesis, \( X \) is open and \( \mu(X) \) is finite. Hence \((0, 1) \times X \) is open as well and \( \mu((0, 1) \times X) \) is finite. Since \( \mathbb{R}^{n+1} \) is second-countable [24], there exists a countable family of disjoint open-intervals \( \{I_i\}_{i \geq 1} \) in \( \mathbb{R}^{n+1} \) such that \((0, 1) \times X = \bigcup I_i \). Clearly each \( I_i \) has a finite measure. By the Lipschitz continuity of \( \Phi_q \) we know that there exists a constant \( c \) such that \( \mu(\Phi_q(I_i)) < c \cdot \mu(I_i) \) for all \( i \). We thus have

\[ \mu(\Phi_q((0, 1), X)) \leq \sum_i \mu(\Phi_q(I_i)) < c \sum_i \mu(I_i) = c \mu((0, 1) \times X) < \infty. \]  

(5)

Therefore \( \Phi_q((0, 1), X) \) has a finite measure. By a similar argument we can show that \( \Phi_q((0, 1), \Phi_q((0, 1), X)) \) has a finite measure as well. Since \( X_j = \bigcup \Phi_q \downarrow \Phi_q((0, 1), \Phi_q((0, 1), X)) \subseteq \Phi_q((0, 1), \Phi_q((0, 1), X)) \) it must have a finite measure.

The remaining parts of the theorem follow easily from the definitions and basic measure theory. □

### 4. RELATING THE BEHAVIORS OF H AND M_H

We shall use bounded linear-time temporal logic (BLTL) [10] to specify time bounded properties and use it to relate the behaviors of \( H \) and \( M_H \). For convenience we shall write \( M \) instead of \( M_H \) from now on.

We assume a finite set of atomic propositions \( AP \) and a valuation function \( K_T : Q \rightarrow 2^AP \). Formulas of BLTL are defined as: (i) Every atomic proposition as well as the constants true, false are formulas. (ii) If \( \varphi, \varphi' \) are formulas then \( \neg \varphi \) and \( \varphi \lor \varphi' \) are formulas. (iii) If \( \varphi, \varphi' \) are formulas and \( \ell \) is a positive integer then \( \varphi U^\ell \varphi' \) is a formula. The derived operators \( F^\ell \) and \( G^\ell \) are defined as usual: \( F^\ell \varphi \equiv \text{true} U^\ell \varphi \) and \( G^\ell \varphi \equiv \neg F^\ell \neg \varphi \).

We shall assume through the rest of the paper that the behavior of the system is of interest only up to a maximum time point \( K > 0 \). This is guided by the fact that given a BLTL formula \( \varphi \) there is a constant \( K_\varphi \) that depends only on \( \varphi \) so that it is enough to evaluate an execution trace of length at most \( K_\varphi \) to determine whether \( \varphi \) is satisfied [5]. Hence we assume that a sufficiently high \( K \) has been chosen to handle the specifications of interest. Having fixed \( K \), we denote by \( TRJ^{K+1} \) the trajectories of length \( K+1 \), and view this set as representing the time bounded non-deterministic behavior of \( H \) of interest.

To develop the corresponding notion for \( M \), we first define a finite path in \( M \) to be a sequence \( \eta_0 \eta_1 \ldots \eta_k \) such that \( \eta_j \in \Upsilon \) for \( 0 \leq j \leq k \). Furthermore for \( 0 \leq j < k \) there exists \( p_j \in (0, 1] \) such that \( \eta_j \xrightarrow{p_j} \eta_{j+1} \). Such a path is said to start from \( \eta_0 \) and its length is \( k+1 \). We define \( \text{paths}_M \) to be the set of finite paths that start from the initial state of \( M \) while \( \text{paths}_M^{K+1} \) is the set of paths in \( \text{paths}_M \) of length \( K+1 \).

**The trajectory semantics.** Let \( \tau = (q_0, v_0) (q_1, v_1) \ldots (q_k, v_k) \) be a finite trajectory, \( \psi \) a BLTL formula and \( 0 \leq j \leq K \). Then \( \tau, j \models_H \psi \) is defined via:

- \( \tau, j \models_H A \) iff \( A \in K_T(q_j) \), where \( A \) is an atomic proposition.
- \( \neg \) and \( \lor \) are interpreted in the usual way.
- \( \tau, j \models_H \psi U^\ell \psi' \) iff there exists \( j' \) such that \( j' \leq \ell \) and \( j + j' \leq k \) and \( \tau, j + j' \models_H \psi' \). Further, \( \tau, (j + j') \models_H \psi' \) for every \( 0 \leq j'' < j' \).

![Figure 1: Markov chain construction.](image-url)
Now we define $\models_M(\psi) \subseteq \text{paths}^{K+1}_M$ via: $\tau \in \models_M(\psi)$ iff $\tau, 0 \not\models_H \psi$. We say that $H$ meets the specification $\psi$ -denoted $H \models \psi$- iff $\models_M(\psi) = \text{TRJ}^{K+1}$.

The Markov chain semantics. Let $\pi = \eta_0 \eta_1 ... \eta_k$ be a path in $M$ with $\eta_j = (p_{j_0}, X_{j_0}, P_{X_{j_0}})$ for $0 \leq j \leq k$. Let $\psi$ be a BLTL formula and $0 \leq j \leq k$. Then $\pi, j \models M \psi$ is given by:

- $\pi, j \models M \psi$ if $A$ is an atomic proposition.
- The remaining clauses are defined just as in the case of $\models_H$.

Now we define $\models_M(\psi) \subseteq \text{paths}^{K+1}_M$ via: $\tau \in \models_M(\psi)$ iff $\tau, 0 \not\models_M \psi$. We can now establish the main result of this section. We wish to show that $\models_M(\psi)$ is compatible with $\models_H$. Hence $\Pr(\pi) = 1$ for every $\pi \in \models_M(\psi)$. Furthermore $\sum_{\pi \in \models_M(\psi)} \Pr(\pi) \leq 1$. Hence $\models_M(\psi)$iff $\models_M(\psi) = \text{paths}^{K+1}_M$ iff $M \models \psi$.

### 4.1 The main result

We wish to show that $H$ meets the specification $\psi$ -denoted $H \models \psi$. This to end let $\pi = \eta_0 \eta_1 ... \eta_k$ be a path in $M$ with $\eta_j = (q_0, q_1, ..., q_k, \psi)$ be a trajectory. Then we say that $\pi$ and $\tau$ are compatible if $k + 1$ and $q_j = q'_j$ and $v_j \in X_j$ for $0 \leq j \leq k$. The following three observations on this notion will easily lead to the main result.

**Lemma 1.** 1. Suppose the path $\pi = \eta_0 \eta_1 ... \eta_k$ in $M$ and the trajectory $\tau = \psi(q_0, v_0)(q_1, v_1)...(q_k, v_k)$ are compatible. Let $0 \leq j \leq k$ and $\pi, j \models M \psi$ be a BLTL formula. Then $\pi, j \models M \psi$ if $\tau \models \psi$.

2. Suppose $\pi$ is a path in $M$. Then there exists a trajectory $\tau$ such that $\pi$ and $\tau$ are compatible. Furthermore if $\pi \in \text{paths}_M$ then $\tau \in \text{TRJ}$.

3. Suppose $\tau$ is a trajectory. Then there exists a path $\pi$ in $M$ such that $\pi$ and $\tau$ are compatible. Furthermore if $\tau \in \text{TRJ}$ then $\pi \in \text{paths}_M$.

The proof follows via a systematic application of the definitions, and details can be found in the Appendix. We can now establish the main result of this section.

**Theorem 2** $H \models \psi$ iff $M \models \psi$.

**Proof.** Suppose $H$ does not meet the specification $\psi$. Then there exists $\tau \in \text{TRJ}^{K+1}$ such that $\tau, 0 \not\models_H \psi$. By the last part of Lemma 1, there exists $\pi \in \text{paths}^{K+1}_M$ which is compatible with $\tau$. By the first part of Lemma 1, we then have $\pi \not\in \models_M(\psi)$ which leads to $\Pr(\pi) = 1$.

Next suppose that $\Pr_{<1}(\tau)$. Then there exists $\pi \in \text{paths}^{K+1}_M$ such that $\tau, 0 \not\models M \psi$. By the second part of Lemma 1, there exists $\tau \in \text{TRJ}^{K+1}$ which is compatible with $\pi$. By the first part of Lemma 1 this implies $\tau, 0 \not\models M \psi$ and this in turn implies that $H$ does not meet the specification $\psi$.

### 5. THE SMC PROCEDURE

To verify whether $H$ meets the specification $\psi$, we solve the equivalent problem whether $\Pr_{>1}(\psi)$ on $M$. However, $M$ cannot be constructed explicitly since its transition probabilities are defined in terms of the solutions to the ODEs which will not be available. Therefore we shall use randomly generated trajectories to sample the paths of $M$ and formulate a sequential hypothesis test to decide with bounded error rate whether $\Pr_{>1}(\psi)$ holds. Algorithm 1 describes our trajectory sampling procedure.

**Algorithm 1 Trajectory simulation**

**Input:** Hybrid automaton $H = (Q, q_0, \{F_q(\mathbf{x})\}_{q \in Q}, G, \rightarrow, \text{INIT})$, maximum time step $K$.

**Output:** Trajectory $\tau$.

1. Sample $q_0$ from $\text{INIT}$ uniformly, set $q_0 := q_0$ and $\tau := (q_0, q_0)$.
2. for $k := 1 \ldots K$ do
3. 1. Generate time points $T := \{t_1, \ldots, t_k\}$ uniformly in $(0, 1)$.
4. 2. Simulate $\psi := \Phi_{q_k-1}(t_j, q_{k-1})$, for $j \in \{1, \ldots, k\}$.
5. 3. Let $\hat{t}_j := \{t \in T : \psi \in \psi_j\}$ be the time points where $\psi_j$ is enabled.
6. 4. Pick $q_j$ randomly according to probabilities $p_j := \frac{\hat{t}_j}{\sum_{i=1}^{K} \hat{t}_i}$.
7. 5. Pick $t_j$ uniformly at random from $\hat{t}_j$.
8. 6. Simulate $\psi := \Phi_{q_j}(1 - t_j, \psi')$, where $\psi'$ is the target of $q_j$.
9. 7. Set $q_k := q', q_k := \psi'$, and extend $\tau := (q_0, q_0) \ldots (q_k, q_k)$.
10. end for
11. return $\tau$

Clearly Algorithm 1 generates a trajectory in $\text{TRJ}^{K+1}$. We now relate these trajectories to paths in $M$.

The initial value $v_0$ is sampled uniformly on INIT, and we start in mode $q_{i_0}$, consistent with the initial state $(q_{i_0}, \text{INIT}, P_{\text{INIT}})$ of $M$. Inductively, suppose $\eta = (p, X, P_X)$ is a state of $M$ with $p$ ending in $q_i$. Suppose $\eta \not\models P_X \models \psi$. Then $\models_M(\psi)$ tends to $p_j$ as $J \rightarrow \infty$.

**Proposition 1.** Suppose, we obtain a sample $v \sim P_X$. The probability of choosing guard $g_j$ whose target mode is $q_j$ in Algorithm 1 tends to $p_j$ as $J \rightarrow \infty$.

**Proof.** According to Algorithm 1, the probability of picking guard $g_j$ for a trajectory starting at $v \in X$ is defined as $p_j(v) := \frac{\mu(T_j(v))}{\sum_{i=1}^{K} \mu(T_i(v))}$ which, by the law of large numbers tends to $p_j(v) := \frac{\mu(T_j(v))}{\sum_{i=1}^{K} \mu(T_i(v))}$ as $J \rightarrow \infty$.

Now if $v$ is randomly sampled according to $P_X$, then the
\[ v \sim P_X \quad \Phi_{q_j}(t, v) \quad \Phi_{q_j}(1-t, \Phi_{q_j}(t, v)) \quad v' \sim P_{X_j} \]

**Figure 2: Propagating a single value \( v \in X \) to \( v' \in X_j \) when taking the transition \( q \rightarrow q_j \) at time \( t \in T_j(v) \).**

The probability of picking guard \( j \) can be expressed as the expected value of \( p_j(v) \) under \( v \sim P_X \) as

\[
\mathbb{E}_{v \sim P_X}[p_j(v)] = \int_{v \in X} p_j(v) dP_X = \int_{v \in X} \frac{\mu(T_j(v))}{\sum_{i=1}^{k} \mu(T_i(v))} dP_X, \tag{7}
\]

which by \( [4] \) is equal to \( p_j \), the corresponding transition probability in the Markov chain. \( \square \)

Similarly, picking the transition time \( t \) from \( \hat{T}_j \) will approximately sampling \( t \sim P_{T_j(v)} \), for sufficiently high \( J \). Next, assume that we have picked \( q, q_j \) as the transition to take. We sample \( t \sim P_{T_j(v)} \), and obtain \( v' \) by numerical simulation via:

\[ v' = \Phi_{q_j}(1-t, \Phi_{q_j}(t, v)). \tag{8} \]

**Proposition 2.** \( v' \) is distributed according to \( P_{X_j} \).

**Proof.** Clearly it suffices to show that for a measurable subset \( Y \subseteq X_j \), \( Pr(v' \in Y) = P_{X_j}(Y) \). We start with

\[ Pr(v' \in Y) = \int_{v \in X \cap Y} 1_{\Phi_{q_j}(1-t, \Phi_{q_j}(t, v) \in Y)} dP_{T_j(v)} \cdot P_X \cdot P_{T_j(v)} \cdot \]

Integrating now over all possible choices of \( v \) with respect to \( P_X \) we have

\[ Pr(v' \in Y) = \int_{v \in X} Pr(v' \in Y \mid v) dP_X. \]

From \( [3] \) it follows that \( Pr(v' \in Y) = P_{X_j}(Y) \) with \( v \sim P_X \) and \( t \sim P_{T_j(v)} \). \( \square \)

Consequently, the trajectory being generated will now be in mode \( q_j \), with \( v' \in X_j \) and \( v' \) distributed according to \( P_{X_j} \), compatible with the state \( \eta_t = (pq_j, X_j, P_{X_j}) \) of \( M \). Inductively it is hence guaranteed that each subsequent iteration of Algorithm \( [3] \) will produce values compatible with a path of \( M \).

Whether the generated trajectory of length \( K+1 \) (and hence the corresponding path of \( M \)) is a model of \( \psi \) can be determined using a standard BLTL model checker \( [10] \). In fact this can be done on the fly which will often avoid generating the whole trajectory. Based on this, we can test whether \( Pr_{v \in Y} \) on \( M \) by testing the following alternative pair of hypotheses: \( H_0 : Pr_{v \in Y} \) and \( H_1 : Pr_{v \not\in Y} \), where \( 0 < \delta < 1 \) is a parameter chosen by the user marking the interval \( [1-\delta, 1) \) as an indifference region in which accepting either hypothesis is fine. In our setting, whenever we encounter a sample (i.e., a randomly generated trajectory) that does not satisfy \( \psi \), we can reject \( H_0 \) and accept \( H_1 \). Thus we only have to deal with false positives (when \( H_0 \) is accepted while \( H_1 \) happens to be true).

This leads to Algorithm \( [2] \) that repeatedly generates a random trajectory (using Algorithm \( [1] \), and decides after a finite number of tries between \( H_0 \) and \( H_1 \). For doing so we also fix a user-defined false positive rate \( \alpha \).

**Algorithm 2** Sequential hypothesis test

**Input:** Markov chain \( M \), BLTL property \( \psi \), indifference parameter \( \delta \), false positive bound \( \alpha \).

**Output:** \( H_0 \) or \( H_1 \).

1. Set \( N := [\log \alpha / \log(1-\delta)] \)
2. For \( i := 1 \ldots N \) do
3. Generate a random trajectory \( \tau \) using Algorithm \( [1] \)
4. If \( \tau, 0 \models \psi \) then Continue
5. Else return \( H_1 \)
6. End for
7. Return \( H_0 \)

The accuracy of Algorithm \( [2] \) is captured by the next result.

**Theorem 3**

1. The probability of choosing \( H_1 \) when \( H_0 \) is true (false negative) is 0.
2. Suppose \( N \geq \log \alpha / \log(1-\delta) \). Then the probability of choosing \( H_0 \) when \( H_1 \) is true (false positive) is no more than \( \alpha \).

**Proof.** As observed earlier the first part is obvious. To prove the second part, if \( H_1 \) is true, then we know that \( Pr_{<c}(\psi) \). The probability of \( N \) sampled trajectories all satisfying \( \psi \) (and thus returning \( H_0 \), a false positive) is at most \( (1-\delta)^N \). Therefore we have \( \alpha \leq (1-\delta)^N \), and this leads to \( N \geq \log \alpha / \log(1-\delta) \). \( \square \)

Hence we use \( N := [\log \alpha / \log(1-\delta)] \) to set the sample size. For example for \( \delta = 0.01 \) and \( \alpha = 0.01 \) we get \( N = 459 \) while for \( \delta = 0.001 \) and \( \alpha = 0.01 \) we get \( N = 4603 \).

### 6. Quantitative Specifications

To specify quantitative properties we fix a finite set of atomic propositions \( AP_{qt} \) of the form \( \langle x_i < c \rangle \) or \( \langle x_i > c \rangle \) where \( c \) is a rational constant. In what follows we shall assume for convenience that all the atomic propositions that we encounter are members of \( AP_{qt} \). It will be straightforward to extend our arguments to include qualitative atomic propositions as well.

We partition \( \mathbb{R}^n \) into hyperscubes according to the constants mentioned in the quantitative atomic propositions in \( AP_{qt} \). (Actually one could just focus on the members of \( AP_{qt} \) that appear in a given specification but we wish to deal with specifications later). Accordingly, define \( C_i \) to be the set of rational constants so that \( c \in C_i \) iff an atomic proposition of the form \( \langle x_i < c \rangle \) or \( \langle x_i > c \rangle \) appears in \( AP_{qt} \). We next define for each dimension \( i \) the set of intervals

\[ \mathcal{I}_i = \{(-\infty, c_{i1}^1], \{c_{i1}^1, c_{i1}^2\}, \{c_{i1}^2, c_{i1}^3\}, \ldots, c_{i1}^m, +\infty) \} \]
where $C_i = \{c_i^1 < c_i^2 < \ldots < c_i^n\}$. In case $C_i = \emptyset$ we set $I_i = \{(-\infty, +\infty)\}$.

This leads to the set of hypercubes $H$ given by

$$H = \{\prod_i I_i \mid I_i \in I_i\}.$$  

Clearly $H$ is a partition of $\mathbb{R}^n$. The states of the Markov chain $M_{qt}$ we wish to define as the approximation of $H$ will be the states of $M$ defined previously but now refined using $H$. More precisely we define $M_{qt} = (\Upsilon_{qt}, \Rightarrow_{qt})$ inductively as follows: $\epsilon \in \Upsilon_{qt}$ and it is the initial state of $M_{qt}$. Every other state in $\Upsilon_{qt}$ will be of the form $(\rho, X, h, P_X)$ where $\rho$ is a path in $H$, $X$ is an open subset of $\mathbb{R}^n$ of finite non-zero measure, $h \in H$ and $P_X$ is a probability distribution over $X$. Furthermore $X \subseteq h$.

As the first step, we form the tuples $(q_{in}, \text{INIT}^h, h, P_{\text{INIT}^h})$ with $\text{INIT}^h = (\text{INIT} \cap h)$. The tuple $(q_{in}, \text{INIT}^h, h, P_{\text{INIT}^h})$ is in $\Upsilon_{qt}$ iff $\mu(\text{INIT}^h) > 0$. Here $P_{\text{INIT}^h}$ is assumed to be the uniform distribution over $\text{INIT}^h$. If $\mu(\text{INIT}^h) > 0$ then since $h$ is open $\text{INIT}^h$ will be open as well.

For every $(q_{in}, \text{INIT}^h, h, P_{\text{INIT}^h})$ in $\Upsilon_{qt}$ we define the triple $(\epsilon, p^h, (q_{in}, \text{INIT}^h, h, P_{\text{INIT}^h}))$ where $p^h$ is defined as:

$$p^h = \frac{\mu(\text{INIT}^h)}{\sum_{h' \in H} \mu(\text{INIT}^{h'})}. \quad (9)$$

We add all such triples $(\epsilon, p^h, (q_{in}, \text{INIT}^h, h, P_{\text{INIT}^h}))$ to $\Rightarrow_{qt}$. Assume inductively that $(\rho, X, h, P_X)$ is in $\Upsilon_{qt}$ with $X$ open and of non-zero finite measure with $X \subseteq h$. Suppose $\rho$ ends in $q$ and there are $m$ outgoing transitions $q \xrightarrow{g_1} q_1, q \xrightarrow{g_2} q_2 \ldots q \xrightarrow{g_m} q_m$ from $q$ in $H$. Then for every $j : 1 \leq j \leq m$ and for every $h' \in H$ we define the tuple $(\rho_j, X_j^{h'}, h', P_{X_j^{h'}})$ as follows. For the rest of this sub-section $j$ will range over $\{1, 2, \ldots, m\}$.

For each $v \in X^h$ and each $j$ we first define the set of time points $T_j(v) \subseteq (0, 1)$ as $T_j(v) = \{1 \mid \Phi(v, t, v) \in g_j\}$.

We next define $X_j$ as

$$X_j = \bigcup_{v \in X} \{\Phi(v, (1-t, \Phi(v, t, v)) \mid t \in T_j(v)\}. \quad (10)$$

Finally for each $h' \in H$ define $X_j^{h'}$ to be

$$X_j^{h'} = X_j \cap h'.$$

Next we denote by $P_{\tau_j(v)}$ the uniform probability over $T_j(v)$. Then the distribution $P_{X_j^{h'}}$ is given by:

Suppose $Y$ is a measurable subset of $X_j^{h'}$. Then

$$P_{X_j^{h'}}(Y) = \int_{v \in X^h} \int_{t \in T_j(v)} 1(\Phi(v, (1-t, \Phi(v, t, v)) \cap Y)) dP_{\tau_j(v)}(v) dP_{X_j^{h'}}. \quad (11)$$

We add the state $(\rho_j, X_j^{h'}, h', P_{X_j^{h'}})$ to $\Upsilon_{qt}$ provided $\mu(X_j^{h'}) > 0$. For each such state we add the triple

$$(\rho, X, h, P_X, \rho_j, \rho_j^{h'}, (\rho_j, X_j^{h'}, h', P_{X_j^{h'}}))$$

to $\Rightarrow_{qt}$ where $\rho_j^{h'}$ is given by

$$p_j^{h'} = \frac{\mu(X_j^{h'})}{\sum_{h'' \in H} \mu(X_j^{h''})} \int_{v \in X^h} \sum_{i \in I} \mu(T_i(v)) dP_{X_j^{h'}}. \quad (12)$$

Using arguments very similar to the ones used in Section 3 we can easily establish that $M_{qt}$ is a Markov chain whose state space has the structure of a finitely branching tree.

### 6.1 The two semantics

For interpreting BLTL formulas over $M_{qt}$ it will be convenient to assume the following syntax in which negation is immediately followed by a quantitative atomic proposition:

$$A \mid \neg A \mid \varphi_1 \lor \varphi_2 \mid \varphi_1 \land \varphi_2 \mid G_{\leq k} \varphi \mid F_{\leq k} \varphi \mid \varphi_1 U_{\leq k} \varphi_2.$$  

Clearly, every BLTL formula can be transformed into an equivalent formula that has the above syntax. This can be achieved by pushing negation inwards using equivalences such as $\neg(\varphi_1 \lor \varphi_2) \equiv \neg \varphi_1 \land \neg \varphi_2$, $G_{\leq k} \varphi \equiv F_{\leq k} \neg \varphi \land \neg (F_{\leq k} \varphi_2)$, etc.

The trajectory semantics is defined along previous lines but the atomic propositions are handled as follows. Let $\tau = (q_0, v_0) \ldots (q_k, v_k)$ be a finite trajectory and $0 \leq \ell \leq k$. Then $\tau, \ell \models_{H_{qt}} (x_i < c)$ iff $v_i(t) < c$. On the other hand $\tau, \ell \models_{H_{qt}} \neg (x_i < c)$ if $\tau, \ell \not\models_{H_{qt}} (x_i < c)$. The clauses for the other cases are defined in the obvious way. As before $\tau$ is a (trajectory) model of $\psi$ if $\tau \models T_{J_{\psi}}$ and $\tau, 0 \models_{H_{qt}} \psi$.

To interpret BLTL formulas over $M_{qt}$, let $\pi = \rho_0 \pi_1 \ldots \pi_k$ be a path in $M_{qt}$ with $\pi_0 = \epsilon$ and $\pi_k = (\rho_{in}, X_{qt}, h, P_X)$ for $0 \leq \ell \leq k$. Let $\psi$ be a BLTL formula and $0 \leq \ell \leq k$. Then $\pi, \ell \models_{\psi}$ is given by:

- $\pi, \ell \models_{\psi} (x_i < c)$ iff there exists $v \in X_\ell$ such that $v(t) < c$.
- $\pi, \ell \models_{\psi} \neg (x_i < c)$ iff there exists $v \in X_\ell$ such that $v(t) \geq c$.
- The remaining clauses are defined in the obvious way.

For $v \in \mathbb{R}^n$ let $v \models A$ denote the fact that $v(t) < c$ in case $A = (x_i < c)$ and $v(t) > c$ in case $A = (x_i > c)$. Next suppose $(\rho, X, h, P_X)$ is a state of $M_{qt}$ and $A \models_{H_{qt}} \psi$. Then $X \subseteq h$ by construction. Furthermore it is easy to check that $v \models A$ for every $v \in h$ or $v \not\models A$ for every $v \in h$. Thus the semantics defined above will be consistent in the sense it will be the case that either $\pi, \ell \models_{\psi} A$ or $\pi, \ell \models_{\psi} \neg A$ but not both.

Let $B$ be the set of paths of length $K + 2$ that start from the initial state of $M_{qt}$. Now we define $\text{models}_{\psi}(\psi) \subseteq B$ via: $\pi \in \text{models}_{\psi}(\psi)$ iff $\pi, 1 \models_{\psi}$.
the probability of satisfaction of a formula in $M_{gt}$. Let $\pi = \eta_0\eta_1 \ldots \eta_{K+1} \in \mathcal{B}$. Then $\Pr(\pi) = \prod_{0 \leq \ell < K} p_\ell$, where $\eta_\ell \downarrow \eta_{\ell+1}$ for $0 \leq \ell < K + 1$. This leads to

$$\Pr(\text{models}_{\text{qs}}(\psi)) = \sum_{\pi \in \text{models}_{\text{qs}}(\psi)} \Pr(\pi).$$

We let $M_{gt} \models \psi$ denote the fact $\Pr(\text{models}_{\text{qs}}(\psi)) = 1$.

### 6.2 The correspondence result

We shall relate the behavior of $H$ to that of $M_{gt}$ using the notion of robust trajectories. To start with, for $\psi \in \mathbb{R}^n$ we let $hc(\psi)$ be the hypercube $h$ in $\mathcal{H}$ such that $\psi \in h$. Since $\mathcal{H}$ is a partition of $\mathbb{R}^n$ we have that $hc(\psi)$ exists and is unique. In what follows we let $\ell$ range over $\{0, 1, \ldots, K\}$. We now define the equivalence relation $\cong$ on $TRJ^{K+1}$ as follows: Let $\tau, \tau' \in TRJ^{K+1}$ with $\tau(\ell) = (q_\ell, v_\ell)$ and $\tau'(\ell) = (q'_\ell, v'_\ell)$. Then $\tau \cong \tau'$ iff $q_\ell = q'_\ell$ and $hc(v_\ell) = hc(v'_\ell)$ for each $\ell$. We let $[\tau]$ denote the $\cong$-equivalence class containing $\tau$.

Next suppose $\tau \in TRJ^{K+1}$ is a trajectory with $\tau(\ell) = (q_\ell, v_\ell)$. Let $Q(\tau, \ell) = q_\ell$ and $V(\tau, \ell) = v_\ell$. Define $[\tau](\ell) = \{V(\tau', \ell) | \tau' \in [\tau]\}$. It is easy to verify that $[\tau](\ell)$ is a measurable set (but perhaps with measure 0) for each $\ell$.

The trajectory $\tau \in TRJ^{K+1}$ is said to be robust iff $\mu([\tau](\ell)) > 0$ for every $\ell$. We will say that $H$ robustly satisfies the specification $\psi$ and this is denoted by $H \models_R \psi$ if $\tau, 0 \models_H \psi$ for every robust trajectory $\tau$ in $TRJ^{K+1}$. It is now straightforward to show (along the lines of the proof of [11]) that:

**Theorem 4** $H \models_R \psi$ iff $M_{gt} \models \psi$.

Thus in terms of the sub-dynamics consisting of robust trajectories there is again a strong relationship between the behaviors of $H$ and $M_{gt}$. It also turns out that in measure-theoretic terms the non-robust trajectories can be ignored. More precisely if one starts with the discrete topology over $Q^{K+1}$ and the usual topology over $\mathbb{R}^{n+1}$ one can easily define a natural measure space over the product topology $Q^{K+1} \times \mathbb{R}^{n+1}$. In this space for every non-robust trajectory $\tau$ the representation of $[\tau]$ will be measurable but with measure 0. In this sense the contributions made by the non-robust trajectories to the dynamics of $H$ are negligible.

**The SMC procedure.** The SMC procedure remains the same. The only difference is we must sample robust trajectories. One can do so by discarding the value states that hit the constants mentioned in the quantitative atomic propositions and restarting the simulation from the previous time step. That this leads with probability 1 to the generation of a robust trajectory is easy to establish.

### 7. CASE STUDIES

We have implemented our method using MATLAB. The source code is available at [24]. The experiments were carried out on a PC with a 3.4GHz Intel Core i7 processor with 8GB RAM. We first evaluated our method on a room heating model adapted from [12]. We also applied our method a model of the electrical dynamics of the cardiac cell [7]. The $\Delta$ time step parameter for the room heating system and the cardiac cell model were set to 0.025, and 0.5, respectively. The parameters used for the statistical model checking were $\delta = 0.01$ and $\alpha = 0.01$, and hence the maximal sample size was set to $N = \lceil \log 0.01 / \log 0.99 \rceil = 459$. We used $J = 10$ as the number of intermediate time steps for choosing mode transitions (an empirical justification of this value is given in Section 7.3).

#### 7.1 Room heating system

Our system consists of 3 rooms and 2 heaters [12]. The temperature in each room depends on the temperature of the adjacent rooms, on the outside temperature and on whether a heater is in the room. Each room may have at most one heater and a heater is switched ON if the temperature is below a certain threshold, and OFF if it is above another threshold. When the temperature in a room falls below a certain level, it may get a heater from one of the adjacent rooms, provided that the room in that room is significantly higher.

The system dynamics is given by

$$\dot{x}_i = c_i h_i + b_i (u - x_i) + \sum_{j \neq i} a_{i,j} (x_j - x_i),$$

where $x_i$ is the temperature in room $i$, $h_i$ is 1 when a heater is switched ON in room $i$ (0 otherwise) and $u$ denotes the outside temperature. The system has a total of 12 modes corresponding to the locations of the 2 heaters and whether each heater is ON or OFF. Additional details about model parameters can be found in the Appendix.

**Property R1** Initially, heaters are in room 1 and room 2, and no heater will be moved within 5 days.

$$G^{\leq 5}(\text{[Heater in R1]} \land \text{[Heater in R2]})$$

The property was verified to be true when the outside temperature is $\geq 16^\circ C$. However, for an outside temperature of 4$^\circ C$, the property evaluates to false. The next property involves quantitative atomic propositions.

**Property R2** The temperature in all three rooms stabilizes within 1 day between 18 and 22 degrees, and stays in that range for 4 days.

$$F^{\leq 1}(G^{\leq 4}([18 < x_1 < 22] \land [18 < x_2 < 22] \land [18 < x_3 < 22]))$$

The property was verified to be true for an outside temperature of $\geq 16^\circ C$. However, the property was verified to be false with an outside temperature of 4$^\circ C$.

#### 7.2 Cardiac cell model

Cardiac muscle cells enable the heart to beat and pump blood throughout the body. Heart rhythm depends on the organized opening and closing of gates–called ion channels–on the cell membrane, which govern the electrical activity of cardiac cells. Disordered electric wave propagation in heart muscle can cause cardiac abnormalities such as tachycardia.
and fibrillation. The dynamics of the electrical activity of a single cardiac cell has been modeled as a hybrid automaton shown in Figure 3. The model contains 4 state variables and 26 parameters. The parameters of the model are summarized in Table 2 in the Appendix. An action potential (AP) is a change in the cell’s transmembrane potential $u$, as a response to an external stimulus (current) $\epsilon$. The flow of total currents is controlled by a fast channel gate $v$ and two slow gates $w$ and $s$.

In mode $q_0$, the “Resting mode”, the cell is waiting for stimulation. We assume an external stimulus $\epsilon$ equal to 1 mV lasting for 1 millisecond. The stimulation causes $u$ to increase which may trigger a mode transition to mode $q_1$. In mode $q_1$, gate $v$ starts closing and the decay rate of $u$ changes. The system will jump to mode $q_2$ if $u \geq \theta_w$. In mode $q_2$, gate $w$ is also closing. When $u \geq \theta_w$, mode $q_3$ can be reached, which means a successful “AP initiation”. In mode $q_3$, $u$ reaches its peak due to the fast opening of a sodium channel. The cardiac muscle then contracts and $u$ starts decreasing.

**Property C1** It is known that the cardiac cell can lose its excitability, which will lead to disorders such as ventricular tachycardia and fibrillation. We formulated the property for responding to stimulus by leaving the resting mode:

$$F^{\leq 500}(\neg \text{[Resting mode]}).$$

The property was verified to be true under the healthy condition. However, under a disease condition (for example $\tau_{v1} = 0.004$ or $\tau_{v2} = 0.1$ [22]) the property was verified to be false no matter what stimulation value of $\epsilon$ was used. Consequently, a region of such unexcitable cells blocks the impulse conduction and can lead to cardiac disorders such as fibrillation. This is consistent with experimental results reported in [26].

**Property C2** After successfully generating an AP with transmembrane potential above 1.2, the cardiac cell should return to transmembrane potential below 0.006 and wait for the next stimulation. The corresponding formula (which uses quantitative propositions) is

$$F^{\leq 500}([1.2 \leq u]) \land F^{\leq 500}((G^{\leq 100}([u \leq 0.006]))).$$

The above query was verified to be true under the healthy condition and transient stimulation. However, if we change the stimulation profile from transient to sustained, i.e. assuming $\epsilon$ lasts for 500 milliseconds, the property was verified to be false—the cell doesn’t return to and settle at a low transmembrane potential resting state. In ventricular tissue the stimulus $\epsilon$ can be delivered from neighboring cells [7].

Thus, our results suggest that the transient activation of a single cardiac cell depends on the stimulation profile of its neighboring cells.

### 7.3 Performance

The overall run times for verifying the properties are summarized in Table 1. Our current implementation is a simple sequential one. The performance can be considerably improved through an optimized parallel implementation.

| Property | Condition | Decision | # samples before stopping | SMC Run-time [s] |
|----------|-----------|----------|--------------------------|------------------|
| R1       | Outside 16 °C | True     | 459                      | 195              |
| R1       | Outside 4 °C  | False    | 3                        | 1.23             |
| R2       | Outside 16 °C | True     | 459                      | 200.2            |
| R2       | Outside 4 °C  | False    | 1                        | 0.42             |
| C1       | Healthy     | True     | 459                      | 1570             |
| C1       | Diseased    | False    | 1                        | 3.52             |
| C2       | Transient   | True     | 459                      | 1523             |
| C2       | Sustained   | False    | 1                        | 3.58             |

**Table 1: Performance of SMC for hybrid systems**

In our experiments, we used $J = 10$ as the number of intermediate time steps for choosing mode transitions. We investigated whether this choice is sufficient for accurate simulation. We simulated 1000 independent realizations of the cardiac cell system with $J = 10$ and $J = 100$, and compared the distributions of the modes that the system is in at a series of discrete time points. The Kolmogorov-Smirnov statistical test did not reject the hypothesis that the two distributions are the same (at confidence level 95%). This indicates that using $J = 10$ is adequate.

### 8. CONCLUSION

We have presented an approximate probabilistic verification method for analyzing the dynamics of a hybrid system $H$ in terms of a Markov chain $M$. For bounded time properties, we have shown a strong correspondence between $H$ and $M$, namely $H$ meets the BLTL specification $\psi$ iff $M$ meets $\psi$ with probability 1. We have also extended this result to handle quantitative atomic propositions and shown a similar correspondence result for the sub-dynamics consisting of robust trajectories. Thus the intractable verification problem for $H$ can be solved approximately using its Markov chain approximation. Accordingly, we have devised a statistical model checking procedure to verify that $M$ almost certainly meets a BLTL specification and then applied this procedure to two examples to demonstrate the applicability of our approximation scheme. A parallel implementation of the trajectory sampling procedure—which should be easy to work out—will considerably improve the performance and scalability of our method.

As an extension, one could consider more sophisticated stochastic assumptions regarding the time points and value states at which the mode transitions take place. Further, we have assumed here a closed system setting in which there is no distinction made between controllable and uncontrollable transitions. However, especially for cyber physical systems a subset of the mode transitions will be controllable. Hence it will be fruitful to extend our technique to this setting and study controller synthesis problems. It will however involve MDPs instead of Markov chains as approximations and hence will require new machinery.

It will be easy to extend our results to bounded PCTL [7] specifications. It is also easy to define the Markov chain approximation of $H$ for infinite trajectories. However, relating the behavior of $H$ to its Markov chain approximation when the specification logic is LTL or PCTL appears to be a hard problem.
Figure 3: The hybrid automaton model for the cardiac cell system [16].

9. REFERENCES

[1] A. Abate, A. D. Ames, and S. S. Sastry. Stochastic approximations of hybrid systems. In ACC’05, pages 1557–1562, 2005.

[2] M. Agrawal, F. Stephan, P. Thiagarajan, and S. Yang. Behavioural approximations for restricted linear differential hybrid automata. In HSCC’06, pages 4–18, 2006.

[3] R. Alur, T. A. Henzinger, G. Lafferriere, and G. J. Pappas. Discrete abstractions of hybrid systems. P. IEEE, 88(7):971–984, 2000.

[4] P. Ballarin, H. Dijfri, M. Duflot, S. Haddad, and N. Pekergin. COSMOS: a statistical model checker for the hybrid automata stochastic logic. In QEST’11, pages 143–144, 2011.

[5] A. Biere, A. Cimatti, E. Clarke, and Y. Zhu. Symbolic model checking without bdds. In Intl. Conf. on Tools and Algorithms for the Analysis and Construction of Systems (TACAS’99), volume 1579. Springer, 1999.

[6] H. A. Blom, J. Lygeros, M. Everdij, S. Loizou, and K. Kyriakopoulos. Stochastic hybrid systems: Theory and safety critical applications. Springer Heidelberg, 2006.

[7] A. Bueno-Orovio, E. M. Cherry, and F. H. Fenton. Minimal model for human ventricular action potentials in tissue. J. Theor. Biol., 253:544–560, 2008.

[8] C. G. Cassandras and J. Lygeros. Stochastic hybrid systems. CRC Press, 2010.

[9] E. Clarke, A. Fehnker, Z. Han, B. Krogh, O. Stursberg, and M. Theobald. Verification of hybrid systems based on counterexample-guided abstraction refinement. In TACAS’03, pages 192–207, 2003.

[10] E. M. Clarke, O. Grumberg, and D. A. Peled. Model checking. MIT press, 1999.

[11] A. David, D. Du, K. G. Larsen, A. Legay, M. Mikučionis, D. B. Poulsen, and S. Sedwards. Statistical model checking for stochastic hybrid systems. In HSB’12, pages 122–136, 2012.

[12] A. Fehnker and F. Ivančić. Benchmarks for hybrid systems verification. In Hybrid Systems: Computation and Control, pages 326–341, Springer, 2004.

[13] G. Frehse. Phaver: Algorithmic verification of hybrid systems past hytech. In HSCC’05, pages 258–273, 2005.

[14] S. Gao, S. Kong, and E. Clarke. Delta-complete reachability analysis (part i). In Technical report, CMU SCS, CMU-CS-13-131, 2013.

[15] A. Girard, C. Le Guernic, and O. Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. In HSCC’06, pages 257–271, 2006.

[16] R. Grosu, G. Batt, F. H. Fenton, J. Gilmum, C. L. Guernic, S. A. Smolka, and E. Bartocci. From cardiac cells to genetic regulatory networks. In CAV’11, pages 396–411, 2011.

[17] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. Formal aspects of computing, 6(5):512–535, 1994.

[18] T. A. Henzinger. The theory of hybrid automata. In LICS’96, pages 278–292, 1996.

[19] T. A. Henzinger and P. W. Kopke. Discrete-time control for rectangular hybrid automata. Theor. Comput. Sci., 221(1):369–392, 1999.

[20] M. Hirsch, S. Smale, and R. Devaney. Differential equations, dynamical systems, and an introduction to chaos. Academic Press, 2012.

[21] A. A. Julius and G. J. Pappas. Approximations of stochastic hybrid systems. IEEE T. Automat. Contr., 54(6):1193–1203, 2009.

[22] B. Liu, S. Kong, S. Gao, and E. M. Clarke. Parameter identification using delta-decisions for hybrid systems in biology. In preparation.

[23] S. Palaniappan, B. Gyori, B. Liu, D. Hsu, and P. Thiagarajan. Statistical model checking based calibration and analysis of bio-pathway models. In CMSB’13, pages 120–134, 2013.

[24] W. Stephen. General topology, 1970.

[25] Supplementary information and source code. http://www.comp.nus.edu.sg/~rpsysbio/hybrid/

[26] K. Tanaka, S. Zikovier, K. L. Vikstrom, M. Yamazaki, J. Moreno, M. Klos, A. V. Zaitsev, R. Vaidyanathan, D. S. Auerbach, S. Landas, G. Guiraudon, J. Jalife, O. Berenfeld, and J. Kalifa. Spatial distribution of fibrosis governs fibrillation wave dynamics in the posterior left atrium during heart failure. Circ. Res., 8(101):839–847, 2007.
Appendix

Proofs for Section 4

Lemma 1. Suppose the path $\pi = \eta_0\eta_1\ldots\eta_k$ in $M$ and the trajectory $\tau = (q_0, v_0), (q_1, v_1), \ldots, (q_k, v_k)$ are compatible. Let $0 \leq j \leq k$ and $\psi$ be a BLTL formula. Then $\pi \models M_j \iff \tau \models H_j$.

2. Suppose $\pi$ is a path in $M$. Then there exists a trajectory $\tau$ such that $\pi$ and $\tau$ are compatible. Furthermore if $\pi \in paths_M$ then $\tau \in TRJ$.

3. Suppose $\tau$ is a trajectory. Then there exists a path $\pi$ in $M$ such that $\pi$ and $\tau$ are compatible. Furthermore if $\tau \in TRJ$ then $\pi \in paths_M$.

Proof. To prove the first part we note that if $A$ is an atomic proposition then $\pi \models M_j A \iff A \in \mathcal{K}T(\pi_j) \iff \tau \models H_j A$. We next note that the suffix of length $m$ of $\pi$ will be compatible with the suffix of length $m$ of $\tau$ whenever $\pi$ and $\tau$ are compatible. The result now follows at once by structural induction on $\psi$.

To show the second part let $\pi = \eta_0\eta_1\ldots\eta_k$ be a path in $M$ with $\eta_j = (q_0, v_0), (q_1, X_1, P_{X_j})$ for $0 \leq j \leq k$. Clearly $X_1$ is non-empty for $0 \leq j \leq k$ since $\eta_j \in \mathcal{T}$ implies $\mu(X_j) > 0$.

We proceed by induction on $k$. If $k = 0$ then we can pick $v_0 \in X_0$ and the trajectory $(q_0, v_0)$ will be compatible with $\tau$. So assume $k > 0$. Then by the induction hypothesis there exists a trajectory $(q_1, v_1)(q_2, v_2)\ldots(q_k, v_k)$ which is compatible with the path $\eta_1\eta_2\ldots\eta_k$. Let $q_0 \rightarrow q_1$. Since $v_1 \in X_1$ there must exist $v_0 \in X_0$ and $t \in (0, 1)$ such that $P_{\eta_0,t}(v_0) \in g$ and $v_1 = (\Phi_{q_1,1-t}(\Phi_{q_0,t}(v_0)))$. Clearly $v_0v_1\ldots v_k$ is a trajectory that is compatible with $\pi$. The fact that $\tau \in TRJ$ if $\pi \in paths_M$ follows from the definition of compatibility.

To prove the third part let $\tau = (q_0, v_0), (q_1, v_1), \ldots, (q_k, v_k) \in TRJ$. Again we proceed by induction on $k$. Suppose $k = 0$. Then $(\eta_0, INIT, P_{INIT})$ is in $paths_M$ which is compatible with $\tau$. So suppose $k > 0$. Then by the induction hypothesis there exists $\pi' = \eta_0\eta_1\ldots\eta_{k-1}$ such that $\pi'$ is compatible with $\tau' = (q_0, v_0)(q_1, v_1)\ldots(q_{k-1}, v_{k-1})$. Let $q_{k-1} \rightarrow q_k$. Since $X_{k-1}$ is open there exists an open neighborhood $Y \subseteq X_{k-1}$ which contains $v_{k-1}$. But then both $\Phi_{q_{k-1},1-t}(Y)$ and $\Phi_{q_k,1-t}(Y \cap g)$ should be open and non-empty (since $g$ is open and $(q_k, v_k)$ is part of the trajectory). Hence $Y' = \bigcup_{c \in (0,1)} \Phi_{q_k,1-t}(\Phi_{q_{k-1},1-t}(Y \cap g))$ is a non-empty open set with a positive measure. Hence there will be a state of the form $\eta_k = (p_k, X_k, P_{X_k})$ in $\mathcal{T}$ with $Y' \subseteq X_k$ and $\eta_{k-1} \rightarrow \eta_k$ for some $p \in (0, 1]$. Clearly $\pi = \pi'\eta_k \in paths_M$ and is compatible with $\tau$. Again the fact that $\pi \in paths_M$ if $\tau \in TRJ$ follows from the definition of compatibility.

Proofs for Section 6

First the following properties of the Markov chain $M_{qt}$ can easily be proved along the lines of the proof of Theorem 3.

Lemma 2. 1. $X^h_j$ is open and is of finite measure for each $j$ and each $h \in \mathcal{H}$.

2. If $(pq_j, X^h_j, h, P_{X^h_j}) \in T_{qt}$ then $\mu(X^h_j) > 0$.

3. $P_{X^h_j}$ is a probability distribution for each $j$ and each $h \in \mathcal{H}$.

4. $M_{qt} = (\mathcal{Y}_{qt}, \Rightarrow_{qt})$ is an infinite state Markov chain whose underlying graph is a finitely branching tree.

We wish to show that for quantitative specifications, $H$ robustly satisfies a BLTL specification $\psi$ if and only if $M_{qt}$ satisfies $\psi$ with probability 1. We begin with:

Lemma 3. Let $\tau = (q_0, v_0), (q_1, v_1), \ldots, (q_K, v_K) \in TRJ^{K+1}$. Then the following statements are equivalent.

1. $\tau$ is robust.

2. There exist open sets of non-zero measure $O_j$ and $b_j \in \mathcal{H}$ such that $v_j \in O_j \subseteq [\tau(j)] \subseteq b_j$ for $0 \leq j \leq K$.

3. $\psi(i) \notin C_i$ for every $j \in \{0, 1, \ldots, K\}$ and every $i \in \{1, 2, \ldots, n\}$.

Proof. In what follows we let $j$ range over $\{0, 1, \ldots, K\}$. Suppose $\tau$ is robust. Let $hc(\psi_j) = b_j$ for each $j$. By the definition of $\approx$, we have $v_j \in [\tau(j)] \subseteq b_j$ for each $j$. Since $\mu([\tau(j)]) > 0$ we have $\mu(b_j) > 0$ for each $j$. This implies that $b_j(i)$ is a finite open interval for $1 \leq i \leq n$. Then $[\tau(j)] \subseteq b_j$ and $\mu([\tau(j)]) > 0$ now together imply that there exists a non-empty open set $O_j$ of finite measure such that $v_j \in O_j \subseteq [\tau(j)]$ for each $j$. Thus (1) implies (2).

Next suppose part (2) of the lemma holds. Then $\mu([\tau(j)]) > 0$ for each $j$. Thus $\tau$ is robust and we have (2) implies (1).

To show that (2) implies (3) assume that $v_j(i) \in C_i$ for some $j$ and $i$. Then $hc(\psi_j) = b_j$. We need to find $b_j$ and an open set of non-zero measure such that $v_j \in O_j \subseteq [\tau(j)] \subseteq b_j$. This implies $hc(\psi_j) = b_j$. But then $\mu(b_j)$ implies there can exist an open set $O_j$ of non-zero measure satisfying $v_j \in O_j \subseteq b_j$. Hence (2) can not hold and this shows (2) implies (3).

Next suppose (3) holds. Let $b_j = hc(\psi_j)$ for each $j$. Then (3) implies $\mu(b_j) > 0$ for each $j$. Let $\tau^{(j)}$ be the $j$-length prefix of $\tau$ for each $j$.

Since INIT is open $O_0 = INIT \cap b_0$ is open. It is non-empty since $v_0 \in O_0$ and hence has non-zero measure. Furthermore $[\tau^{(0)}](0) = O_0$. We now have $v_0 \in O_0 \subseteq [\tau^{(0)}](0) \subseteq b_0$. Assume inductively $0 < j < K$ and for $0 \leq k \leq j$ there exist open sets $O_k$ of non-zero measure such that $v_k \in O_k \subseteq [\tau^{(j)}](k) \subseteq b_k$.

Since $\tau$ is a trajectory there exist $q_j \rightarrow q_{j+1}$ and $\Phi_{q_j,t_j}(v_j) \in v_j$ and $v_{j+1} = \Phi_{q_{j+1},1-t_j}((\Phi_{q_j,t_j}(v_j)))$. Let $Y_j = [\tau^{(j)}](j)$ and $Y_{j+1} = \bigcup_{c \in (0,1)} \Phi_{q_{j+1},1-t_j}(\Phi_{q_j,t_j}(v_j)) \subseteq \mathcal{Y}(v)$ where $\mathcal{Y}(v) = \{\Phi_{q_j,t}(v) \in g\}$. Clearly $[\tau^{(j+1)}](1) = Y_{j+1} \cup \mathcal{H}_{j+1}$. Next define $O_{j+1} = \Phi_{q_{j+1},1-t_j}(\mathcal{O}_j)$. Since both $\Phi_{q_{j+1},1-t_j}$ and $\Phi_{q_j,t_j}$ are continuous bijections, $O_{j+1}$ is an open set and $v_{j+1} \in O_{j+1}$. Let $O_{j+1} = O_{j+1} \cap b_{j+1}$. Since $v_{j+1} \in b_{j+1}$ and $b_{j+1}$ is open we have $O_{j+1}$ open and non-empty and hence with non-zero measure.


Further $O_{j+1} \subseteq [\tau^{(j+1)}](j+1) \subseteq h_{j+1}$. This establishes the induction hypothesis and hence (3) implies (2).

We define the notion of compatibility as before. Let $\pi = \eta_0 \eta_1 \ldots \eta_k$ be a path in $M_{q_\tau}$ with $\eta_j = (q_0 q_1 \ldots q_{j-1}, X^{\eta_j}_{\eta_j}, h_j, Pr_{X^{\eta_j}_{\eta_j}})$ for $0 < j \leq k$, and $\eta_0 = \epsilon$. Let $\tau = (q_0, v_1)(q_2, v_2) \ldots (q_k, v_k)$ be a trajectory. Then we say that $\pi$ and $\tau$ are compatible iff $k = k'$ and for $1 \leq j \leq k$, $q_j = q'_j$ and $v_j \in X^{\eta_j}_{\eta_j}$. As it will turn out, if $\pi$ and $\tau$ are compatible then $\tau$ will be robust.

In what follows we shall assume that our BLTL specifications involve only quantitative atomic propositions in $AP_{q_\tau}$ and the formulas obey the syntax in which negation is immediately followed by an atomic proposition. Further the semantic notions $\models_H$ and $\models_{M_{q_\tau}}$ (abbreviated as $\models_{q_\tau}$) are defined in the expected way.

**Lemma 4.** 1. Suppose the trajectory $\tau = (q_1, v_1)(q_2, v_2) \ldots (q_k, v_k) \in TRJ$ and the path $\pi = \eta_0 \eta_1 \ldots \eta_k$ in $M_{q_\tau}$ with $\eta_0 = \epsilon$ are compatible. Let $\psi$ be a BLTL specification and $j \in \{1, \ldots, k\}$. Then $\tau, j \models_H \psi$ iff $\pi, j \models_{q_\tau} \psi$.

2. Suppose $\pi$ is a path in $M_{q_\tau}$ starting from $\epsilon$. Then there exists a robust trajectory $\tau$ in $TRJ$ such that $\pi$ and $\tau$ are compatible.

3. Suppose $\tau$ is a robust trajectory in $TRJ$. Then there exists a path $\pi$ in $M_{q_\tau}$ starting from $\epsilon$ such that $\pi$ and $\tau$ are compatible.

**Proof.** 1. From the definitions it follows that if $A \in AP_{q_\tau}$ and $h \in H$ then $v \models A$ for every $v \in h$ or $v \models \neg A$ for every $v \in h$ but not both. Since $v_j \in h_j$ we then have $\tau, j \models_H A$ iff $\pi, j \models_{q_\tau} A$ and $\tau, j \models_H \neg A$ iff $\pi, j \models_{q_\tau} \neg A$ for every atomic proposition. The remaining cases now follow easily by structural induction on $\psi$.

2. Let $\pi = \eta_0 \eta_1 \ldots \eta_k$ in $M_{q_\tau}$ with $\eta_0 = \epsilon$ and $\eta_j = (q_0 q_1 \ldots q_{j-1}, X^{\eta_j}_{\eta_j}, h_j, Pr_{X^{\eta_j}_{\eta_j}})$ for $0 < j \leq k$. For notational convenience we will write $X_j$ instead of $X^{\eta_j}_{\eta_j}$.

Since $\mu(X_k) > 0$ we can fix $v_k \in X_k$. Further fix $b_k$ being a product of open intervals in $\mathbb{R}$ with $X_k \subseteq b_k$, we can find an open set $O_k$ of non-zero measure such that $v_k \in O_k \subseteq X_k$. Thus we have $v_k \in O_k \subseteq X_k \subseteq b_k$.

From the construction of $M_{q_\tau}$ it follows there exists $q_{k-1} \to q_k$ and $T(v) \subseteq (0,1)$ for each $v \in X_k$ such that $\Phi_{q_{k-1},q_k}(v) \subseteq g$ for every $t \in T(v)$. Let $X_{k-1} = \bigcup_{v \in X_k} \Phi_{q_{k-1},q_k}^{-1}(\Phi_{q_{k-1},q_k}(v))$. From the construction of it follows that $Y_{k-1} \subseteq X_{k-1}$.

Next let $O_{k-1} = \bigcup_{v \in O_k} \Phi_{q_{k-1},q_k}^{-1}(\Phi_{q_{k-1},q_k}^{-1}(v))$. Clearly $O_{k-1}$ is an open set of non-zero measure with $O_{k-1} \subseteq Y_{k-1}$.

Moreover we can fix $v_{k-1} \in O_{k-1}$ such that $\Phi_{k-1,k}(v_k) = \Phi_{k-1,k}(v_{k-1})$ for some $t \in T(v_k)$. Continuing this way we can find $v_j, O_j, Y_j$ for $1 \leq j \leq k$ with $Y_k = X_k$ such that $\tau = (q_1, v_1)(q_2, v_2) \ldots (q_k, v_k)$ is a trajectory and $v_j \in O_j \subseteq Y_j \subseteq h_j$ for $1 \leq j \leq k$. From the construction of $M_{q_\tau}$ it follows that $Y_j = [\tau](j)$ for $1 \leq j \leq k$. From Lemma 3 it follows that $\pi$ and $\tau$ are compatible. It is also clear due to Lemma 3 that $\tau$ is robust.

3. Suppose $\tau = (q_0, v_1)(q_2, v_2) \ldots (q_k, v_k) \in TRJ$ is robust. Then by Lemma 3 there exist open sets $O_j$ of non-zero measure and $h_j \in H$ such that $v_j \in O_j \subseteq [\tau](j) \subseteq b_j$ for $1 \leq j \leq k$. Let $\tau^{(j)}$ denote the $j$-length prefix of $\tau$ for $1 \leq j \leq k$. We now define $X_j = [\tau^{(j)}](j)$ for $1 \leq j \leq k$. Then using the construction of $M_{q_\tau}$ it is easy to show that there exists distributions $Pr_j$ over $X_j$ such that $\pi = \eta_0 \eta_1 \ldots \eta_k$ is a path in $M_{q_\tau}$ with $\eta_j = (q_j, X_j, h_j, Pr_j)$ for $1 \leq j \leq k$ and that $\pi$ is compatible with $\tau$.

We can now prove Theorem 4.

**Theorem 4.** $H \models_H \psi$ iff $M_{q_\tau} \models_{q_\tau} \psi$.

**Proof.** Suppose $H \not\models_H \psi$. Then there exists $\tau \in TRJ$ such that $\tau$ is robust and $\tau, 0 \not\models_H \psi$. By Lemma 3 there exists a path $\pi$ in $M_{q_\tau}$ which is compatible with $\tau$. Hence again by Lemma 3 we then have $\pi \notin \models_{M_{q_\tau}} \psi$ which leads to $Pr_{<1}(\psi)$. Next suppose that $Pr_{<1}(\psi)$. Then there exists a path $\pi$ in $M_{q_\tau}$ such that $\pi, 1 \not\models_{M_{q_\tau}} \psi$. By Lemma 3 there exists a robust trajectory $\tau$ which is compatible with $\pi$ and $\tau, 0 \not\models_H \psi$. This implies $H \not\models_H \psi$.

Finally, we wish to show that the number of non-robust trajectories are negligible compared with the robust ones. Hence they do not contribute much towards the dynamics of $H$. For that we need the following lemma.

**Lemma 5.** Suppose $\tau = (q_0, v_0)(q_1, v_1) \ldots (q_k, v_k)$ is a non-robust trajectory and $\tau^{(j)}$ is the $j$-length prefix of $\tau$ for $1 \leq j \leq k$. Let $h_j = he(v_j)$ and $Y_j = [\tau^{(j+1)}](j+1)$ for $0 \leq j \leq k$. Then $Y_j$ is measurable and $Y_j \subseteq b_j$ for $0 \leq j \leq k$. Furthermore $Y_j$ is of measure $0$ for each $j$ in $\{0, 1, \ldots, k\}$.

**Proof.** Since $\tau$ is not robust, there exists $j : 0 \leq j \leq k$ such that $v_j(i) = c_i \in C_i$ for some $i$ and hence for all $v \in h_j$, $\psi(i) = c_j$ which implies $\mu(h_j) = 0$. We induct on $j$. For $j = 0$, $Y_0 = INIT \cap h_0$ is measurable and has measure $0$. Suppose $q_0 \to q_1$ and let $Y'_j = \bigcup_{v \in Y_j} \Phi_{q_{j-1},q_j}^{-1}(\Phi_{q_{j-1},q_j}(v)) \cap T(v)$ where $T(v) = \{ t \mid \Phi_{q_{j-1},q_j}(v) \in g \}$. Then $Y_j = Y_j \cap b_j$. Let $Y_j = \Phi_{q_0}(0,1) \times \Phi_{q_0}(0,1) \cap T(v)$. Since $\mu(Y_j) = 0$ hence $\mu((0,1) \times X_j) = 0$. Now both $\Phi_{q_0}$ and $\Phi_{q_0}$ are Lipschitz, and hence $\mu(Y_j) = 0$ since the image of a set of measure $0$ has measure $0$ under a Lipschitz function. Now note that $Y_j \subseteq X_j$ and hence $Y_j$ is measurable and $\mu(Y_j) = 0$.

Continuing this way we can show that $Y_j$ is measurable for all $j : 2 \leq j \leq k$ and $\mu(Y_j) = 0$.

Next suppose $j > 0$. By a similar argument we can show that $Y_j$ is measurable for all $j < k$ and $\mu(Y_j) = 0$. Let $q_{j-1} \to q_j$ and let $Y'_{j-1} = \bigcup_{v \in Y_{j-1}} \Phi_{q_{j-1},q_j}^{-1}(\Phi_{q_{j-1},q_j}(v)) \cap T(v)$ where $T(v) = \{ t \mid \Phi_{q_{j-1},q_j}(v) \in g \}$. Then $Y_{j-1} = Y'_{j-1} \cap T(v)$.
Thus by the above lemma, if a trajectory $\tau \in TRJ^{K+1}$ is not robust then there exists a $j \in \{0, 1, \ldots, K\}$ such that $\mu(Y_j) = 0$. This implies that in the product topology of $Q^{K+1} \times \mathbb{R}^{K+1}$, $[\tau]$ has measure 0. Thus, the contribution made by the non-robust trajectories to the dynamics of $H$ is negligible.

**Trajectory simulation for quantitative specifications**

Algorithm 3 gives the procedure for simulating robust trajectories for the verification of qualitative BLTL specifications. By Lemma 3, a trajectory is robust iff it does not hit any of the constants mentioned in the atomic propositions. The procedure is the same as Algorithm 1 before, except that whenever a value state $v_k$ at any time step $k$ hits a constant mentioned in any of the atomic propositions, we discard $v_k$ and start the simulation again from the value state of the previous time step.

**Algorithm 3** Robust trajectory simulation

Input: Hybrid automaton $H = (Q, q_0, (F_q(x))_{q \in Q}, \Phi, \rightarrow, \text{INIF})$, maximum time step $K$.
Output: Trajectory $\tau$.
1. Sample $v_0 \in \text{INIT}$ uniformly. If $v_0(i) \notin C_i$ for any $i$, repeat.
2. Set $q_{0} := q_{00}$ and $\tau := (q_{0}, v_{0})$.
3. for $k := 1, \ldots, K$ do
   4. repeat
      5. Generate time points $T := \{t_1, \ldots, t_J\}$ uniformly in $(0, 1)$.
      6. Simulate $\nu^i := \Phi_{q_{k-1}}(t_k, v_{k-1})$, for $i \in \{1, \ldots, J\}$
      7. Let $T_j := \{t \in T : \nu^i \in g_j\}$ be the time points where $g_j$ is enabled.
      8. Pick $g_k$ randomly according to probabilities $p_j := \frac{|T_j|}{\sum_{j=1}^{\phi} |T_j|}$.
      9. Pick $t_k$ uniformly at random from $T_j$.
      10. Simulate $\nu'^i := \Phi_{q_{k}}(1-t_k, \nu^k)$, where $q'$ is the target of $g_k$.
      11. until $\nu'^i \notin \text{C}_i$ for any $i$
6. Set $q_k := q'$, $v_k := \nu'$, and extend $\tau := (q_0, v_0) \ldots (q_k, v_k)$.
12. end for
13. return $\tau$

To see that the algorithm terminates with probability 1, note that if $v_0 \in h$ and $h(i) = \{c\}$ for some $c \in C_i$, then $\mu(h) = 0$. Thus Step 1 repeats with probability 0. As a result with probability 1 it will be repeated only a finite number of times. Similarly the repeat loop of Step 4-11 will terminate with probability 1.

**Room heating system**

The heaters are switched ON or OFF, and moved from one room to another based on temperature thresholds. For each room we define two thresholds $on_i$ and $off_i$. The heater in room $i$ is ON if $x_i \leq on_i$ and OFF if $x_i \geq off_i$. A heater is moved from room $j$ to an adjacent room $i$ if the following holds: room $i$ has no heater, room $j$ has a heater, temperature $x_i \leq get_i$, and the difference $x_j - x_i \geq diff_i$.

We set the initial temperature to be uniformly distributed in the interval [20, 20.5] in all 3 rooms. We use the model parameters as they appear in [12], which are as follows.

$$a = \begin{pmatrix} -0.9 & 0.5 & 0 \\ 0.5 & -1.3 & 0.5 \\ 0 & 0.5 & -0.9 \end{pmatrix}, b = \begin{pmatrix} 0.4 \\ 0.3 \\ 0 \end{pmatrix}, c = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 8 \end{pmatrix}.$$  

Further, $off_i = 21$, $on_i = 20$, $get_i = 18$, and $diff_i = 1$.

**Cardiac cell model**

| Parameter | Value | Parameter | Value |
|-----------|-------|-----------|-------|
| $\theta_a$ | 0.006 | $\tau_v^1$ | 60 |
| $\theta_w$ | 0.13 | $\tau_v^2$ | 1150 |
| $\theta_c$ | 0.3 | $\tau_w^1$ | 60 |
| $\tau_{-}$ | 0.03 | $\tau_w^2$ | 15 |
| $\tau_{so}$ | 0.65 | $\tau_{so1}$ | 400 |
| $\tau_{p}$ | 0.9078 | $\tau_{so2}$ | 30.0181 |
| $\tau_{u}$ | 1.55 | $\tau_{so2}$ | 0.9957 |
| $\tau_{w}$ | 0.94 | $\tau_{w}$ | 2.7342 |
| $\tau_{m}$ | 65 | $\tau_{w}$ | 16 |
| $\tau_{ao}$ | 2.458 | $\tau_{w}$ | 0.11 |
| $\tau_{s}$ | 2.994 | $\tau_{w}$ | 1.8875 |
| $\tau_{w}$ | 1.4506 | $\tau_{w}$ | 0.07 |

Table 2: Parameter values of the cardiac cell model under healthy condition