Formal Semantics of Hybrid Automata
Technical Report

Manasvi Saxena¹, Nishant Rodrigues¹, Xiaohong Chen¹, and Grigore Roșu¹

¹ University of Illinois at Urbana Champaign
² {msaxena2, nishant2, xc3, grosu}@illinois.edu

Abstract. Hybrid Automata (HA) form the backbone of modeling systems with both discrete and continuous components. However, the semantics of HA are usually described loosely using Labeled Transition Systems (LTS), and reasoning about HA involves informal proofs over LTS. In this paper, we propose a formally rigorous, concise, and semantically correct definition of HA in Matching Logic (ML), which is a uniform logic for programming languages design and verification. We show how our definition allows formal reasoning about HA using ML’s proof system. Our approach exposes HA to a rich set of tools that operate over ML and provide a sound logical basis for various techniques like Deductive Verification, Monitoring and Runtime Verification.

1 Introduction

The framework of Hybrid Automata is widely used to model dynamical systems - systems that combine discrete dynamics with continuous dynamics. Cyber Physical Systems (CPS), or systems that combine cyber capabilities (computation, communication and control) with physical capabilities (motion or other physical processes) are examples of such dynamical systems. In recent years, CPS are increasingly being employed to tackle challenges in domains like medicine, transportation and energy. The use of CPS in safety critical applications, however, makes their correctness and reliability extremely important. Moreover, the inherent complexity of CPS make their analysis challenging. HA have been instrumental in addressing these challenges by providing an intuitive mechanism for modeling CPS, and have become central to a rich ecosystem of CPS analysis tools [5,9,6,10].

In this paper, we propose a formally rigorous, and semantically correct definition of HA. Our approach is centered around embedding HA in Matching Logic (ML) [4]. Given a HA $H$ as described in [8], we derive a ML theory $Γ^H$ from $H$ such that Labeled Transition System (LTS) of $H$ is an ML-model of $Γ^H$. Intuitively, $Γ^H$ can be thought of as an axiomatization of $H$’s transition relation. Since $Γ^H$ is an ML theory, we can use ML’s proof system to formally reason about $H$.

We now briefly describe the paper’s layout. In 2 we describe relevant mathematical preliminaries. In 3 we describe the process of embedding HA in ML, and present its correctness in 1.A. In 4.2 we discuss monitoring and runtime
verification using the embedding from \[3\] In \[5\] we discuss directions for future work and conclude.

\section{Preliminaries}

\subsection{Hybrid Automata}

Hybrid Automaton \(H\) \[8\] consists of: (1) A finite set \(X = \{x_1, \ldots, x_n\}\) of \textit{real valued variables}, a finite set \(\dot{X} = \{\dot{x}_1, \ldots, \dot{x}_n\}\) of \textit{dotted variables} for derivatives, and a finite set \(X' = \{x'_1, \ldots, x'_n\}\) of \textit{primed variables} for final values of discrete changes. (2) A finite directed multigraph \((V, E)\), with vertices referred to as \textit{control modes} and edges as \textit{control switches}. (3) For all \(v \in V\), predicates \textit{init}(\(v\)), \textit{inv}(\(v\)) and \textit{flow}(\(v\)) called \textit{initial}, \textit{invariant} and \textit{flow conditions} respectively. \textit{init}(\(v\)) and \textit{inv}(\(v\)) are defined using variables in \(X\), while \textit{flow}(\(v\)) is defined using those in \(X \cup \dot{X}\). (4) For all \(e \in E\), predicate \textit{jump}(\(e\)) called \textit{jump condition}, defined over free variables in \(X \cup X'\). (5) A finite set \(\Sigma_H\) of events, and an edge labeling function \textit{event}: \(E \rightarrow \Sigma_H\), assigning to each \textit{control switch} \(e \in E\) an event \(s \in \Sigma_H\).

\subsection{Labeled Transition Systems}

For the purpose of this discussion, a \textit{Labeled Transition System} (LTS) \(S\) consists of (1) A possibly infinite set of states \(Q\), and set \(Q_0 \subseteq Q\) of initial states. (2) A possibly infinite set \(A\) of labels, and for each \(a \in A\), a binary relation \(\xrightarrow{a}\) on \(Q\).

For a given \textit{Hybrid Automaton} \(H\), the \textit{timed transition system} \(S_H \subseteq H\) is a LTS that captures transition semantics of \(H\) \[8\], defined as: (1) \(Q_0 \subseteq (V \times \text{Real}^n)\). Say, \((v, x) \in Q\) iff \textit{inv}(\(v\))[\(x/X\]] and \((v, x) \in Q_0\) iff \textit{init}(\(v\))[\(x/X\]]. Let label set \(A = \Sigma_H \cup \text{Real}_{\geq 0}\). (2) For given \(\sigma \in \Sigma_H\), say \((v, x) \xrightarrow{\sigma} (v', x')\) iff (a) there exists \textit{control switch} \(e\) with source \(v\) and destination \(v'\). (b) \textit{jump}(\(e\))[\(x/X, x'/X'\]] holds, and \textit{event}(\(e\)) = \(\sigma\). (3) For each non negative real \(\delta \in \text{Real}_{\geq 0}\), say \((v, x) \xrightarrow{\delta} (v', x')\) iff (a) \(v = v'\) (b) there exists a differentiable function \(f: [0, \delta] \rightarrow \text{Real}^n\) where \(\dot{f}: (0, \delta) \rightarrow \text{Real}^n\) is the first order derivative of \(f\) such that \(f(0) = x\) and \(f(\delta) = x'\). (c) \(\forall \epsilon \in (0, \delta), \text{inv}(\epsilon)[\text{flow}(\epsilon)/X, \text{flow}(\epsilon)/X]\) hold.

\subsection{Matching Logic}

Matching Logic \[14\] is a logic for specifying static structures, logic constraints, and dynamic properties. ML serves as the foundation of the \(k\) framework \[1\], which is a language semantic framework where the formal semantics of languages are defined and all language tools of the given languages are automatically generated in a correct-by-construction manner. In this section, we give a compact overview of ML.

In short, ML is a many-sorted FOL variant combined with the least fixpoint \(\mu\)-binder. Unlike FOL, ML makes no distinction between \textit{functions} and \textit{predicates}, but only has \textit{symbols} that uniformly construct \textit{patterns}, which can capture static structure, dynamic properties, and FOL and modal logic constraints.

ML \textit{syntax} is parametric in a \textit{signature} \(\Sigma = (S, \text{VAR}, \Sigma)\) consisting of (1) a \textit{sort set} \(S\); (2) a disjoint union set \(\text{VAR} = \text{EVAR} \cup \text{SVAR}\) of \textit{element variables} in \(\text{EVAR}\) denoted \(x:s, y:s\) etc. and \textit{set variables} in \(\text{SVAR}\) denoted \(X:s, Y:s\) etc; and
Patterns are inductively defined by the following grammar:

\[ \varphi_s := x:s \in \text{EVAR} \mid X:s \in \text{SVAR} \mid \varphi_s \land \varphi_s \mid \neg \varphi_s \mid \forall \varphi_s \cdot \varphi_s \mid \sigma(\varphi_{s_1}, \ldots, \varphi_{s_n}) \] with \( \sigma \in \Sigma_{s_1}, \ldots, s_n \).

We say \( \varphi_s \) is positive in \( X:s \) if all occurrences of \( X:s \) are under an even number of negations in \( \varphi_s \). Sorts are omitted when they are irrelevant or can be inferred from the context. Common propositional connectives can be defined in the usual way. We define \( \exists x. \varphi \equiv \neg \forall x. \neg \varphi \), and \( \nu X. \varphi \equiv \neg \mu X. \neg \varphi[-X/X] \) (the greatest fixpoint), where \( \nu [\cdot/\cdot] \) is the standard notion of capture-avoiding substitution as in FOL. Define \( \top \equiv \exists x.x \) as the pattern that matches all elements and \( \bot \equiv \neg \top \) the one that matches nothing. Let \( \text{PATTERN} = \{ \text{PATTERN}_s \}_{s \in S} \) be the \( S \)-indexed set of all patterns, modulo \( \alpha \)-renaming of bound variables.

Given the signature \( \Sigma \) as above, a model \( M = (\{M_s\}_{s \in S}, M) \) consists of (1) a nonempty carrier set \( M_s \) for each \( s \in S \); and (2) an interpretation \( \sigma_M : M_s \times \cdots \times M_{s_n} \to \mathcal{P}(M_s) \) for each \( \sigma \in \Sigma_{s_1}, \ldots, s_n \), where \( \mathcal{P}(M_s) \) is the powerset of \( M_s \). Note that symbols are interpreted as relations. Standard FOL models are special cases of ML models where \( |\sigma_M(a_1, \ldots, a_n)| = 1 \) for all \( a_i \in M_{s_i}, 1 \leq i \leq n \). Partial FOL models are also special cases where \( |\sigma_M(a_1, \ldots, a_n)| \leq 1 \). We tacitly use the same \( \sigma_M \) to mean its pointwise extension, \( \sigma_M : (\mathcal{P}(M_s) \times \cdots \times \mathcal{P}(M_{s_n})) \to \mathcal{P}(M_s) \), defined as: \( \sigma_M(A_1, \ldots, A_n) = \bigcup \{ \sigma_M(a_1, \ldots, a_n) \mid a_i \in A_1, \ldots, a_n \in A_n \} \) for all \( A_i \subseteq M_{s_i}, 1 \leq i \leq n \). An \( (M) \)-valuation \( \rho : \text{VAR} \to (M \cup \mathcal{P}(M)) \) is a function s.t. \( \rho(x) \in M_s \) for \( x:s \in \text{EVAR} \) and \( \rho(X) \in \mathcal{P}(M_s) \) for \( X:s \in \text{SVAR} \), i.e., element variables are evaluated to elements and set variables are evaluated to sets. Its extension \( \bar{\rho} : \text{PATTERN} \to \mathcal{P}(M) \) is defined inductive over patterns as follows:

\[
\bar{\rho}(x) = \{ \rho(x) \} \quad \bar{\rho}(\varphi) = \{ \rho(\varphi) \} \quad \bar{\rho}(\varphi_1 \land \varphi_2) = \bar{\rho}(\varphi_1) \cap \bar{\rho}(\varphi_2) \quad \bar{\rho}(\forall x. \varphi) = \bigcap_{a \in M_s} \bar{\rho}[^a/x](\varphi) \quad \bar{\rho}(\sigma(\varphi_1, \ldots, \varphi_n)) = \sigma_M(\rho(\varphi_1), \ldots, \rho(\varphi_n))
\]

\[
\bar{\rho}(\mu X. \varphi) = \mu F^\rho \varphi X, \text{ where } F^\rho \varphi X : \mathcal{P}(M_s) \to \mathcal{P}(M_s) \text{ is the monotone function given as } F^\rho \varphi X (A) = \bar{\rho}[^A/X](\varphi) \text{ for all } A \subseteq M_s \text{ and } \mu F^\rho \varphi X \text{ denotes its least fixpoint.}
\]

Here, \( \{\cdot\} \) is set difference; \( \rho[^a/x] \) (resp. \( \rho[^A/X] \)) is the valuation \( \rho' \) with \( \rho'(x) = a \) (resp. \( \rho'(X) = A \)) and \( \rho'(y) = \rho(y) \) for \( y \neq x \) (resp. \( \rho'(Y) = \rho(Y) \) for \( Y \neq X \)). We define \( M \models \varphi \) iff \( \bar{\rho}(\varphi) = M \) for all \( \rho \). Let \( \Gamma \) be a pattern set called axiom set. We define \( M \models \Gamma \) iff \( M \models \varphi \) for all \( \varphi \in \Gamma \) and \( \Gamma \models \varphi \) iff \( M \models \varphi \) for all \( M \models \Gamma \). A theory is a pair \((\Sigma, \Gamma)\), often abbreviated as \( \Gamma \), where \( \Gamma \) is a set of \( \Sigma \)-axioms.

In this paper, we only need the FOL fragment of ML, meaning that most ML symbols occurred in this paper can be safely understood as FOL functions or predicates. The only exception is the “one-path next” symbol \( \bullet \) (defined in Section 3.2) which we use to capture the transition relations in transition systems. We will elaborate it in details when we define it.

### 3 Matching Logic Embedding of Hybrid Automata

Given an HA \( H \), we derive an ML theory \( H^H \) from \( H \), and prove, in Appendix 1.A, that the theory captures faithfully the behavior of \( H \).
3.1 Augmented Theory of Reals

We assume $\Gamma^{\text{Real } t}$, the ML theory of Real Closed Fields \cite{15}. We define $\Gamma^{\text{Real } t}$ which extends $\Gamma^{\text{Real}}$ with sorts $\text{Real }^{x}$, $\text{Real }^{x} \to \text{Real }^{y}$ representing n-ary products of $\text{Real }$ and relations between $\text{Real }$ to n-ary products of $\text{Real }$ respectively, and $\Gamma^{\text{Real } t}$’s signature with symbol $\text{app} \in \Sigma_{\text{Real }^{x} \to \text{Real }^{y} \to \text{Real }^{z}}$. We briefly describe the need for $\Gamma^{\text{Real } t}$, and its need for embedding $H$ in ML.

Consider $\mathcal{M}_{\text{Real } t}$ to be an ML model of $\Gamma^{\text{Real } t}$, with $\mathbb{R}$ and $\mathbb{R}^{n}$ as the carrier sets of sorts $\text{Real }$ and $\text{Real }^{n}$ respectively. Intuitively, the sort $\text{Real }^{n}$ can be thought of as the sort of relations between $\text{Real }$ sets of sorts $\text{Real }$ and relations between $\text{Real }$ sets of sorts $\text{Real }$. Since any binary relation $R$ can be described as a set $S_R$, where $(a, b) \in S_R$ iff $a R b$, any relation between $\mathbb{R}$ and $\mathbb{R}^{n}$, is simply a subset of $\mathbb{R}^{n+1}$. Thus, the carrier set of sort $\text{Real }^{n}$ would be $\mathcal{P}(\mathbb{R}^{n+1})$. For more information on ML models, we refer the reader to \cite{4}. The sort $\text{Real }^{n}$ and symbol $\text{app} \in \Sigma_{\text{Real }^{x} \to \text{Real }^{y} \to \text{Real }^{z}}$ give us the ability to quantify over relations that behave functionally in an interval. For instance, consider relations $a, b,$ and a variable $f: \text{Real }^{n+1}$. Say we have ML pattern $\varphi \equiv \forall a < l < t: \text{Real } < b . (\exists y: \text{Real }^{n} . (\text{app}(f, t) = y))$. In a model of $\Gamma^{\text{Real } t}$, the (extended) evaluation of $\varphi$ will be $\top$ iff the evaluation of $f$ is a relation that behaves as a function in the closed interval $[a, b]$. In section 3.2, we use aforementioned sort and symbol in the axiomatization of flow predicates.

We define syntactic sugar for frequently used $\Gamma^{\text{Real } t}$-terms. Say we have variables $f: \text{Real }^{n} \to \text{Real }^{n+1}, l: \text{Real }^{n}, u: \text{Real }^{n}, x: \text{Real }^{n},$ and $y: \text{Real }^{n}$, then we say $f(x)$ instead of $\text{app}(f, x): f : [l, u]$ instead of $\forall l \leq t \leq u . (\exists y : f(t) = y)$ and $f:[l, u]$ instead of $\forall l < t < u . (\exists y : f(t) = y)$. Given $f, f: \text{Real }^{n} \to \text{Real }^{n}$, we say $\dot{f}$ is the first order derivative of $f$ in interval $l, u$ as:

$$\varphi_{\text{isDerivativeOf}}(\dot{f}, f, l, u) \equiv f : [l, u] \land \dot{f} : (l, u) \land \forall l < t \leq u . \left( \exists h : \text{Real }^{n} . \left( \dot{f}(t) = \frac{f(t + h) - f(t)}{h} \right) \right) \land \forall l < t < u . \left( \exists h : \text{Real }^{n} . \left( \dot{f}(t) = \frac{f(t + h) - f(t)}{h} \right) \right).$$

(1)

Intuitively, the valuation of $\varphi_{\text{isDerivativeOf}}$ will be $\top$ iff (1) valuation of $f$ is a relation that behaves functionality in closed interval $[a, b]$, and (2) valuation of $\dot{f}$ is a relation that behaves functionally in the open interval $(a, b)$, and (3) at time $t \in (a, b)$, the valuation of $\dot{f}(t)$ is the first order derivative of $f$.

3.2 ML Theory of Hybrid Automata

In section 3.1, we defined $\Gamma^{\text{Real } t}$, an augmented theory of Reals. The ML embedding $\Gamma^{H} = (\Sigma^{H}, A^{H})$ of $H$ as:

($\text{Sorts}$) $\Sigma^{H} = ((\{V, E, \text{State}, \text{Transition}, \text{Event}\} \cup S^{\text{Real } t})$, $\text{VAR}^{H}$, $\Sigma^{H})$, where $S^{\text{Real } t}$ is the sort-indexed set of $\Gamma^{\text{Real } t}$ sorts. Sorts $V, E$ are understood to represent $H$’s control graph. We assume $\Sigma_{V}$ and $\Sigma_{E}$ contain sorts $\sigma_{v}$ and $\sigma_{e}$ for every $v \in V$ and $e \in E$ respectively. Similarly, we say $\text{Event}$ is the sort of $H$-events, and assume $\Sigma_{\text{Event}}$ to be the corresponding (finite) signature of $H$-events. Sort $\text{State}$ is assumed to a subset of $V \times \text{Real }^{n}$. The sort $\text{Transition}$ represents both continuous and discrete transitions of $H$. We assume appropriate axioms such that in any ML-model, the carrier sets of sorts $\text{Event}$ and $\text{Real }^{n}$ are subsets of the carrier set of sort $\text{Transition}$. Intuitively, $\text{State}$ and $\text{Real }^{n}$ can be thought of as subsorts of $\text{Transition}$.  

Manasvi Saxena, Nishant Rodrigues, Xiaohong Chen, and Grigore Roșu
(Symbols) We define symbols first ∈ Σ_{State,V} and second ∈ Σ_{State,Real^n}, with appropriate axioms such that they behave as projection functions. Say we have s:State, then we use s_v and s_x as syntactic sugar to refer to first(s) and second(s) respectively. Intuitively, the sort State can be thought of as a subset of V × Real^n, where first and second are projections into V and Real^n. In the remainder of this work, we may use (v, x):State instead of s:State, where it is understood that v = s_v and x = s_x. We also define symbol b ∈ Σ_{Transition,State}. The b (one path next) symbol is the idiomatic way of capturing transition systems in ML. We refer the reader to [4] for further information. We tacitly assume that flow, inv, init and jump behave similarly for ML-symbols corresponding to vertices and edges in H’s control graph. In other words, given v ∈ V and corresponding ML symbol σ_v ∈ Σ_V, flow(v) = flow(σ_v).

(Axioms) A^H, the set of I^H axioms is defined as:

(Invariant) For each σ_v ∈ Σ_V, we define an axiom:

∀ x : Real^n . (inv(σ_v)[x / X] ⇔ ∃(v', x'):State . v' = σ_v ∧ x' = x) (2)

(Jump) For each σ_e ∈ Σ_E, we define an axiom:

∀ (v, x), (v', x') : State . ((v, x) → b(event(σ_e), (v', x'))) ⇔ (jump(σ_e)[x / X, x' / X'] ∧ (source(σ_e) = v) ∧ (destination(σ_e) = v')) (3)

(Flow) For each σ_v ∈ Σ_V, we define an axiom:

∀ δ : Real_{≥0} . ∀ (v, x), (v', x') : State . (v = σ_v) ∧ ((v, x) → b(δ, (v', x'))) ⇔ (v = v') ∧ ∃ f, ċ : Real → Real^n . f isDerivativeOf(ċ, f, 0, δ) ∧ (f(0) = x ∧ f(δ) = x') ∧ ∀ 0 < ϵ < δ . (inv(σ_v)[f(ϵ) / X] ∧ flow(σ_v)[f(ϵ) / X, ċ(ϵ) / X]) (4)

(Init) For each σ_v ∈ Σ_V we also define aliases:

init_{σ_v} ≡ ∃ (v, x) : State . init(σ_v)[x / X] ∧ (v = σ_v) (5)

4 Applications

4.1 Verification

HA are commonly used to model safety-critical hybrid systems like cars, planes and medical devices, where safety is important. As a prelude to talking about safety, we briefly describe trace semantics of HA, and the Reachability Problem. Given a HA H and its LTS S_H = (Q, Q_0, A), a duration is assigned to each transition a ∈ A. For discrete events σ ∈ Σ_H, the duration is 0. For reals δ ∈ R_{≥0}, the duration of q δ → q’ is δ, where q, q’ ∈ Q [8]. If q_0 is the initial state and q_0 a_0 → q_1 , then ⟨a_i, q_i⟩_{i≥1} is an initialized trajectory.

In [8], the reachability problem a fundamental subtask for safety verification, but is only described informally as “existence of an initialized trajectory that visits a state of the form (v’, x’).” Our embedding however, allows us to formally
and concisely define the Reachability Problem, for a given HA $H$, its ML embedding $Γ^H$, and initial state $(v, x)$ as $(v, x) \rightarrow ∅(v', x')$ while safety can be then be stated in terms of the reachability problem as $\psi_{safety} \equiv \neg((v, x) \rightarrow ∅\varphi_{unsafe})$.

Intuitively, the above formalization says that given an initial state $(v, x)$, it must not be the case that an initialized trajectory will *eventually* reach an unsafe state (denoted by $\varphi_{unsafe}$). For more information on modal operators in ML, we refer the reader to [4]. Deductive verification is then proving $Γ_H \vdash \psi_{safety}$. Deductive verification of Hybrid Systems isn’t a novel idea. In [13,14], the authors present *Differential Dynamic Logic* and *Hybrid Hoare Logic* respectively - logics for verification of Hybrid Systems. These approaches however use *Hybrid Programs* and *Hybrid CSP* respectively to model hybrid systems. This places an additional requirement of understanding a different modeling approach instead of widely used HA. On the other hand our approach is centered around HA which eliminates the need for learning new modeling approaches for deductive verification.

### 4.2 Monitoring and Runtime Verification

Given a hybrid system $S$, and a HA $H$ that models $S$, we can use $Γ^H$, the embedding of $H$ in ML, and the ML proof system to deductively verify properties (like safety, liveness, et.c) about $H$. However, verification doesn’t guarantee that $S$ behaves as expected, since $H$ may not be an adequate model of $S$, as it is impossible to completely model real word physics. Thus it is vital, even after deductive verification, to monitor $S$’s execution for properties like model compliance and safety. In [12,13], the authors build on [13] to present monitoring mechanisms for stronger safety guarantees. However, since the aforementioned frameworks can only generate monitors for Hybrid Programs, and cannot be directly used with HA.

We now attempt to formally define monitoring in the context of HA. In Section 5, we briefly discuss approaches for efficient monitoring. We assume an 0-duration event is generate on every discrete transition, and at time interval $t_{SR}$, some pre determined sampling rate for continuous transitions. We also assume that for each 0-duration event, the discrete transition associated with the event is known.

#### Model Compliance

Consider an initialized trajectory $π = ⟨a_i, q_i⟩_{i \geq 1}$. Recall $a_i$ is a *duration*, and $q_i$ a state in the LTS of HA. We say $π \vdash^\text{trajectory} Γ_H$ iff (a) Let $π = π'⟨a_i, q_i⟩$, where $π'$ is sub-trajectory. If $π'$ is non empty then $π' \vdash^\text{trajectory} Γ_H$ (b) For events with duration $a_i \in \mathbb{R}_{>0}$, $Γ_H \vdash (q_{i-1} \rightarrow •(a_i, q_i))$. (c) For 0-duration (discrete) events, with discrete transition $σ$, there must exists an intermediate event $⟨δ, q'_i⟩$ with duration $δ \in \mathbb{R}_{\geq 0}$ such that $Γ_H \vdash (q_{i-1} \rightarrow •(δ, q'_i)) ∧(q'_i \rightarrow •(σ, q_i))$.

#### Safety

In section 4.1 we presented $\psi_{safety}$ - a formalization of safety using the Reachability Problem. Intuitively, $\varphi_{unsafe}$ is a unsafe state that an initialized trajectory must not reach to be considered safe. Formally, we say an initialized trajectory $π = ⟨a_i, q_i⟩_{i \geq 1}$ is a safe iff (a) Initial state $Γ_H \vdash \neg[q_0 \rightarrow \varphi_{unsafe}]$. (b) Let $π = π'⟨a_i, q_i⟩$, where $π'$ is sub-trajectory. If $π'$ is non empty then $π'$ must be a safe trajectory. (c) The most recent observed event $⟨a_i, q_i⟩$ must not match the unsafe pattern, i.e. $Γ_H \vdash \neg[q_i \rightarrow \varphi_{unsafe}]$.  

6 Manasvi Saxena, Nishant Rodrigues, Xiaohong Chen, and Grigore Roșu
Note that while monitoring, we can produce ML proof objects certifying how each event adheres to the property being monitored.

5 Future Work and Conclusion
In the immediate future, we plan to develop efficient algorithms that accomplish monitoring as described in section 4.2. In [7] the authors presented an algorithm for efficiently monitoring propositional LTL formulas by using the LTL property itself as a monitor, and rewriting the property w.r.t. every event to obtain a derived formula to be used as a monitor. We plan to extend their approach to our ML-embedding of Transition Systems, and derive efficient algorithms for monitoring Transition Systems expressed in ML, of which our HA embedding is a special case.

In the long term, we plan to identify classes of HA for which generation of efficient monitors can be automated. We plan to use and extend the existing infrastructure of RV-Monitor [11,24], to implement and test our approach using examples. Our choice is driven by RV-Monitor’s existing support for instrumenting LLVM and ROS. LLVM support is needed to instrument simulation of Hybrid Systems, while ROS (widely used for embedded systems) support allows monitoring actual ROS based Hybrid Systems.

In conclusion, this short paper presents a faithful (Appendix 1.A) embedding of HA in ML. Unlike other logical formalizations, our embedding can express all classes of HA. Importantly our work provides a framework for deductive verification of Hybrid Systems without going through alternative modeling approach and logics.

We also provided concise and formal definitions of important but informally defined problems from [8] such as the Reachability Problem and safety. We then formally defined monitoring model compliance and safety. Since we our definitions are expressed in a well understood logic, we hope to be able to produce proof objects certifying compliance of an observed trajectory with properties of interest. Finally, as future work, we present ideas for efficient online monitoring techniques that can be used with offline deductive verification to provide strong safety guarantees about Hybrid Systems.

References
Appendix 1.A Proof of Faithfulness

Let $\Gamma^H_q = (Q, Q_0, A)$ be the LTS expressing the transition semantics of $H$, and $\Gamma^H$ be the ML embedding of $H$. We refer the reader to section 2.2 and [8] for more information on transition semantics of Hybrid Automata.

Lemma 1. For every $q, q' \in Q$ and $a \in A$ $(v, x) \xrightarrow{a} (v', x')$ iff $\Gamma^H \vdash (v, x) \rightarrow \bullet (a, (v', x'))$.

Since $A = \Sigma_H \cup \mathbb{R}_{\geq 0}$, where $\Sigma_H$ is finite and $\Sigma_H \cap \mathbb{R}_{\geq 0} = \emptyset$, we have the following cases:

**Discrete** When $a \in \Sigma_H$, $(v, x) \xrightarrow{a} (v', x')$ iff there is a control switch $e \in E$ such that

- $(d_1)$ source$(e) = v$ and destination$(e) = v'$
- $(d_2)$ event$(e) = a$
- $(d_3)$ jump$(e)[x / X, x' / X]$ holds

We first prove $(\rightarrow)$ direction. Assume $(v, x) \xrightarrow{a} (v', x')$. By assumption $[d_1], [d_2]$ and $[d_3]$ hold. Using the [3] (Jump axiomatization) from section 3.2, since $[d_1]$, $[d_2]$ and $[d_3]$ hold, we get $\forall (v, x), (v', x')$ such that $\sigma(e)$ hold, which proves $(\rightarrow)$ direction. Next we prove $(\leftarrow)$ direction. Assume event$(e) = a$ and $\forall (v, x), (v', x')$ such that $\delta(e)$ hold, leading to $(\leftarrow)$ direction.

**Continuous** When $a \in \mathbb{R}_{\geq 0}$, $(v, x) \xrightarrow{a} (v', x')$ iff

- $(c_1)$ $v = v'$
- $(c_2)$ There exist functions $f : [0, a] \rightarrow \mathbb{R}^n$ and $\dot{f} : (0, a) \rightarrow \mathbb{R}^n$ such that $\dot{f}$ is the first-order derivative of $f$.
- $(c_3)$ $f(0) = x$ and $f(a) = x'$
- $(c_4)$ $\forall 0 < \epsilon \in \mathbb{R}^n < a$. $\text{inv}(v)[\dot{f}(e) / X]$ and $\text{flow}(v)[f(e) / X, \dot{f}(e) / \dot{X}]$ hold.

We first prove $(\rightarrow)$ direction. Assume $(v, x) \xrightarrow{a} (v', x')$. By assumption $[c_1], [c_2], [c_3]$ and $[c_4]$ hold. Using [3] (Flow axiomatization) from section 3.2, we get, $\sigma(e)$ hold iff $(v, x) \rightarrow \bullet (a, (v', x'))$. For proof of $(\leftarrow)$ we assume $(v, x) \rightarrow \bullet (a, (v', x'))$. Using Flow, we get $[c_1], [c_2], [c_3]$ and $[c_4]$ hold, leading to $(v, x) \xrightarrow{a} (v', x')$. 
