Center for Foundations of Intelligent Systems

Technical Report 98-14

On Hybrid Systems and the Modal $\mu$-calculus

J. M. DAVOREN

November 1998
**ON HYBRID SYSTEMS AND THE MODAL μ-CALCULUS**

**ABSTRACT**

Much of the contemporary work in logics for the formal verification of hybrid systems (notably the work of Henzinger at UC Berkeley and Manna at Stanford) builds directly on the framework of temporal logic verification of discrete systems. The core computational model is that of a hybrid automaton, which is represented formally as a transition system over a hybrid state space $X \subseteq Q \times IR^n$, where $Q$ is a finite set of discrete modes. While the temporal logic framework is adequate to formally express many qualitative dynamic properties of such systems, it fails to capture the "continuity" of continuous dynamics, or to reflect the topological and metric structure of Euclidean space. In addressing this deficiency, we look to the modal μ-calculus, a richly expressive formal logic over transition system models, into which virtually all temporal and modal logics can be translated. The key move in this paper is to view the transition system models of hybrid automata not merely as some form of "discrete abstraction", but rather as a skeleton which can be fleshed out by imbuing the state space with topological, metric tolerance or other structure. Drawing on the resources of modal logics, we give explicit symbolic representation to such structure in polymodal logics extending the modal μ-calculus...

**SUBJECT TERMS**

formal verification, hybrid systems, fixed points, modal logic, temporal logic, general topology, continuity, stability
Technical Report
98-14

On Hybrid Systems and the Modal
$\mu$-calculus

J. M. Davoren

November 1998
On Hybrid Systems and the Modal $\mu$-calculus

J. M. Davoren*

Center for Foundations of Intelligent Systems
626 Rhodes Hall, Cornell University
Ithaca NY 14853, USA
davoren@cornell.edu

Abstract. We start from a basic and fruitful idea in current work on the formal analysis and verification of hybrid and real-time systems: the uniform representation of both sorts of state dynamics -- both continuous evolution within a control mode, and the effect of discrete jumps between control modes -- as abstract transition relations over a hybrid space $X \subseteq Q \times \mathbb{R}^n$, where $Q$ is a finite set of control modes. The resulting "machine" or transition system model is currently analyzed using the resources of concurrent and reactive systems theory and temporal logic verification, abstracted from their original setting of finite state spaces and purely discrete transitions. One such resource is the propositional $\mu$-calculus: a richly expressive formal logic of transition system models (of arbitrary cardinality), which subsumes virtually all temporal and modal logics. The key move here is to view the transition system models of hybrid automata not merely as some form of "discrete abstraction", but rather as a skeleton which can be fleshed out by imbuing the state space with topological, metric tolerance or other structure. Drawing on the resources of modal logics, we give explicit symbolic representation to such structure in polymodal logics extending the modal $\mu$-calculus. The result is a logical formalism in which we can directly and simply express continuity properties of transition relations and metric tolerance properties such as "being within distance $\epsilon$" of a set. Moreover, the logics have sound and complete deductive proof systems, so assumptions of continuity or tolerance can be used as hypotheses in deductive verification. By also viewing transition relations in their equivalent form as set-valued functions, and drawing on the resources of set-valued analysis and dynamical systems theory, we open the way to a richer formal analysis of robustness and stability for hybrid automata and related classes of systems.

1 Introduction

It is hardly controversial to claim that the $\mu$-calculus is a formal logic of central import for the analysis and verification of hybrid automata and related classes of systems. The fundamental concepts of reachability and invariance are expressible

* Research supported by the ARO under the MURI program "Integrated Approach to Intelligent Systems", grant no. DAA H04-96-1-0341.
in terms of fixed-points of operators mapping sets of states to sets of states, and
are thus definable in the language of the $\mu$-calculus. The iterative computation
of the denotation of such fixed point formulas lies at the heart of symbolic model
checking tools for hybrid and real-time systems such as HyTech [4], [19] and
KRONOS [13]. More generally, the propositional $\mu$-calculus is well-recognized as a
richly expressive logic over transition system models: the power of its fixed-point
quantifiers are such that it subsumes virtually all temporal, modal and dynamic
logics [15], [25].

However, the current practice, within the allied field of automated verification
of (discrete) reactive systems as well as within the hybrid systems community, is
to consider the $\mu$-calculus not as a working or usable logic but rather as a logic
of the substratum. It provides a common "machine" language and semantics
for verification by model checking, with user-input specifications written in the
more "natural" languages of temporal logics, and then translated into that of
the $\mu$-calculus.

This paper challenges that practice, and demonstrates that the propositional
$\mu$-calculus and various of its modal logic extensions can provide both an expres-
sively rich and "human readable" formalism for reasoning about properties of
hybrid dynamical systems.

We begin with the "machine" or transition system models of hybrid systems,
in which both sorts of state transformation – continuous evolution within a
control mode, and the effects of discrete jumps between control modes – are
uniformly represented as abstract transition relations $r \subseteq X \times X$ over a hybrid
state space $X \subseteq Q \times \mathbb{R}^n$, where $Q$ is a finite set of control modes or discrete
states.

Formally, define a labeled transition system (LTS) (or generalized Kripke
model) to be a structure

$$\mathcal{M} = (X, \{a^{\mathcal{M}}\}_{a \in \Sigma}, \{\|p\|^{\mathcal{M}}\}_{p \in \Phi})$$

where $X \neq \emptyset$ is the state space (of arbitrary cardinality); for each transition
label $a \in \Sigma$, $a^{\mathcal{M}} \subseteq X \times X$ is a binary relation on $X$; and for each propositional
constant (observation or event label) $p \in \Phi$, $\|p\|^{\mathcal{M}} \subseteq X$ is a fixed subset of
$X$.

An LTS model is a clean and simple abstraction of a finite automaton. Such an
$\mathcal{M}$ is an abstract machine over state space $X$, with input or action alphabet
$\Sigma$ and transition map $\delta : X \times \Sigma \to \mathcal{P}(X)$ given by: $x' \in \delta(x, a)$ iff $x \xrightarrow{a} x'$.
It is additionally equipped with an observation alphabet $\Phi$, and an output map
$o : X \to \mathcal{P}(\Phi)$ given by: $o(x) = \{p \in \Phi \mid x \in \|p\|^{\mathcal{M}}\}$; sets of initial or final states
can be identified by specific labels in $\Phi$.

A (basic) hybrid automata $\mathcal{H}$ is typically represented by a graph of the form
depicted in Figure 1. Hybrid automata and their associated LTS models are
examined in more detail in Section 2; for now, we give a high-level description,
based on Henzinger's "time-abstract" transition system in [19] §1.2.
An LTS model $\mathcal{M}_H$ of a hybrid automaton $\mathcal{H}$ has a state space $X \subseteq Q \times \mathbb{R}^n$, with $Q$ finite. So states are pairs $(q, x)$, where $q \in Q$ and $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. For each $q \in Q$, let $X_q \subseteq \mathbb{R}^n$ be the projection of $X$ under $q$. The transition alphabet $\Sigma$ will include symbols such as $e^q$ for the relation of evolution (a "time-step" or "continuous transition") within each discrete mode $q \in Q$. In the basic case, such a relation is defined by: $(q, x) \xrightarrow{e^q} (q, x')$ iff there is an integral curve along the flow $\phi_q$ connecting $x \in X_q$ to $x' \in X_q$, and all points on the curve between $x$ and $x'$ lie inside the invariant set $\text{Inv}_q \subseteq X_q$. The transition alphabet will also include, for each edge $(q, q')$ in the discrete transition graph $G \subseteq Q \times Q$ of $\mathcal{H}$, a symbol $c_{q, q'}$ for the controlled jump relation (a "step" or "discrete transition") modeling the effect of making a controlled switch from mode $q$ to mode $q'$. Such relations are standardly defined by: $(q, x) \xrightarrow{c_{q, q'}} (q', x')$ iff $x \in \text{Grd}_{q, q'}$, $x' \in \text{Inv}_{q'}$, and $x' \in r_{q, q'}(x)$, where $r_{q, q'} \subseteq X_q \times X_{q'}$ is a reset relation for the real-valued coordinates, and the domain $\text{Grd}_{q, q'} \subseteq X_q$ is known
as the guard set of the discrete transition \((q, q')\). The alphabet \(\Phi\) of atomic propositions will include \(\text{Init}_q\) and \(\text{Inv}_q\) for \(q \in Q\), and \(\text{Grd}_{q, q'}\) for \((q, q') \in G\).

A trajectory of \(H\) is a finite or infinite sequence \(\langle \delta_i, q_i, \gamma_i \rangle_{i \in I}\) such that for each \(i \in I\): the duration \(\delta_i \geq 0\); the curve \(\gamma_i : [0, \delta_i] \to X_{q_i}\) is such that \((q_i, \gamma_i(0)) \xrightarrow{\delta_i} (q_i, \gamma_i(t))\) for all \(t \in [0, \delta_i]\); \((q_i, q_{i+1}) \in G\); and \((q_i, \gamma_i(\delta_i)) \xrightarrow{\delta_{i+1}} (q_{i+1}, \gamma_{i+1}(0))\). When \(I\) is finite, with largest element \(N\), it is allowed that \(\delta_N = \infty\). When a hybrid automaton is thought of as a discrete controller interacting with a physical plant, the class of trajectories, so defined, are founded on implicit operational assumptions of continuous and perfect precision sensing, and instantaneous control switches ([19]).

In the modal – as distinct from temporal – variant of the \(\mu\)-calculus\(^1\), the propositional language (over an alphabet \((\Sigma, \Phi)\)) includes a dual pair of modal operators \([a]\) and \((a)\), for each transition label \(a \in \Sigma\). The (standard) relational Kripke semantics of the labeled modalities are given by the universal and existential pre-image operators of the corresponding relations \(r = a^\text{m}\). For relations \(r \subseteq X \times Y\), and sets \(A \subseteq Y\),

\[
\tau(r)(A) = \{ x \in X \mid \forall y \in Y \{ x \xrightarrow{a} y \Rightarrow y \in A \} \}
\]

\[
\sigma(r)(A) = \{ x \in X \mid \exists y \in Y \{ x \xrightarrow{a} y \land y \in A \} \}
\]

In the notation of [20], \(\sigma(r) = \text{pre}[r]\) and \(\tau(r) = \text{pre}[r]\). The semantic readings of the modalities are forward-looking, and in temporal logics, they are known as relativized next operators:

\([a] \varphi \equiv \text{"All } a\text{-successors satisfy } \varphi\"

\((a) \varphi \equiv \text{"Some } a\text{-successor satisfies } \varphi\"

The temporal variant of the \(\mu\)-calculus usually works with the global transition relation \(R^\text{m} = \bigcup_{a \in \Sigma} a^\text{m}\) (standardly assumed to be total) and the modal operators are replaced by global temporal \("next\) operators: \(\forall X\) or \(\forall O\), and \(\exists X\) or \(\exists O\).

Sentences \(\varphi\) of the \(\mu\)-calculus denote sets of states \(||\varphi||^\text{m} \subseteq X\), and a sentence is true in \(M\), written \(M \vdash \varphi\), iff \(||\varphi||^\text{m} = X\), or equivalently, \(||\neg \varphi||^\text{m} = \emptyset\). The propositional connectives \(\neg, \land\) and \(\lor\) are interpreted by set theoretic complement, intersection and union, and other connectives and constants defined in the usual way. In particular, \(||\top||^\text{m} = X\), and an implication \(\varphi \rightarrow \psi\) is true in \(M\) exactly when \(||\varphi||^\text{m} \subseteq ||\psi||^\text{m}\). As a point of contrast, in the language of linear temporal logic LTL, sentences denote sets of (finite or infinite) paths or trajectories of the LTS model, rather than sets of states. In the language of the branching temporal logic CTL*, there are two sorts of sentences: state sentences, true or false at states of the LTS model, and path sentences, true or false at states of the LTS model.
false of infinite paths through the model. An $\exists$ or $\forall$ path quantifier applied to a path sentence produces a state sentence, and such quantification is definable using the least and greatest fixed-point quantifiers of the $\mu$-calculus.

The principal advantage of working in the modal rather than temporal framework is that it gives a modular specification language for expressing properties of transition systems: we can describe and reason about each of the component transition relations of an LTS model, and how they are combined to form more complex transition relations. In particular, we can give a clean and modular formal description of classes of trajectories of the system.

The modal sentences:

$$\psi \rightarrow [c_{q,q'}] \varphi$$

with the semantic readings “If $\psi$ holds, then all $c_{q,q'}$-successors satisfy $\varphi$”, and likewise for $e_{q}$, correspond precisely to Manna and Pnueli’s two types of (temporal logic) safety verification conditions for hybrid systems in [29] §4.1. Their notation is: $\{\psi\} \tau \{\varphi\}$ and $\{\psi\} \text{cont}\{\varphi\}$, respectively, where $\tau$ ranges over jump transitions and “cont” denotes the union of all the evolution relations.

The modal sentence

$$(e_{q}) (c_{q_{0},q_{1}}) (e_{q_{1}}) (c_{q_{1},q_{2}}) (e_{q_{2}}) \cdots (e_{q_{k}}) (c_{q_{k},q_{k+1}}) (e_{q_{k+1}}) \varphi$$

(3)

denotes the set of states $(q_{0}, x)$ from which some trajectory with discrete trace $(q_{0}, q_{1}, \ldots, q_{k})$ reaches the set $||\varphi||^{\mu} \subseteq X$. Dually, the modal sentence

$$[e_{q_{0}}] [c_{q_{0},q_{1}}] [e_{q_{1}}] [c_{q_{1},q_{2}}] [e_{q_{2}}] \cdots [e_{q_{k}}] [c_{q_{k},q_{k+1}}] [e_{q_{k+1}}] \varphi$$

(4)

denotes the set of states from which all $(q_{0}, q_{1}, \ldots, q_{k})$-trajectories reach the set $||\varphi||^{\nu}$, upon the last jump $c_{q_{k},q_{k+1}}$ and remain in $||\varphi||^{\nu}$ throughout the last evolution $e_{q_{k+1}}$.

Defining $e$ and $c$ to denote the relational sum (union) of, respectively, the relations for the $e_{q}$'s for $q \in Q$, and the relations for the $c_{q,q'}$'s for $(q, q') \in G$, the dynamics of the class of all hybrid trajectories with finite discrete traces are captured by the dual fixed-point definable modalities:

$$\langle h \rangle \varphi \equiv \mu Z. (e) \varphi \lor (e) (c) Z$$

and

$$[h] \varphi \equiv \nu Z. [e] \varphi \land [e] (c) Z$$

(5)

The sentence $\langle h \rangle \varphi$ “unwinds” to the infinite union of all sentences of the form (3), and dually, $[h] \varphi$ corresponds to the intersection of all sentences of the form (4). As a regular expression, we have $h = (ec)^{*}e = e(ec)^{*}$ (so we are in fact working in the weaker propositional dynamic logic PDL, rather than the full $\mu$-calculus.) Semantically, $\langle h \rangle$ and $[h]$ correspond to the dual pre-image operators of the reachability relation $h$ of the system under the control of $H$; that is, $(q, x) \xrightarrow{h} (q', x')$ if some trajectory $(\delta_i, q_i, \gamma_i)_{i \in I}$ with $q_0 = q$ and $\gamma_0(0) = x$ passes through the point $(q', x')$.

We now have the formal linguistic machinery to succinctly express various system specifications. The safety sentence

$$\text{Init} \rightarrow [h] \varphi$$

(6)
is true in the model $\mathcal{M} = \mathcal{M}_H$ exactly when every trajectory that starts in the set $\|\text{Init}\|^{\mathcal{M}}$ always remains within $\|\varphi\|^{\mathcal{M}}$. More generally, we say a set $\|\varphi\|^{\mathcal{M}}$ is future-invariant under $\mathcal{H}$ exactly when the sentence $\varphi \rightarrow [h]\varphi$ is true in $\mathcal{M}$. We also have at our disposal (previously unutilized) deductive proof systems for the $\mu$-calculus, such as Kozen’s axiomatization $L_\mu$ [23], [5], [40], which is sound and complete over arbitrary LTS models. From the fixed-point rules of $L_\mu$ (given in Section 5), one readily derives an obvious invariance rule for hybrid trajectories:

$$\psi \rightarrow \varphi \rightarrow [c_q]\varphi \quad \varphi \rightarrow [c_{q,q'}]\varphi$$

for $q \in Q$, $(q, q') \in G$.

This is a simpler $\mu$-calculus analog of the LTL invariance rule used in the verification of safety properties for hybrid automata in [29], [30].

To express liveness properties, we use modal analogs of the “box-diamond” construct in temporal logic. For example, the sentence

$$\varphi \rightarrow [h](e)(c)(e)tt$$

is true in $\mathcal{M}$ exactly when every maximal $\mathcal{H}$ trajectory from a state in $\|\text{Init}\|^{\mathcal{M}}$ has an infinite discrete trace. This is so because $[h](e)(c)(e)tt$ denotes the set of states from which every trajectory with a finite discrete trace can be properly extended. Similarly, the sentence $\varphi \rightarrow [h](e)(c)(e)\varphi$ is true in $\mathcal{M}$ exactly when every trajectory from $\|\varphi\|^{\mathcal{M}}$ returns to $\|\varphi\|^{\mathcal{M}}$ via a controlled jump infinitely often. And $[h](h)\varphi$ denotes the set of states from which every hybrid trajectory eventually reaches $\|\varphi\|^{\mathcal{M}}$. Note that at this level of description, we cannot expressly rule out Zeno trajectories ($\delta_i, q_i, \gamma_i$)$_{i \in I}$ such that $I$ is infinite but $\sum_{i \in I} \delta_i < \infty$, but by considering variant evolution relations $\hat{\mathcal{E}}_\varphi$ defined using a minimal time duration $\delta$, we could.

A clean $\mu$-calculus definition of the higher-order modalities $(h)$ and $[h]$ also opens up new possibilities for aggregation in complex systems. We could model a complex system as a hybrid “meta-automaton”, where the dynamics at each discrete meta-mode $p \in P$ are given by the reachability relation $h_p$ of a (basic) hybrid automaton over state space $X_p \subseteq Q_p \times \mathbb{R}^n$, with switching relations from $X_p$ to $X_{p'}$ between automata, as illustrated in Figure 2. We now have the machinery with which to formally reason about the dynamics of such a creature.

We also gain a clearer view of the enterprise of symbolic model checking for hybrid and real-time systems, as implemented in tools such as HYTECH and KRONOS. The basic task of such systems is to compute the reachable region of a hybrid dynamical system under the control of a given hybrid automaton $\mathcal{H}$. As noted in the recent paper of Henzinger, Kupferman and Qadeer [20], to capture the notion “reachable from $\varphi$”, as distinct from “reaches $\varphi$”, one needs in the semantics the post-image, rather than the pre-image, operator of a relation. The cleanest way to do it is to use the basic identity: $\text{post}[r] = \text{pre}[\bar{r}]$, where $\bar{r}$ is the relational converse or inverse of $r$, and to extend the $\mu$-calculus with a converse operation governed by the rule:

$$\langle a \rangle \psi \rightarrow \varphi \quad \text{iff} \quad \psi \rightarrow [a] \varphi$$
Fig. 2. Aggregation in complex systems

Then the sentence

\( (\bar{h}) \text{Init} \) (10)

denotes the reachable region, where the post modalities \( (\bar{h}) \) and \( [\bar{h}] \) are defined as in (5), but substituting the converse relations. Symbolic model checking tools attempt to compute the value of \( \| (\bar{h}) \text{Init} \|_{\mathcal{M}} \) as a first-order formula in \( n + 1 \) free variables \( (x, x_1, \ldots, x_n) \), in the language \( L(\mathbb{R}) \) of, say, the structure \( \mathbb{R} = (\mathbb{R}; <, +, -, 0, 1, \{ q \}_{q \in Q}) \) as the real closed field\(^2\) plus discrete constants. The procedure computes a sequence of first-order formulas \( \chi_0, \chi_1, \ldots, \chi_k \) which are translations of the \( \mu \)-calculus formulas forming the approximation sequence for \( (\bar{h}) \text{Init} \), with the translation starting from the explicit first-order definitions of the set \( \text{Init} \) and the relations \( e_q \) and \( c_{q,q'} \). The procedure terminates at stage \( k+1 \) if the formula: \( \chi_{k+1} \leftrightarrow \chi_k \) is provable in the first-order theory \( Th(\mathbb{R}) \) of the relevant structure over \( \mathbb{R} \), in which case the reachable region is defined by \( \chi_k \). The procedure is guaranteed to terminate when the model \( \mathcal{M} = \mathcal{M}_H \) has a finite bisimulation quotient \( \mathcal{M}^\approx \), where \( \approx \) is an equivalence relation on \( X \subseteq Q \times \mathbb{R}^n \) which respects each of the transition relations \( e_q \) and \( c_{q,q'} \) and the

---

\(^2\) The real closed field \( \mathbb{R} \) admits elimination of quantifiers, so all first-order formulas in the language are provably equivalent in the theory \( Th(\mathbb{R}) \) to a quantifier-free formula. The definable subsets of \( \mathbb{R}^n \) in \( \mathbb{R} \) are the semi-algebraic sets: finite unions of sets defined by equalities and inequalities over polynomials \( f \in \mathbb{R}[X_1, \ldots, X_n] \) [14].
observation sets $\text{Init}_q$, $\text{Inv}_q$, $\text{Grd}_q$. The recent work by Lafferriere, Pappas, Sastry and Yovine [27], [28], identifies a class of systems whose LTS models $\mathcal{M}_q$ are first-order definable in an $\omega$-minimal structure $\mathbb{R}$ expanding the real-closed field. The finite cell decomposition property of such structures (together with a restriction on the form of the controlled jumps relations $c_{q,q'}$) is used to construct the finite bisimulation equivalence. (The theory of definable sets in $\omega$-minimal structures is developed in van den Dries' monograph *Tame Topology and $\omega$-minimal Structures* [14].)

The basic propositional modal $\mu$-calculus can provide both a usable and a richly expressive formalism for reasoning about the abstract dynamics of hybrid systems. We want and need more. We want to be able to express in our logical formalisms what we mean by continuous and discrete dynamics, and hybrids of the two. We want to be able to formally express notions of imprecision or metric tolerance, such as the property of "being within distance $\epsilon$" of a set, for a particular $\epsilon > 0$. More generally, we want a logical formalism that supports not only the specification and verification of single properties, but the larger task of representing and building up a knowledge base of properties of a system, starting with structural properties assumed in the modeling, and then adding new facts as they are verified by either model-checking or deductive means.

The remainder of this paper is an exploration of how the propositional modal $\mu$-calculus can form a basis for a cohesive and expressively rich logical framework for the formal analysis of hybrid systems. In developing the logics, our key resources include:

1. modal logics, considered as a general formalism for reasoning about binary relations and operators on sets ([9], [35], [38], [5]); and
2. set-valued analysis and dynamical systems theory, brought into play by considering transition relations $\mathcal{R} \subseteq X \times X$ in their equivalent form as set-valued maps $\mathcal{R} : X \rightrightarrows X$, i.e. functions $\mathcal{R} : X \rightarrow \mathcal{P}(X)$ ([1], [6], [7]).

In the course of this paper, it will be important to keep an eye on both the distinction and the interplay between:

- the $\mu$-calculus and various extensions as propositional modal logics (and thus ultimately monadic second-order logics [25]), in which formulas of the same formal language can be meaningfully interpreted in a variety of LTS models of any cardinality; in particular, in both continuum-sized models $\mathcal{M}$ and in finite quotients $\mathcal{M}^{\mathbb{N}}$; and
- the first-order languages $\mathcal{L}(\mathbb{R})$ and theories $\text{Th}(\mathbb{R})$ of specific structures $\mathbb{R} = (\mathbb{R}; <, +, -, 0, 1, ...)$ over the reals, used in defining the components — the state space $X$, the transition relations $\mathcal{R}^{\mathbb{N}}$ and observation sets $||p||^{\mathbb{N}}$ — of particular, albeit intended, LTS models $\mathcal{M}$.

With regard to the latter, note that in the theory of $\omega$-minimal structures, relations $\mathcal{R}^{\mathbb{N}} : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ go by the name of definable families $(\mathcal{R}_z)_{z \in \mathbb{R}}$ ([14] §3.3).
To restate the point, the system description language is that of first-order logic, while the system specification language is that of propositional polymodal logic with fixed-point quantifiers.

This paper is one installment of a larger project. An analysis of the concept of bisimulation, and its relation to the algebraic semantics for the $\mu$-calculus, is given in [11], and [12] gives the completeness of deductive proof systems for normal polymodal extensions of the $\mu$-calculus. Related logics and earlier versions of some of the ideas are found in [10].

The paper is organized as follows. Section 2 is a review and analysis of basic hybrid systems and their associated LTS models. Section 3 is a review of the syntax and LTS semantics of the modal $\mu$-calculus. In Section 4, we flesh out the skeleton of an LTS model by imbuing the state space with topological and metric tolerance structure; we explore continuity and tolerance properties of relations $r : X \sim Y$ and applications to components of hybrid automata. Section 5 presents deductive proof systems for the new logics, extending Kozen's axiomatization of $L_\mu$. Section 6 is a brief discussion of ongoing research.

2 Basic hybrid automata and associated LTS models

First, a note on notation. For a set $X$, $\mathcal{P}(X)$ denotes the family of all subsets of $X$ (a complete Boolean algebra). Following [6], the notation $r : X \sim Y$ means $r \subseteq X \times Y$ is a relation, or equivalently, $r : X \rightarrow \mathcal{P}(Y)$ is a set-valued map, with values $r(x) \subseteq Y$ for $x \in X$. The expressions:

$$x \xrightarrow{r} y, \quad (x, y) \in r, \quad y \in r(x) \quad \text{and} \quad x r y$$

are synonymous. The domain of $r : X \sim Y$ is defined by $\text{dom}(r) = \sigma(r)(Y)$, and the range $\text{ran}(r) = \sigma(\tilde{r})(X) = \text{dom}(\tilde{r})$. Relational compositions $r \cdot s$ of $r : X \sim Y$ and $s : Y \sim Z$ are read from left to right in sequential order, defined by:

$$x \xrightarrow{r \cdot s} z \triangleq (\exists y \in Y) \quad x \xrightarrow{r} y \quad \text{and} \quad y \xrightarrow{s} z$$

(cf. [1] where composition is written in the reverse order, as for functional composition.)

We base our discussion on a generalization of the systems considered in [27],[28], depicted in Figure 1. Figure 3 is an illustration.

Definition 1. A (basic, evolution time-deterministic) hybrid system is a structure

$$\mathcal{H} = (Q, G, \{X_q\}_{q \in Q}, \{\phi_q\}_{q \in Q}, \{\text{Init}_q\}_{q \in Q}, \{\text{Inv}_q\}_{q \in Q}, \{r_{q,q'}\}_{(q,q') \in G}, \{\text{Grd}_{q,q'}\}_{(q,q') \in G})$$

where
\(- \) is a finite set of discrete states or control modes;
\(- G \subseteq Q \times Q is the control graph of discrete transitions;
\(- \) for each \( q \in Q, \)
  \( \cdot X_q \subseteq \mathbb{R}^n \) is the state space for mode \( q \);
  \( \cdot \phi_q : X_q \times \mathbb{R}^+ \to X_q \) is the continuous semi-flow of a vector field on \( X_q \);
  \( \cdot Inv_q \subseteq X_q \) is the set of invariant states for mode \( q \), or the domain of permitted evolution within mode \( q \);
  \( \cdot Init_q \subseteq Inv_q \) is the set of initial states for mode \( q \) (possibly empty);
\(- \) for each discrete transition \((q, q') \in G, \)
  \( \cdot Grd_{q,q'} \subseteq X_q \) is the guard set for the jump from \( q \) to \( q' \);
  \( \cdot r_{q,q'} : X_q \sim X_{q'} \) is the reset relation;
  for \( x \in X_q, r_{q,q'}(x) \subseteq X_{q'} \) is the set of possible reassignment states after the jump from \( q \) to \( q' \).

The hybrid state space of the system \( H \) is the set
\[ X = \bigcup_{q \in Q} \{ q \} \times X_q \]
To keep things simple, assume a fixed number \( n \) of real-valued coordinates, so \( X_q \subseteq \mathbb{R}^n \) for each \( q \in Q \). In [27],[28], the systems under consideration are simpler again in that they have constant reset relations \( r_{q,q'} = Grd_{q,q'} \times Rst_{q,q'} \), with the constant set of reassignment states \( Rst_{q,q'} \subseteq Inv_q \).

The intention is that a hybrid system, so defined, is the semantic content of a hybrid automaton in the sense of Henzinger [19], Def. 1.1. For definiteness, we take a (basic, evolution time-deterministic) hybrid automaton to be a hybrid system \( H \) with a concrete syntactic description, namely:

- the discrete structure is given by a finite graph \((Q, G)\), where \( G \subseteq Q \times Q \);
- each of the component sets \( X_q, Init_q, Inv_q, Grd_{q,q'} \subseteq \mathbb{R}^n \), semi-flows \( \phi_q : X_q \times \mathbb{R}^+ \to X_q \), and reset relations \( r_{q,q'} \subseteq X_q \times X_{q'} \) have explicit first-order definitions in the language \( L(<, +, −, \cdot, 0, 1, \ldots) \) of some specified structure \( \mathbb{R} \) over the reals.

From [27], [28], we have reason to want such a structure \( \mathbb{R} \) to be o-minimal.

Operationally, a hybrid automaton \( H \) can be thought of as defining a non-deterministic hybrid control policy, partially defined on states \((z, x) \in X\):

if \( z = q \) and \( x \in Inv_q \)
then \( \text{stay in discrete mode } q \) and \( \text{continue evolution according to } \phi_q \);  
if \( z = q \) and \( x \in Grd_{q,q'} \) for some \((q, q') \in G, \)
then \( \text{switch to discrete mode } q' \), \text{ re-initialize to some } z' \in r_{q,q'}(x), \)  
and then \( \text{evolve according to the flow } \phi_{q'} \).  

The domain of definition of \( H \) is given by:
\[ \text{dom}(H) = \left( \bigcup_{q \in Q} \{ q \} \times Inv_q \right) \cup \left( \bigcup_{(q,q') \in G} \{ q \} \times Grd_{q,q'} \right) \]
Fig. 3. Operation of basic hybrid automaton

If $z = q$ and $x \in \text{Grd}_{q,q'}$ for some $(q, q') \in G$, then that discrete control switch is said to be enabled; if $(q, x) \in \text{dom}(\mathcal{H})$ but $x \notin \text{Inv}_q$, then some discrete control switch is said to be forced. It is generally assumed that $r_{q,q'}(x) \subseteq \text{Inv}_{q'}$ for all $x \in \text{Grd}_{q,q'}$; in words, $\text{Inv}_{q'}$ is (forward) $r_{q,q'}$-invariant from $\text{Grd}_{q,q'}$. In some expositions (e.g. [27]), it is required that $\mathcal{H}$ be total or non-blocking, which amounts to the assumption that $\text{dom}(\mathcal{H}) = X$.

In descriptions of the operation of a hybrid automaton and the ensuing class of trajectories of the system, it is generally assumed (e.g. [19]) that the state $x = (x_1, ..., x_n) \in \mathbb{R}^n$ of the physical plant is being continuously sensed, with perfect precision, and that the action and effect of a discrete control switch is instantaneous.

The accepted ([19], [27]) definition of the ("time-abstract") transition system of a hybrid automaton, with modified notation, is as follows.

**Definition 2.** Given a hybrid system $\mathcal{H}$, the LTS model $\mathcal{M}_\mathcal{H}$ determined by $\mathcal{H}$ has the following components:

- the state space $X \equiv \bigcup_{q \in Q} \{q\} \times X_q$;
for each discrete state \( q \in Q \), the constrained evolution relation
\[ e_q : X_q \leadsto X_q \]
defined by:
\[ x \xrightarrow{e_q} x' \triangleq (\exists t \in \mathbb{R}^+) \left[ x' = \phi_q(x, t) \land (\forall s \in [0, t]) \phi_q(x, s) \in Inv_q \right] \]

for each discrete transition \((q, q') \in G\), the controlled jump relation
\[ c_{q,q'} : X_q \leadsto X_{q'} \]
defined by:
\[ x \xrightarrow{c_{q,q'}} x' \triangleq x \in \text{Grd}_{q,q'} \land x' \in Inv_{q'} \land x \xrightarrow{r_{q,q'}} x' \]

the observation sets \( X_q \), \( \text{Init}_q \), \( Inv_q \), \( \text{Grd}_{q,q'} \).

We adopt the notational convention of identifying, when convenient, sets \( A_q \subseteq X_q \) and \( \{q\} \times A_q \subseteq X \); moreover, the relations \( e_q : X_q \leadsto X_q \) and \( c_{q,q'} : X_q \leadsto X_{q'} \) can be "lifted" to relations \( X \leadsto X \) in the obvious way.

From the definition of the evolution relation \( e_q \), a desired property of the domain of evolution \( Inv_q \) is that it be convex with respect to the semi-flow \( \phi_q \), in the sense that:

if \( x \in Inv_q \) and \( \phi_q(x, t) \in Inv_q \) for some \( t \geq 0 \),
then \( \phi_q(x, s) \in Inv_q \) for all \( s \in [0, t] \)

So no curve segment of the semi-flow with both endpoints in \( Inv_q \) ever leaves \( Inv_q \) at an intermediate point.

In the terminology of [1] Ch. 6, Definition 6.3, the (positive) orbit relation \( f : X \leadsto X \) of a semi-flow \( \phi : X \times \mathbb{R}^+ \to X \) is defined by:
\[ x \xrightarrow{f} x' \triangleq (\exists t \in \mathbb{R}^+) \left[ x' = \phi(x, t) \right] \quad (11) \]

With respect to the orbit relation \( f_q : X_q \leadsto X_q \) of \( \phi_q \), the desired convexity property for \( Inv_q \) has the form:

if \( x_0, x_1 \in Inv_q \) and \( x_0 \xrightarrow{f_q} x \xrightarrow{f_q} x_1 \) then \( x \in Inv_q \)

So when \( Inv_q \) if \( f_q \)-convex, we have the decompositions

\[ e_q = f_q \cap (Inv_q \times Inv_q) \quad \text{and} \quad c_{q,q'} = r_{q,q'} \cap (\text{Grd}_{q,q'} \times Inv_{q'}) \]
in which case we may as well assume the LTS model \( \mathcal{M}_H \) includes the (unconstrained) orbit relations \( f_q \) and the uncontrolled reset relation \( r_{q,q'} \). If we want to express properties which require both the orbit relation \( f_q \) and its converse (convexity is one such), then we should include \( f_q \) as a component of \( \mathcal{M}_H \) as well (see also [20]).

The modularity of the modal \( \mu \)-calculus allows us to succinctly express not only desired properties — i.e. those to be verified, but also various of the structural properties of the LTS model \( \mathcal{M}_H \) that it will typically possess by assumption. In
a deductive framework, such sentences and sentence schemes (formulas with free propositional variables $Z$) provide an initial stock of facts known to be true in the model, and serve as hypotheses in application of inference rules when seeking to expand one's stock of knowledge.

\[ 1 \] \( (f_q) \text{Inv}_q \land (f_q) \text{Inv}_q \rightarrow \text{Inv}_q \)

\[ 2 \] \( \text{Init}_q \rightarrow \text{Inv}_q \)

\[ 3 \] \( \text{Init} \leftrightarrow \bigvee_{q \in Q} \text{Init}_q \)

\[ 4 \] \( \text{Inv} \leftrightarrow \bigvee_{q \in Q} \text{Inv}_q \)

\[ 5 \] \( (r_{q,q'}) \text{Grd}_{q,q'} \rightarrow \text{Inv}_{q'} \)

\[ 6 \] \( \text{Grd}_{q,q'} \rightarrow (r_{q,q'}) \text{tt} \)

\[ 7 \] \( (e_q)Z \leftrightarrow \text{Inv}_q \land (f_q)(Z \land \text{Inv}_q) \)

\[ 8 \] \( (e_q)Z \leftrightarrow \text{Inv}_q \land (f_q)(Z \land \text{Inv}_q) \)

\[ 9 \] \( (c_{q,q'})Z \leftrightarrow \text{Grd}_{q,q'} \land (r_{q,q'}) (Z \land \text{Inv}_{q'}) \)

\[ 10 \] \( (c_{q,q'})Z \leftrightarrow \text{Inv}_{q'} \land (r_{q,q'}) (Z \land \text{Grd}_{q,q'}) \)

\[ 11 \] \( (f)Z \leftrightarrow \bigvee_{q \in Q} (f_q)Z \)

\[ 12 \] \( Z \rightarrow (f)Z \)

\[ 13 \] \( (f_q)(f_q)Z \rightarrow (f_q)Z \)

\[ 14 \] \( (e)Z \leftrightarrow \bigvee_{q \in Q} (e_q)Z \)

\[ 15 \] \( (e)Z \leftrightarrow \bigvee_{(q,q') \in G} (e_{q,q'})Z \)

\[ 16 \] \( (h) \text{tt} \leftrightarrow \bigvee_{q \in Q} \text{Inv}_q \lor \bigvee_{(q,q') \in G} \text{Grd}_{q,q'} \)

[1] says that $\text{Inv}_q$ is $f_q$-convex. [2] is merely that $\text{Init}_q \subseteq \text{Inv}_q$. [3] and [4] define the global initial and invariant sets. [5] is the assumption that $\text{Inv}_{q'}$ is (future) $r_{q,q'}$-invariant from $\text{Grd}_{q,q'}$. [6] says that every point in $\text{Grd}_{q,q'}$ has an $r_{q,q'}$-successor; i.e. $\text{Grd}_{q,q'} \subseteq \text{dom}(r_{q,q'})$. [7] \textendash [10] follow from the decompositions $e_q = f_q \cap (\text{Inv}_q \times \text{Inv}_q)$ and $c_{q,q'} = r_{q,q'} \cap (\text{Grd}_{q,q'} \times \text{Inv}_{q'})$. In particular, using the rule for converse (9) in Section 1 above, we have:

\[ \varphi \rightarrow [e_q] \varphi \iff \text{Inv}_q \land (f_q)(\varphi \land \text{Inv}_q) \rightarrow \varphi \]  

(12)

and

\[ \varphi \rightarrow [c_{q,q'}] \varphi \iff \text{Inv}_{q'} \land (r_{q,q'})(\varphi \land \text{Grd}_{q,q'}) \rightarrow \varphi \]  

(13)
[11] defines \( f \) as the union of the orbit relations \( f_q \). From the zero semi-flow property, each \( f_q \) is reflexive on its domain \( X_q \), so \( f \) is reflexive (and total) on the whole space \( X \), which is [12]. From the sum semi-flow property, each \( f_q \) is transitive; this is [13]. [14] and [15] are the definitions \( e = \bigcup_{q \in Q} e_q \) and \( c = \bigcup_{(q,q') \in G} c_{q,q'} \). From [7], [14] and [12], it follows that:

\[
(Z \land \text{Inv}) \rightarrow (e)(Z \land \text{Inv})
\]

that is, the relational sum \( e \) is reflexive on its domain. And from [7] and [13], we get:

\[
\langle e_q \rangle \langle e_q \rangle Z \rightarrow \langle e_q \rangle Z
\]

which says each \( e_q \) is transitive.

[16] defines the domain \( \text{dom}(H) \). The definitions of \( \langle h \rangle \) and \[ h \] in (5) above should also be added to the list.

Using convexity assumption [1] and (12), the invariance assumption [5] and (13), and the invariance rule (7), it follows that \( \text{Inv} \rightarrow [h] \text{Inv} \) will be true in \( 2^H \); i.e. the set \( \text{Inv} \) is future-invariant under \( H \). More generally, whenever \( \text{Inv} \rightarrow \varphi \) is true in \( 2^H \), then \( \text{Init} \rightarrow [h] \varphi \) will be true, and thus on the current interpretation, \( \|\varphi\|^H \) is safe under the action of \( H \), since no (perfect precision) hybrid trajectory starting in \( \text{Init} \) ever leaves \( \text{Inv} \). So in this scenario, the situation of a controlled jump being forced — that is, \( (q, x) \in \text{dom}(H) \) but \( x \notin \text{Inv}_q \) — can in fact never arise. Perfect precision trajectories start or land inside \( \text{Inv}_q \), evolve continuously according to \( \phi_q \), and then while the state is still inside \( \text{Inv}_q \), or at worst on the (topological) boundary of \( \text{Inv}_q \), a jump is made according to \( c_{q,q'} \).

In some accounts of the LTS model of a hybrid automata (including that in [19]), the definition of the constrained evolution relation \( e_q \) is slightly weaker, with the requirement: \( \forall s \in [0, t], \phi_q(x, s) \in \text{Inv}_q \), so the end-point \( \phi_q(x, t) \) need not lie in \( \text{Inv}_q \). If \( \text{Inv}_q \) is closed (in the standard topology on \( X_q \subseteq \mathbb{R}^n \)), then the continuity of \( \phi_q : X_q \times \mathbb{R}^+ \rightarrow X_q \) entails that all such end-points will lie in \( \text{Inv}_q \) regardless, so the weakening makes no difference. In virtually all concrete examples of hybrid automata in the literature, the invariant sets \( \text{Inv}_q \) are closed.

In Section 4, when we adjoin modalities corresponding to the interior and closure operators of a topology, we will be able to formally express properties such as being open, closed, or the topological boundary of a set. We will also be able to give formal expression to the assumption that the orbit relations \( f_q \) are those of continuous semi-flows, and to consider consequences of continuity.

We also clearly need to entertain the possibility that a physical realization of a hybrid automaton as a control policy might be less than perfect: sensors will be accurate only up to some level of precision; we should allow for delay between sensing the state and acting on that sensor reading in accordance with the control policy; and then there are margins of error in real-valued constants used in first-order definitions of the components of the model. In Section 4, we will consider alternative classes of hybrid trajectories by playing with the definitions of the fixed-point modalities \( \langle h \rangle \) and \[ h \] in an enriched modal language containing
modalities ($\epsilon$) and [$\epsilon$] interpreted by metric $\epsilon$-tolerance relations, for concrete values of $\epsilon > 0$.

3 Syntax and LTS semantics of the modal $\mu$-calculus

The $\mu$-calculus originated in the late 1960's (Scott and de Bakker) as a formal logic of digital programs, the input-output behavior of an atomic program being represented as a binary transition relation on (discrete) states. Contemporary introductions to the $\mu$-calculus can be found in [38], [15]. In this section, we review the syntax and semantics over LTS models of the propositional modal $\mu$-calculus.

Definition 3. A modal signature is a pair $(\Phi, \Sigma)$, where $\Phi$ is a set of propositional constants and $\Sigma$ is a set of transition labels. Let PVar denote a fixed set of propositional (second-order or set-valued) variables. The collection $\mathcal{F}_\mu(\Phi, \Sigma)$ of formulas of the propositional modal $\mu$-calculus is generated by the grammar:

$$\varphi ::= \mathbf{ff} \mid p \mid Z \mid \neg \varphi \mid \varphi_1 \lor \varphi_2 \mid (a)\varphi \mid \mu Z.\varphi$$

for propositional constants $p \in \Phi$, propositional variables $Z \in \text{PVar}$, and transition labels $a \in \Sigma$, and with the proviso that in $\mu Z.\varphi$, the variable $Z$ occur positively, i.e. each occurrence of $Z$ in $\varphi$ is within the scope of an even number of negations.

The other (classical) propositional connectives, modalities and greatest fixed point quantifier are defined in the usual way:

$$\mathbf{tt} \triangleq \neg \mathbf{ff} \quad \varphi_1 \land \varphi_2 \triangleq \neg (\neg \varphi_1 \lor \neg \varphi_2)$$
$$\varphi_1 \rightarrow \varphi_2 \triangleq \neg \varphi_1 \lor \varphi_2 \quad \varphi_1 
\leftrightarrow \varphi_2 \triangleq (\varphi_1 \rightarrow \varphi_2) \land (\varphi_2 \rightarrow \varphi_1)$$
$$[a]\varphi \triangleq \neg (a)\neg \varphi \quad \nu Z.\varphi \triangleq \neg \mu Z.\neg \varphi [Z := \neg Z]$$

An occurrence of a variable $Z \in \text{PVar}$ in a formula that is within the scope of a $\mu Z$ is called bound, otherwise it is free (as in first-order logic). Let $S_\mu(\Phi, \Sigma)$ denote the set of all sentences, or closed formulas of $\mathcal{F}_\mu(\Phi, \Sigma)$, i.e. those without any free variables, and let $\mathcal{F}(\Phi, \Sigma)$ and $S(\Phi, \Sigma)$ denote, respectively, the set of all purely modal formulas and sentences, i.e. those containing no fixed point quantifiers, and in case of sentences, no variables $Z$.

For formulas $\varphi, \psi \in \mathcal{F}_\mu(\Phi, \Sigma)$, let $\varphi[Z := \psi]$ denote the result substituting $\psi$ for all free occurrences of $Z$. By renaming bound variables in $\varphi$ if necessary, we can assume such substitutions do not result in the unintended capture of free variables.

Definition 4. Given an LTS $\mathfrak{M} = (X, \{s^m\}_{s \in \Sigma}, \{p^m\}_{p \in \Phi})$ of modal signature $(\Phi, \Sigma)$, a (propositional, or second-order) variable assignment in $\mathfrak{M}$ is any
map $\xi : \text{PVar} \to \mathcal{P}(X)$. Each such assignment $\xi$ uniquely extends to a denotation map $\|\|_\xi : \mathcal{F}_\mu(\Phi, \Sigma) \to \mathcal{P}(X)$ as follows:

\[
\begin{align*}
\|p\|_\xi &= t(p), & \text{for } p \in \Phi \\
\|Z\|_\xi &= \xi(Z), & \text{for } Z \in \text{PVar} \\
\|\neg \phi\|_\xi &= \mathcal{X} - \|\phi\|_\xi \\
\|\phi_1 \lor \phi_2\|_\xi &= \|\phi_1\|_\xi \cup \|\phi_2\|_\xi \\
\|\sigma(a)\phi\|_\xi &= \sigma(a)\left(\|\phi\|_\xi\right) & \text{for } a \in \Sigma \\
\|\mu Z.\phi\|_\xi &= \bigcap\{A \in \mathcal{P}(X) \mid \|\phi\|_\xi(A/Z) \subseteq A\}
\end{align*}
\]

where the pre-image operator $\sigma(a^{\text{dual}})$ is defined as in (2) above, and for sets $A \in \mathcal{P}(X)$, the variant assignment $\xi(A/Z) : \text{PVar} \to \mathcal{P}(X)$ is given by:

\[\xi(A/Z)(W) = \xi(W) \text{ if } W \neq Z, \text{ and } \xi(A/Z)(W) = A \text{ if } W = Z.\]

For formulas $\phi \in \mathcal{F}_\mu(\Phi, \Sigma)$ and assignments $\xi : \text{PVar} \to \mathcal{P}(X)$ in $\mathcal{M}$, we say:

- $\phi$ is true at state $x$ in $(\mathcal{M}, \xi)$, written: $\mathcal{M}, \xi \models \phi$, iff $x \in \|\phi\|_\xi$;
- $\phi$ is true in $(\mathcal{M}, \xi)$, written: $\mathcal{M}, \xi \models \phi$, iff $\|\phi\|_\xi = \mathcal{X}$; i.e. $\phi$ is true at all states $x$ in $(\mathcal{M}, \xi)$; and
- $\phi$ is true in $\mathcal{M}$, written: $\mathcal{M} \models \phi$, iff $\phi$ is true in $(\mathcal{M}, \xi)$ for all assignments $\xi$ in $\mathcal{M}$.

For sentences $\phi \in \mathcal{S}_\mu(\Phi, \Sigma)$, the denotation $\|\phi\|_\xi$ is independent of the variable assignment $\xi$, and is written $\|\phi\|^{\text{dual}}$. So $\mathcal{M} \models \phi$ iff $\mathcal{M}, \xi \models \phi$ for any assignment $\xi$.

Given a model $\mathcal{M}$ and variable assignment $\xi$, each formula $\phi \in \mathcal{F}_\mu(\Phi, \Sigma)$ and each variable $Z \in \text{PVar}$ free in $\phi$, together determine an operator on sets $\varphi_{\xi,Z}^{\text{dual}} : \mathcal{P}(X) \to \mathcal{P}(X)$ given by:

\[ (\varphi_{\xi,Z}^{\text{dual}})(A) = \|\phi\|_{\xi(A/Z)} \] (16)

The variant assignment construct corresponds to substitution: for all formulas $\psi \in \mathcal{F}_\mu(\Phi, \Sigma)$,

\[ (\varphi_{\xi,Z}^{\text{dual}})(\|\psi\|_\xi) = \|\psi[Z := \psi]\|_\xi \] (17)

When the variable $Z$ occurs positively within $\phi$, so $\mu Z.\phi \in \mathcal{F}_\mu(\Phi, \Sigma)$, the operator $\varphi_{\xi,Z}^{\text{dual}}$ is $\subseteq$-monotone:

\[ A \subseteq B \quad \Rightarrow \quad F(A) \subseteq F(B) \]
for $F = \varphi^\mathbb{M}_{\Sigma}$. The clause in Definition 4 for $\mu$-formulas says that $||\mu Z.\varphi||_\xi^\mathbb{M}$ is the $\subseteq$-least pre-fixed-point of the monotone operator $\varphi^\mathbb{M}_{\xi Z}$ in the complete lattice $\mathcal{P}(X)$. So by the Tarski-Knaster fixed-point theorem, $||\mu Z.\varphi||_\xi^\mathbb{M}$ must also be the $\subseteq$-least fixed-point of $\varphi^\mathbb{M}_{\xi Z}$; that is:

$$||\mu Z.\varphi||_\xi^\mathbb{M} = \bigcap\{A \in \mathcal{P}(X) \mid ||\varphi||_\xi^\mathbb{M} \subseteq A \}$$

In the standard set-theoretic semantics for the $\mu$-calculus, as presented here and given in [23], [38], [40], [15], the propositional variables $Z$ range over the full power-set (and complete Boolean algebra) $\mathcal{P}(X)$ — that is, all subsets of $X$. An alternative, developed by Kwiatkowska and colleagues [5], [8], is an algebraic semantics in which the range of propositional variables is restricted to a sub-family $A \subseteq \mathcal{P}(X)$. This work has roots in a number of classic studies from the 1950's, notably that of Henkin [18] on completeness of higher-order logic; of Jönsson and Tarski [26] on Boolean algebras with operators; and that of Rasiowa and Sikorski [36] on algebraic logic.

**Definition 5.** ([5], [8]). Given an LTS model $\mathcal{M}$, a family of sets $A \subseteq \mathcal{P}(X)$ is said to be a modal algebra for $\mathcal{M}$, and the pair $(\mathcal{M}, A)$ is known as a modal frame, when each of the following holds:

1. $A$ contains each of the observation sets $||p||^\mathbb{M}$, for $p \in \Phi$;
2. $A$ is a Boolean algebra under the finitary set-theoretic operations; and
3. $A$ is closed under each of the pre-image operators $\sigma(a^\mathbb{M})$ and $\tau(a^\mathbb{M})$, for $a \in \Sigma$.

For purely modal formulas $\varphi \in \mathcal{F}(\Phi, \Sigma)$, the clauses in the inductive definition of the denotation $||\varphi||^A_\xi \subseteq X$ with respect to a modal frame $(\mathcal{M}, A)$ are identical to those in Definition 4 for $||\varphi||^\mathbb{M}_\xi$, with the proviso that variable assignments $\xi$ are restricted to $A$, i.e. $\xi : \text{PVar} \to A$.

A formula $\varphi$ is true in the frame $(\mathcal{M}, A)$, written $(\mathcal{M}, A) \vDash \varphi$, iff $||\varphi||^A_\xi = X$ for all assignments $\xi \in A$.

An LTS model $\mathcal{M}$ is identified with the modal frame $(\mathcal{M}, \mathcal{P}(X))$.

Modal algebras $A \subseteq \mathcal{P}(X)$ need not be complete as lattices, so unlike $\mathcal{P}(X)$, we have no guarantee that the set being the $\subseteq$-least pre-fixed-point of $\varphi^A_{\xi Z}$ in fact exists in $A$; when it does, it is the least fixed-point in $A$ of $\varphi^A_{\xi Z}$, by a variant of the argument in the Tarski-Knaster fixed-point theorem.

**Definition 6.** ([5], [8]). A modal algebra $A \subseteq \mathcal{P}(X)$ is called a modal $\mu$-algebra, and the pair $(\mathcal{M}, A)$ called a modal $\mu$-frame, if for each formula $\mu Z.\varphi \in \mathcal{F}_\mu(\Phi, \Sigma)$ the infinitary meet or infimum of the family in $A$ of pre-fixed-points of $\varphi^A_{\xi Z}$

$$\land\{A \in A \mid ||\varphi||^A_{\xi(A/Z)} \subseteq A \}$$

exists in $A$, in which case $||\mu Z.\varphi||_\xi^A$ is that set.
In general, the denotations $\|\varphi\|^{\mathfrak{M}}_\xi$ and $\|\varphi\|^{A}_\xi$ part company on $\mu$-formulas, since the smallest of all sets $A \in \mathcal{P}(X)$ such that a condition holds will be contained in the smallest of all sets $A \in A$ for which the same condition holds. In [11], we identify conditions under which a modal $\mu$-frame $(M, A)$ is in semantic agreement with $M$, i.e. for all $\mu$-formulas $\varphi \in F_\mu(\Phi, \Sigma)$, $\|\varphi\|^{A}_\xi = \|\varphi\|^{\mathfrak{M}}_\xi$ for all assignments $\xi$ restricted to $A$. The smallest $\mu$-algebra for an LTS $M$ is the countable algebra

$$\mathcal{S}^{\mathfrak{M}} = \{ \|\varphi\|^{\mathfrak{M}} | \varphi \in \mathcal{S}(\Phi, \Sigma) \}$$

of denotations of $\mu$-sentences in $M$. It is readily verified that $\mathcal{S}^{\mathfrak{M}}$ is in semantic agreement $M$.

From the purely modal clauses in Definition 4, together with the definitions of the pre-image operators in (2), it follows that if the state space, transition relations and observation sets of an LTS model $M$ are all first-order definable in some structure, then for all modal sentences $\varphi \in \mathcal{S}(\Phi, \Sigma)$, the denotation $\|\varphi\|^{\mathfrak{M}} \subseteq X$ is first-order definable. Otherwise put, the countable algebra

$$\mathcal{S}^{\mathfrak{M}} = \{ \|\varphi\|^{\mathfrak{M}} | \varphi \in \mathcal{S}(\Phi, \Sigma) \}$$

of denotations in $M$ of purely modal sentences, has a finitary syntactic representation as a family of first-order formulas; a family finitely generated by the explicit first-order definitions of the components of $M$, under the straight-forward translation of modal sentences based on the definitions (2) and the (classical) meaning of the Boolean connectives. Of course, an optimal situation is when the first-order structure admits quantifier-elimination, as then the naive translation of a modal sentence can be reduced to a quantifier-free formula, and so the algebra $\mathcal{S}^{\mathfrak{M}}$ will have a simpler and more tractable representation. Such algebras are the semantic content of Henzinger’s notion of a symbolic execution theory in [19] §3.1.

Returning to the standard set-theoretic semantics, the completeness of $\mathcal{P}(X)$ as lattice ensures that the set $\|\mu Z.\varphi\|^{\mathfrak{M}}_\xi$ has an equivalent characterization (by the Park-Hitchcock fixed-point theorem) as the union of an $\subseteq$-increasing sequence of approximations:

$$\|\mu Z.\varphi\|^{\mathfrak{M}}_\xi = \bigcup_{\alpha < \text{Ord}(M)} \|\varphi\|^{\mathfrak{M}}_{\xi, \alpha}$$

where

$$\|\varphi\|^{\mathfrak{M}}_{\xi, 0} = \emptyset$$
$$\|\varphi\|^{\mathfrak{M}}_{\xi, \alpha+1} = \varphi^{\mathfrak{M}}_{\xi, \alpha} (\|\varphi\|^{\mathfrak{M}}_{\xi, \alpha})$$
$$\|\varphi\|^{\mathfrak{M}}_{\xi, \eta} = \bigcup_{\alpha < \eta} \|\varphi\|^{\mathfrak{M}}_{\xi, \alpha} \text{ for limit ordinals } \eta$$
and \( \text{Ord}(\mathfrak{M}) < \kappa^+ \), for \( \kappa = \text{Card}(X) \), is the closure ordinal of \( \mathfrak{M} \). The sets \( ||\varphi||^\mathfrak{M}_{\xi,\alpha} \) are \( \mu \)-approximations of \( ||\mu Z. \varphi||^\mathfrak{M}_{\xi} \). Likewise, the denotation of \( \nu Z. \varphi \) can be represented as the intersection of an \( \subseteq \)-decreasing sequence of \( \nu \)-approximations.

In the general case, over LTS models \( \mathfrak{M} \) of arbitrary cardinality, approximation sequences for the denotation of fixed-point formulas proceed through transfinite ordinals; when \( X \) has the cardinality of the continuum, \( \text{Ord}(\mathfrak{M}) \) could be much longer than we care to deal with.

When the operator \( \varphi^\mathfrak{M}_{\xi,Z} \) corresponding to the body of a \( \mu \)-formula \( \mu Z. \varphi \) is \( \omega \)-chain-additive, that is, for \( F = \varphi^\mathfrak{M}_{\xi,Z} \)

\[
F \left( \bigcup_{n < \omega} A_n \right) = \bigcup_{n < \omega} F(A_n) \quad \text{where} \quad A_n \subseteq A_{n+1} \quad \text{for all} \quad n < \omega
\]

then the ordinal of convergence for \( ||\mu Z. \varphi||^\mathfrak{M}_{\xi} \) is at worst \( \omega \). In this case, we have a sequence of approximation formulas

\[
\varphi^0 = \mathfrak{f} \quad \text{and} \quad \varphi^{n+1} = \varphi[Z := \varphi^n] \quad \text{for} \quad n < \omega
\]

and

\[
||\mu Z. \varphi||^\mathfrak{M}_{\xi} = \bigcup_{n < \omega} ||\varphi^n||^\mathfrak{M}_{\xi}
\]

since \( ||\varphi^n||^\mathfrak{M}_{\xi} = ||\varphi||^\mathfrak{M}_{\xi,n} \). The terms "order-continuous" and "continuous from below" are also used instead of \( \omega \)-chain-additive, since such an \( F : \mathcal{P}(X) \rightarrow \mathcal{P}(X) \) is a continuous function with respect to the Scott topology on the complete partial order \( (\mathcal{P}(X), \subseteq) \). We adapt the terminology of Jónsson and Tarski [26] on Boolean algebras with operators, since we are interested in other meanings of "continuous". Dually, when \( \varphi^\mathfrak{M}_{\xi,Z} \) is \( \omega \)-chain-multiplicative, the ordinal of convergence for \( ||\nu Z. \varphi||^\mathfrak{M}_{\xi} \) is at worst \( \omega \), and the sequence of approximation formulas starts at \( \mathfrak{f} \) and decreases.

In particular, the semantic operator corresponding to the body of \( \langle h \rangle \varphi \) (or \( \overline{\langle h \rangle \varphi} \)), as defined in (5), for sentences \( \varphi \), is:

\[
A \mapsto \sigma(c)(||\varphi||^\mathfrak{M}_{\xi}) \cup \sigma(ec)(A)
\]

Since the \( \exists \)-pre-image of any relation is completely additive, i.e. distributes over arbitrary unions, it follows that \( ||\langle h \rangle \varphi||^\mathfrak{M} \) is the union of the denotations of the approximation sequence

\[
\mathfrak{f}, \quad \langle e \rangle \varphi, \quad \langle e \rangle \varphi \lor \langle e \rangle \langle c \rangle \langle e \rangle \varphi, \quad \langle e \rangle \varphi \lor \langle e \rangle \langle c \rangle \langle e \rangle \varphi \lor \langle e \rangle \langle c \rangle \langle e \rangle \langle e \rangle \langle e \rangle \varphi, \ldots
\]

Dually, the semantic operator corresponding to \( [h] \) is completely multiplicative. When \( \approx \) is a bisimulation equivalence on \( \mathfrak{M} \) – that is, an equivalence relation on \( X \) which respects the transition relations \( a^\mathfrak{M} \) and the observation sets \( ||p||^\mathfrak{M} \)
in a suitable sense$^3$ – then the fundamental property of truth-preservation is as follows: for all sentences $\varphi \in S_\mu(\Phi, \Sigma)$ and all $x, y \in X$,

$$x \approx y \implies [x \in \|\varphi\|^<_\mu \iff y \in \|\varphi\|^<_\mu]$$

(19)

It follows that if $\approx$ is a bisimulation equivalence of finite index $N$, then the denotation $\|\varphi\|^<_\mu$ of each sentence is a finite union of equivalence classes under $\approx$. Hence for sentences $\mu Z \varphi$ and $\nu Z \varphi$, the ordinal of convergence for $\|\mu Z \varphi\|^<_\mu$ and $\|\nu Z \varphi\|^<_\mu$ is bounded by $N$. In this case, the finite quotient LTS $2^\mathbb{M}_\approx$ is a finite simulacrum, and finite automaton representation, of the original system $\mathbb{M}$. If such is the case, the countable $\mu$-algebra $S^\mathbb{M}_\mu$ is in fact a finite algebra, and the atoms of the algebra are the equivalence classes under $\approx$. The familiar bisimulation algorithm ([19] §3.1; [27] §2) can be reinterpreted algebraically as the construction of a sequence of algebras $S^\mathbb{M}_k$ for $k < \omega$, where

$$S^\mathbb{M}_k = \{\|\varphi\|^<_\mu | \varphi \in S_k(\Phi, \Sigma)\}$$

is the finite Boolean algebra of denotations of modal sentences of modal degree $\leq k$. The modal degree measures depth of nesting of modal operators; for example, for hybrid trajectory formulas of the form (3), the degree is $2n + 1$, where $n$ is the length of the discrete trace. It follows that $S^\mathbb{M}_{k+1}$ is the smallest Boolean algebra generated by $S^\mathbb{M}_k \cup \{\sigma(a^\mathbb{M})(A) | A \in S^\mathbb{M}_k\}$. The algorithm terminates at stage $k + 1$ if $S^\mathbb{M}_{k+1} = S^\mathbb{M}_k$, in which case the equivalence relation:

$$x \approx S^\mathbb{M}_k y \triangleq (\forall A \in S^\mathbb{M}_k)[x \in A \iff y \in A]$$

is a finite bisimulation equivalence whose equivalence classes are atoms of the algebra $S^\mathbb{M}_k$, and $S^\mathbb{M}_\mu = S^\mathbb{M}_k$.

4 Adding topological and metric tolerance structure

Within modal logic, there is a well-known way of representing a topology $T$ on the state space $X$ of an LTS or Kripke model. From McKinsey and Tarski's work in the 1940's ([31], [32], [36]), the axioms for the box $\Box$ modality of the modal logic $S4$ correspond exactly to those of the Kuratowski axioms for the topological interior operator $\operatorname{int}_T$, and dually, the $S4$ diamond $\Diamond$ corresponds to topological closure $\operatorname{cl}_T$. $S4$ is a well-studied modal logic, and is of particular interest in virtue of the 1933 Gödel translation of Intuitionistic logic into (classical) $S4$. The relational Kripke semantics for $S4$ is in terms of pre-orders:

$^3$ The concept is not formally defined here. An analysis of the concept of bisimulation is given in [11]. See also the handbook article [38] §5.3, where it is noted that if one wants to preserve the truth of sentences containing the converse operation, then the notion of bisimulation must be strengthened so as to include respect for the converses of the $a^\mathbb{M}$. 
reflexive and transitive relations $\subseteq X \times X$, and can be shown to be a special case of the topological semantics via Alexandroff topologies, which are in one-one correspondence with pre-orders (see [11]). For background on general topology, see [33], [24].

Let $F_{\mu, \Box}(\Phi, \Sigma)$ denote the collection of formulas defined as in Definition 3 with an additional clause for a plain $\Box$ modality, with analogous notation for the collection of sentences, and the purely modal fragments. The diamond is defined by the usual negation (de Morgan) duality: $\Diamond \varphi \equiv \neg \Box \neg \varphi$.

**Definition 7.** If $M = (X, T, \{\varphi^a\}_{a \in A}, \{\varphi^p\}_{p \in P})$ is a topologized LTS model then the additional clauses to be added to Definition 4 for the semantics of formulas $\varphi \in F_{\mu, \Box}(\Phi, \Sigma)$ are:

$$||\Box \varphi||^T = \text{int}_T \left(||\varphi||^T\right) \quad \text{and} \quad ||\Diamond \varphi||^T = \text{cl}_T \left(||\varphi||^T\right)$$

In the enriched language, we can simply express topological properties of sets of states. For example, a set $||\varphi||^M \subseteq X$ is, respectively, open, closed, dense or nowhere dense (empty interior), with respect to $T$, exactly when the sentences $\varphi \rightarrow \Box \varphi$, $\Box \varphi \rightarrow \varphi$, $\varphi$, or $\neg \varphi$ are true in $M$. The topological boundary of $||\varphi||^M$ is denoted by the sentence $\Diamond \varphi \land \neg \Box \varphi$ (and boundary sets are always nowhere dense).

Note that if $X \subseteq \mathbb{R}^n$ is first-order definable in an o-minimal structure $\mathbb{R}$, $T$ is the subspace topology on $X$ inherited from the standard metric topology on $\mathbb{R}^n$ (derived from the order $<$ on $\mathbb{R}$), and $A \subseteq X$ is definable, then $\text{int}_T(A)$ and $\text{cl}_T(A)$ are also definable ([14], Lemma 3.4). Thus if the components of a topologized model $M$ are definable in $\mathbb{R}$, then the topological modal algebra

$$S^M_{\Phi} \equiv \{||\varphi||^M | \varphi \in S_{\Phi}(\Phi, \Sigma)\}$$

of denotations of modal sentences including $\Box$ is also definable. From the perspective of o-minimality, observe that the cells of a cell decomposition of a definable $X \subseteq \mathbb{R}^n$ are either open in $\mathbb{R}^n$, or else are boundary sets ([14], Proposition 2.5) - properties expressible in the enriched modal language.

Note that if we want a bisimulation to be truth-preserving with respect to sentences $\varphi \in S_{\Phi}(\Phi, \Sigma)$, then it must also respect the topology $T$. For equivalence relations $\simeq$, this amounts to the requirement that for each equivalence class $B$ under $\simeq$, the closure $\text{cl}_T(B)$ must be a union of equivalence classes, thus either $\text{int}_T(B) = B$ or $\text{int}_T(B) = \varnothing$; in brief, the equivalence classes $B$ are “cell-like”.

OK, so we've formally got topologies in the picture, so we should be able to express some notion of continuity. A sticking point is that the standard notion of continuity is for functions, not relations. In purely topological terms, a function $f : (X, T) \rightarrow (Y, S)$ is continuous iff for every open set $U$ in $Y$, the inverse-image $f^{-1}(U)$ is open in $X$. The relevant notions for relations $r : (X, T) \sim (Y, S)$ were introduced by Kuratowski and Bouligand in the 1930's, and replace the functional inverse-image with the relational $\forall$- and $\exists$-pre-image operators.
Definition 8. ([6] §1.4; [1] Ch. 7; [24] §18.) A relation \( r : (X, T) \rightrightarrows (Y, S) \) is:

- upper semi-continuous (u.s.c.) iff for every open set \( U \) in \( Y \), the \( \forall \)-pre-image \( \tau(r)(U) \) is open in \( X \);
- lower semi-continuous (l.s.c.) iff for every open set \( U \) in \( Y \), the \( \exists \)-pre-image \( \sigma(r)(U) \) is open in \( X \);
- continuous iff it is both u.s.c. and l.s.c..

When \( r : (X, T) \rightrightarrows (Y, S) \) is in fact a (single-valued) function, each of the semi-continuity properties is equivalent to functional continuity, since in that case, the two relational pre-image operators collapse to the familiar inverse-image operator: \( \sigma(r) = \tau(r) = r^{-1} \). Logics of continuous functions are developed in [10].

The two semi-continuity properties are simply expressible in the language of the topological \( \mu \)-calculus by the formulas (sentence schemes):

\[
\left[ \alpha \right] \Box Z \rightarrow \square [\alpha] Z \quad \text{and} \quad \left[ \langle a \rangle \Box Z \rightarrow \Box \langle a \rangle Z \quad \right. \tag{20}
\]

In dual form, upper semi-continuity can be read as preservation of closed sets by the familiar \( \exists \)-pre-image \( \sigma(r) = \text{Pre}(r) \):

\[
\Diamond (a) Z \rightarrow \langle a \rangle \Box Z
\]

From these simple characterizations of the semi-continuity properties, it follows purely formally that each of the properties is inherited under finite relational compositions and finite relational unions (sums). Inheritance of continuity properties under infinitary fixed-point quantification is a topic of continuing investigation.

So far, the discussion of continuity is still rather formal, and a tad insubstantial. But in the case of compact metric spaces, we get to see some meat on the bones.

Proposition 1. ([1] Ch.7, Proposition 11) For relations \( r : X \rightrightarrows Y \) where \( X \) and \( Y \) are compact metric spaces and the direct image \( r(x) \subseteq Y \) for each \( x \in X \) is closed, the following are equivalent:

1. \( r \) is u.s.c.;
2. for all \( x \in X \) and all \( \epsilon > 0 \), there is a \( \delta > 0 \) such that for all \( x' \in X \) and \( y' \in Y \),
\[
d_X(x, x') < \delta \quad \text{and} \quad x' \xrightarrow{x} y' \quad \Rightarrow \quad (\exists y \in Y)(x \xrightarrow{x} y \text{ and } d_Y(y, y') < \epsilon)
\]
3. as a subset of \( X \times Y \), (the graph of) \( r \) is closed;

\(^4\) Note that in [6], [7], Aubin uses the terms "core" and "inverse-image" instead of universal and existential pre-image, while in [1], Akin uses but has neither names nor notation for the pre-image operators.
4. \( r : Y \leadsto X \) is u.s.c.

The following are also equivalent:

1. \( r \) is l.s.c.;
2. for all \( x \in X \) and all \( \epsilon > 0 \), there is a \( \delta > 0 \) such that for all \( x' \in X \) and \( y \in Y \),
\[
d_X(x, x') < \delta \quad \text{and} \quad x \xrightarrow{r} y \Rightarrow (\exists y' \in Y)[x' \xrightarrow{r} y' \text{ and } d_Y(y, y') < \epsilon]
\]

![Fig. 4. The u.s.c. property in the compact metric setting.](image)

The metric u.s.c. property says that if an input \( x' \) is within \( \delta \) of \( x \), then every point \( y' \) in the output or image \( r(x') \) is contained within an \( \epsilon \) “ball” or “tube” around \( r(x) \). For the orbit relation \( f : X \leadsto X \) of a semi-flow \( \phi : X \times \mathbb{R}^+ \rightarrow X \) (defined in (11)), where \( f(x) = \{\phi(x, t) \mid t \in \mathbb{R}^+\} \) is the positive trajectory from \( x \), the picture really is that of an \( \epsilon \)-tube: if \( d_X(x, x') < \delta \) then the trajectory \( f(x') \) lies inside an \( \epsilon \)-tube around the trajectory \( f(x) \), as illustrated in Figure 4. The idea is certainly reminiscent of the “tube neighborhoods” in the work of Gupta, Henzinger and Jagadeesan [17] on robust timed automata; the interest in that paper is on metrics on trajectories \( r \in (\Phi \times \mathbb{R}^+) \), where \( \Phi \) is a finite alphabet of event names.

When \( X \) is a compact metric space, \( \phi : X \times \mathbb{R}^+ \rightarrow X \) is a continuous semi-flow, and \( T \subseteq \mathbb{R}^+ \) is compact, the restricted orbit relation \( f^T : X \leadsto X \) given by \( f^T(x) = \{\phi(x, t) \mid t \in T\} \) has a closed graph and hence is u.s.c. ([1], Ch. 6). This leads to the following result on continuity properties of both sort of transition relations in an LTS model of a hybrid automaton.

**Proposition 2.** Let \( \mathcal{M}_q \) be the LTS model of a hybrid automaton, as in Definition 2. Assume that each \( X_q \subseteq \mathbb{R}^n \) is compact in the standard topology on \( \mathbb{R}^n \). Let \( T_q \) be the subspace topology on \( X_q \), and assume the semi-flow \( \phi_q : X_q \times \mathbb{R}^+ \rightarrow X_q \) is continuous.

1. If \( \text{Inv}_q \) is closed in \( T_q \), and time-bounded under \( \phi_q \), in the sense that there is a \( t_q > 0 \) such that for all \( x \in \text{Inv}_q \) and all \( t > t_q \), \( \phi_q(x, t) \not\in \text{Inv}_q \), then the relation \( e_q : X_q \leadsto X_q \) defined by \( e_q = f_q \cap (\text{Inv}_q \times \text{Inv}_q) \) is u.s.c.
2. If \( Grd_{q,q'} \subseteq X_q \) and \( Inv_{q} \subseteq X_q \) are both closed, in \( T_q \) and \( T_{q'} \) respectively, and the graph of \( r_{q,q'} : X_q \sim X_{q'} \) is closed, then the relation \( c_{q,q'} : X_q \sim X_{q'} \) defined by \( c_{q,q'} = r_{q,q'} \cap (Grd_{q,q'} \times Inv_{q'}) \) is u.s.c.

The point is that the u.s.c. property is sufficiently attractive that we may wish it to be the case that all our transition relations possess it. From our observations above, all finite compositions and unions of the \( e_q \) and \( c_{q,q} \) will be u.s.c. if the \( e_q \) and \( c_{q,q} \) are u.s.c.. Note also that for the constant jump relations \( c_{q,q'} = Grd_{q,q'} \times Rst_{q,q'} \) of [27], \( c_{q,q'} \) is u.s.c. when both \( Grd_{q,q'} \) and \( Rst_{q,q'} \) are closed.

When the relations \( e_q : X_q \sim X_q \) and \( c_{q,q'} : X_q \sim X_{q'} \) are lifted to relations \( X \sim X \), the issue arises as to what is the appropriate topology on the hybrid state space \( X \subseteq Q \times \mathbb{R}^n \)? Taking the \( X_q \) equipped with their standard topology from \( \mathbb{R}^n \), the question then becomes: what topology \( T_Q \) on the finite discrete state space \( Q \)? One reasonable choice is that \( Q \) really is discrete and has no topological structure, which amounts to taking \( T_Q \) to be the discrete topology. Then the lifted relations will be u.s.c. or l.s.c. whenever their unlifted counterparts are. An alternative reasonable choice is to consider \( Q \) as structured by the control graph \( G \subseteq Q \times Q \), so take \( T_Q = T_G \) to be the (Alexandroff) topology determined by the reflexive-transitive closure \( \leq_G \) of \( G \). The open (closed) sets in \( T_G \) are those \( P \subseteq Q \) that are up- (down-) invariant under \( \leq_G \); the clopen sets in \( T_G \) are cycles under \( G \). The inherited topology on \( X \subseteq Q \times \mathbb{R}^n \), and the continuity properties, are more complicated, and under current investigation.

Metric structure on the state space of an LTS model can be used to define explicit metric tolerance relations that allow us to express such properties as being within \( \epsilon \) of a set, for a particular \( \epsilon > 0 \). Again, the resources of modal logic come into play. For \( X \) a metric space and \( \epsilon > 0 \), define a relation of \( \epsilon \)-tolerance or \( \epsilon \)-indiscernability \((\epsilon) : X \sim X \) by:

\[
x \ (\epsilon) x' \iff d_X(x, x') < \epsilon
\]

Such a relation is reflexive and symmetric, but not transitive. My source for the notion of a tolerance relation is Smyth’s [37]. A motivating idea in that paper, which is traced back to Poincaré’s The Value of Science (1905) and independently, to the topologist Zeeman in the early 1960’s, is that perceptual or physical continua, as opposed to the idealized continua of classical mathematics, are of finite or countable cardinality and are structured by a relation of indiscernability that is reflexive and symmetric, but not transitive. In [1] Ch.1, the relation \((\epsilon)\) goes by the name \( V_\epsilon \).

Formally, we extend the alphabet \( \Sigma \) of transition labels with a new symbol \( \epsilon \). Interpreting the new modalities \((\epsilon)\) and \([\epsilon]\) in the standard way by the pre-image operators \( \sigma(\epsilon) \) and \( \tau(\epsilon) \), the sentence \((\epsilon)\varphi\) denotes the \( \epsilon \)-ball around \( \|\varphi\|_P \), or the \( \epsilon \)-closure of \( \|\varphi\|_P \) – that is, the set of states within \( \epsilon \) of some point in \( \|\varphi\|_P \), while \([\epsilon]\varphi\) denotes the \( \epsilon \)-interior of \( \|\varphi\|_P \) – that is, the set of states all of whose
\( \varepsilon \)-neighbors are in \( \| \varphi \|^{\mathcal{M}} \). The modalities for symmetric and reflexive relations are axiomatized by the modal logic \( \text{KTB} \); see [9] §4.3.

The combination of topological and tolerance structure opens up new possibilities. For example ([1] Ch.1, Corollary 2), if \( a^{\mathcal{M}} : X \rightarrow X \) is u.s.c. in a compact metric space \( X \), then for each closed set \( \| \varphi \|^{\mathcal{M}} \subseteq X \), and each \( \varepsilon > 0 \), there is a \( \delta > 0 \) such that the sentence

\[
(\delta)(a) \varphi \rightarrow (a)(\varepsilon) \varphi
\]

is true in \( \mathcal{M} \).

Metric tolerance structure can be used to define "imperfect precision" hybrid trajectories. In the LTS model \( \mathcal{M}_H \) of a hybrid automaton \( H \), suppose that on each projection \( X_q \subseteq \mathbb{R}^n \), we have a metric tolerance \( (\delta_q) : X_q \rightarrow X_q \) for some given \( \delta_q > 0 \). Then instead of considering "perfect precision" trajectories formed from the simple alternation of constrained evolution and controlled jump relations, as in (3), we might want to consider transition sequences:

\[
e_{q_0} \cdot (\delta_{q_0}) \cdot e_{q_0,q_1} \cdot e_{q_1} \cdot \delta_{q_1} \cdot e_{q_1,q_2} \cdot e_{q_2} \cdots e_{q_{k-1}} \cdot \delta_{q_{k-1}} \cdot e_{q_{k-1},q_k} \cdot e_{q_k}
\]

Operationally, this can be construed as allowing metric "gaps" of up to size \( \delta_q \) between the decision to make a controlled switch \( c_{q,q'} \), and the point at which such a switch actually occurs. Defining \( (\delta) : X \rightarrow X \) to be the union of each of the lifted relations \( (\delta_q) \), the dynamics of the class of all \( \delta \)-imperfect" hybrid trajectories with finite discrete traces are captured by the dual fixed-point modalities

\[
(\mathfrak{h}_q) \varphi \triangleq \mu Z. (e)(\varphi \lor (\delta)(c)Z) \quad \text{and} \quad [\mathfrak{h}_q] \varphi \triangleq \nu Z. [e] \varphi \land [e][\delta][c]Z
\]

Alternatively, one could "relax" the definition of the constrained evolution relation, and take

\[
(\delta_q)Z \leftrightarrow (\delta_q) \text{Inv}_q \land (f_q)(Z \land \text{Inv}_q)
\]

that is, \( \dot{e}_q = f_q \cap (\text{Inv}_q \times \sigma(\delta_q) \text{Inv}_q) \), where the revised convexity property is:

\[
(\tilde{f}_q) \text{Inv}_q \land (f_q)(\delta_q) \text{Inv}_q \rightarrow (\delta_q) \text{Inv}_q
\]

which says: curves along \( \phi_q \) that start in \( \text{Inv}_q \) and end in \( \sigma(\delta_q) \text{Inv}_q \) lie inside \( \sigma(\delta_q) \text{Inv}_q \).

5 Deductive Proof Systems

We present simple Hilbert-style axiomatic proof systems for the logics of interest. The axiomatizations are not intended to be minimal; rather, they are meant to
serve as a useful reference list. In particular, we give the axioms and rules for both of the dual diamond and box modalities. Kozen’s axiomatization $L_\mu$ [23] forms the foundation, with extensions developed in a modular fashion. So far, we have identified $S4$ for topological and relational pre-order modalities, and $KTB$ for tolerance relations. A further candidate is $S5$, the modal logic of equivalence relations: we can give modal representation to any partition of the state space of our choosing; bisimulation equivalences spring to mind. $S5$ is also the base of logics of knowledge [16]: the knowledge of an agent is modeled by the equivalence relation of indistinguishability relative to its knowledge base.

Equivalent Gentzen sequent-style proof systems for the $\mu$-calculus are presented in [5], [8], and also in [40].

**Definition 9.** The Hilbert-style proof system for the logic $L_\mu$ has the following axioms: for transition labels $a \in \Sigma$, propositional variables $Z, W \in \text{PVar}$, and formulas $\varphi \in \mathcal{F}_\mu(\Phi, \Sigma)$,

\[
\begin{align*}
\text{CP :} & \quad \text{axioms of classical propositional logic} \\
\vee-\langle a \rangle : & \quad \langle a \rangle (Z \lor W) \leftrightarrow ((\langle a \rangle Z) \lor (\langle a \rangle W)) \\
\wedge-[a] : & \quad [a] (Z \land W) \leftrightarrow ([a] Z \land [a] W) \\
\mu-\text{f.p.} : & \quad [\varphi[Z := \mu Z.\varphi] \rightarrow \mu Z.\varphi] \\
\nu-\text{f.p.} : & \quad [\nu Z.\varphi \rightarrow \varphi[Z := \nu Z.\varphi]]
\end{align*}
\]

and the inference rules, for formulas $\varphi, \psi \in \mathcal{F}_\mu(\Phi, \Sigma)$:

- **modus ponens:** \[ \frac{\varphi, \varphi \rightarrow \psi}{\psi} \]
- **substitution:** \[ \frac{\varphi[Z := \psi]}{\varphi} \]
- **$\langle a \rangle$-monotonicity:** \[ \frac{\varphi \rightarrow \psi}{\langle a \rangle \varphi \rightarrow \langle a \rangle \psi} \]
- **$[a]$-monotonicity:** \[ \frac{\varphi \rightarrow \psi}{[a] \varphi \rightarrow [a] \psi} \]
- **$\mu$-least-f.p.:** \[ \frac{\varphi[Z := \psi] \rightarrow \psi}{\mu Z.\varphi \rightarrow \psi} \]
- **$\nu$-greatest-f.p.:** \[ \frac{\psi \rightarrow \varphi[Z := \psi]}{\psi \rightarrow \nu Z.\varphi} \]
- **Hoare composition:** \[ \frac{\psi \rightarrow \langle a \rangle \chi \quad \chi \rightarrow \langle b \rangle \varphi}{\psi \rightarrow \langle a \rangle \langle b \rangle \varphi} \]
- **Hoare composition:** \[ \frac{\psi \rightarrow [a] \chi \quad \chi \rightarrow [b] \varphi}{\psi \rightarrow [a][b] \varphi} \]
We write: \( L \vdash \varphi \) for formulas \( \varphi \in \mathcal{F}_\mu(\Phi, \Sigma) \) if there is a proof of \( \varphi \) in \( L_\mu \).

The axioms and monotonicity rules for \( \langle a \rangle \) and \( [a] \) together assert they are normal diamond (possibility) and box (necessity) modalities ([9] Ch. 4); they are equivalent to system \( K \) (for Kripke), the logic of generic binary relations. In the language of [26], \( \langle a \rangle \) denotes a normal and finitely additive operator on a Boolean algebra. The Hoare composition rules follow readily from monotonicity. As always, we assume substitutions \( \varphi[Z := \psi] \) are legitimate ones; i.e. no capture of free variables.

The axioms and rules for the fixed-point quantifiers assert what they ought: that \( \mu Z. \varphi (\nu Z. \varphi) \) is the least (greatest) fixed point of the operator defined by \( \varphi \).

Each of the rules is readily verified to be truth-preserving, in the sense that for any LTS model \( M \), if the hypotheses of a rule is true in \( M \) then the conclusion is true in \( M \). From the verification that the each of the axioms is true in every LTS model, we then get soundness: if \( L_\mu \vdash \varphi \) then \( M \models \varphi \) for all LTS models \( M \) of signature \( (\Phi, \Sigma) \).

**Definition 10.** The Hilbert-style proof system for the logic \( L_\mu + S4 \) in the language \( \mathcal{F}_\mu, \mathcal{D}(\Phi, \Sigma) \) is obtained from that of \( L_\mu \) by adding the normality axioms and rules for \( \ominus \) and \( \Box \), together with: for propositional variables \( Z \in PVar, \)

\[
\begin{align*}
T\ominus & : Z \to \ominus Z \\
T\Box & : \Box Z \to Z \\
4\ominus & : \Box Z \to \ominus Z \\
4\Box & : Z \to \Box Z
\end{align*}
\]

The proof system for the logic \( L_\mu + S4 + C_a \) is that of \( L_\mu + S4 \) together with \( C_a \), where \( C_a \) is one or more of the semi-continuity axiom schemes:

\[
\begin{align*}
usc(a) & : \Box \langle a \rangle Z \to \langle a \rangle \Box Z \\
usc[a] & : [a] \Box Z \to \Box [a] Z \\
Isc(a) & : \langle a \rangle \Box Z \to \Box [a] Z \\
Isc[a] & : \Box [a] Z \to \langle a \rangle \Box Z
\end{align*}
\]

In the relational (preorder) semantics for \( S4 \), the \( T \) axioms correspond to reflexivity, while the \( 4 \) axioms correspond to transitivity. Extensions of the Hoare composition rules:

\[
\begin{align*}
\psi \to [a] \Box \chi & \quad \chi \to [b] \Box \varphi \\
\psi \to \langle a \rangle \Box \chi & \quad \chi \to \langle b \rangle \Box \varphi
\end{align*}
\]

can be derived in the systems \( L_\mu + S4 + usc[a] + usc[b] \) and \( L_\mu + S4 + Isc(a) + Isc(b) \) respectively.

**Definition 11.** The Hilbert-style proof system for the logic \( L_\mu + KTB \) in the language \( \mathcal{F}_\mu(\Phi, \Sigma \cup \{\epsilon\}) \) is obtained from that of \( L_\mu \) by adding the normality axioms and rules for \( \epsilon \) and \( [\epsilon] \); the axioms \( T(\epsilon) \) and \( T[\epsilon] \); and also:

\[
\begin{align*}
B(\epsilon) & : \langle \epsilon \rangle [\epsilon] Z \to Z \\
B[\epsilon] & : Z \to [\epsilon] \langle \epsilon \rangle Z
\end{align*}
\]

The \( B \) axioms express that tolerance relations \( (\epsilon) \) are symmetric.
Definition 12. The Hilbert-style proof system for the logic $L_\mu + S5$ in the language $\mathcal{F}_\mu(\Phi, \Sigma \cup \{\approx\})$ is obtained from that of $L_\mu$ by adding the normality axioms and rules for $\langle \approx \rangle$ and $[\approx]$; the axioms $T(\approx)$, $T[\approx]$, $4(\approx)$ and $4[\approx]$; and also:

\[ 5(\approx) : \langle \approx \rangle [\approx] \rightarrow [\approx] \quad 5[\approx] : \langle \approx \rangle \rightarrow [\approx] [\approx] \]

The 5 axioms express that $\approx$ is a Euclidean relation: if $x \approx y$ and $x \approx z$ then $y \approx z$. And reflexive, transitive and Euclidean binary relations are exactly equivalence relations. Under the knowledge interpretation of $S5$, the axiom $5[\approx]$ is usually referred to as the axiom of negative introspection: $\neg[\approx] \varphi \rightarrow [\approx] \neg[\approx] \varphi$, which reads: “if it is not the case that agent A knows $\varphi$, then agent A knows that it is not the case that she knows $\varphi$.”

Walukiewicz has recently established the completeness of the Kozen axiomatization with respect to the standard set-theoretic semantics for the $\mu$-calculus.

Theorem 1. ([39],[40]) Soundness and Completeness of $L_\mu$ (set-theoretic semantics)

For all formulas $\varphi \in \mathcal{F}_\mu(\Phi, \Sigma)$,
\[ L_\mu \vdash \varphi \iff M \vdash \varphi \quad \text{for all LTS models } M \text{ of signature } (\Phi, \Sigma). \]

The completeness part of the cited theorem is stated in the form: if $\varphi$ is unsatisfiable in every LTS model $M$, i.e. $[\varphi]_\xi = \emptyset$ for all assignments $\xi$ in $\mathcal{P}(X)$, then $\neg \varphi$ is provable in $L_\mu$. Walukiewicz’s proof is very intricate, proceeding by first contracting to a subclass of “nice” formulas, and then producing a “tableaux refutation” of unsatisfiable formulas of nice form, where such a refutation in turn implies that the negation of the given formula is provable in $L_\mu$. Topics of continuing enquiry include whether the Walukiewicz proof can be extended to cover specific modal enrichments of $L_\mu$, and the relationship between his tableaux refutation system and a tableaux proof system for the $\mu$-calculus and polymodal extensions, in the style of [35] and [10].

The algebraic semantics of Kwiatkowska et al. [5], [8], provide a framework for extending Stone duality theory to the algebra of fixed-points. Their proof of completeness for modal $\mu$-frames starts with the Lindenbaum algebra $\mathcal{F}_{L_\mu}$ of formulas in $\mathcal{F}_\mu(\Phi, \Sigma)$ modulo provable equivalence in $L_\mu$, then realizes the abstract $\mu$-algebra as a canonical LTS model $\mathbb{M}_{L_\mu}$ with state space the Stone space $X = \text{Ult}(\mathcal{F}_{L_\mu})$ of (Boolean) ultrafilters in $\mathcal{F}_{L_\mu}$, together with the canonical $\mu$-algebra $\mathcal{A}_{L_\mu} = \text{Clop}(\text{Ult}(\mathcal{F}_{L_\mu})) \cong \mathcal{F}_{L_\mu}$ of subsets of $X$ clopen in the Stone topology. For each $a \in \Sigma$, and $M = \mathbb{M}_{L_\mu}$, the relations $\xrightarrow{a}$ on $X$ are defined by:
\[ x \xrightarrow{a} y \iff (\forall \overline{\varphi} \in \mathcal{F}_{L_\mu}) \left[ [a] \overline{\varphi} \in x \Rightarrow \overline{\varphi} \in y \right]. \]

The formal statement of the result is as follows.

Theorem 2. ([5]) Soundness and Completeness of $L_\mu$ (algebraic semantics)

For all formulas $\varphi \in \mathcal{F}_\mu(\Phi, \Sigma)$,
\[ L_\mu \vdash \varphi \iff (M, A) \models \varphi \quad \text{for all modal } \mu\text{-frames } (M, A) \text{ of signature } (\Phi, \Sigma). \]
In [8] §6, it is established if \((M, A)\) is a descriptive modal \(\mu\)-frame, then \((M, A)\) is in semantic agreement with \(M\). In particular, the canonical frame \((M_{L^\mu}, A_{L^\mu})\) is descriptive, and thus in semantic agreement with the underlying LTS model \(M_{L^\mu}\). Thus the “easy” algebraic proof of completeness can be used to give an alternative proof of completeness of \(L^\mu\) with respect to the standard set-theoretic semantics, as stated in Theorem 1.

The Kwiatkowska algebraic completeness proof extends quite smoothly to normal polymodal extensions of the \(\mu\)-calculus, including topological \(S4\) extensions with semi-continuity axioms. For example, if \(L = L^\mu + S4 + \{usc(a) + lsc(a)\}_{a \in V}\), the topology on the canonical model \(M_L\) comes from a relation \(\preceq\) on \(X = Ult(F_L)\) defined in the same way as the relations \(a^{M^L}\) as above. The \(S4\) axioms ensure that the relation \(\preceq\) is a preorder, so the topology is Alexandroff, and from the semi-continuity axiom schemes, one proves that each of the relations \(a^{M^L}\) have the corresponding semi-continuity property. A more detailed treatment is given in [12].

6 Discussion

We have developed a family of expressively rich and usable logical systems and broadened horizons for the formal analysis of hybrid dynamical systems. In addition to those mentioned in the text, further lines of enquiry include the following.

- Investigation of non-deterministic continuous dynamics, in the form of set-valued or parametrized semi-flows, and their topological properties. Our relation-based view of dynamics is of course conducive to such generalizations.
- A deeper investigation of relations (definable families) in \(o\)-minimal structures, and of the use of finite cell-decomposition in the construction of topological bisimulations.
- Further investigation of finite sub-topologies of the standard topology on \(X \subseteq \mathbb{R}^n\), and semi-continuity properties of relations in such topologies, pursuing themes developed in [11].
- Application to hybrid systems of the theory of knowledge in multi-agent settings and its formalization in \(S5\) based logics of knowledge.
- LTS models and \(\mu\)-calculus specifications of \(hybrid petri nets\). One approach is to take the state space \(X\) to be a set of finite partial functions \(x: P \rightharpoonup \mathbb{R}\) (equivalently, variable-length vectors over \(\mathbb{R}\)), where \(P\) is the finite set of \(places\) of the net.
- Application of game-theoretic methods for the \(\mu\)-calculus, and related work on automata over transition systems; e.g. [25], [22].
- Investigation of \(tableaux proof systems\) for polymodal logics and the \(\mu\)-calculus, in the style of [35] and [10].
- Investigation of \(Intuitionistic\) (constructive) logics for hybrid systems, using topological semantics and \(S4\) as a bridge between the classical and constructive worlds.
Acknowledgments: I would like to thank Prof. Anil Nerode, David Cook, Joe Miller, Suman Ganguli and Prof. Dexter Kozen for valuable conversations, and Xi Krump for graphic artistry.

References


