Proving Safety Properties of Hybrid Systems*

Arjun Kapur[†] Thomas A. Henzinger[‡] Zohar Manna[§] Amir Pnueli[¶]

Abstract

We propose a methodology for the specification, verification, and design of hybrid systems. The methodology consists of the computational model of *Concrete Phase Transition Systems* (CPTSs), the specification language of *Hybrid Temporal Logic* (HTL), the graphical system description language of *Hybrid Automata*, and a proof system for verifying that hybrid automata satisfy their HTL specifications.

The novelty of the approach lies in the continuous-time logic, which allows specification of both point-based and interval-based properties (i.e., properties which describe changes over an interval) and provides direct references to derivatives of variables, and in the proof system that supports verification of point-based and interval-based properties. The proof rules demonstrate that sound and convenient induction rules can be established for continuous-time logics. The proof rules are illustrated on several examples.

1 Introduction

Hybrid systems are real-time systems that allow continuous state changes, over time periods of positive duration, as well as discrete state changes, in zero time. Ubiquitous examples of hybrid systems appear in nature, since all analog physical phenomena, typically modeled by differential equations, that interact with digital devices, usually modeled by finite automata, can be regarded as hybrid systems. It is the interaction of continuous and discrete change that makes hybrid systems interesting and nontrivial targets for formal analysis. While mathematical methods for continuous equations and for discrete transitions have been studied independently for quite some time, the development of methods for formal reasoning about hybrid systems is relatively recent; it's origin in computer science can be traced to [Schn88, MMP92].

Suppose engineers are charged with designing a digital controller for some physical phenomenon and wish to ensure that the designed controller meets the requirements specification: how should they proceed? We offer a methodology that allows the engineers to specify a hybrid design in a convenient formalism, and to prove, using verification rules, that the design satisfies the desired properties.

Our methodology rests on three foundations. For the formal description of hybrid systems, we use *Hybrid Automata* [ACHH93], an extension of finite automata with analog variables that are governed by differential equations. For the formal description of system requirements, we use *Hybrid Temporal Logic* (HTL) [HMP93], an extension of interval temporal logic with limit and derivative terms for analog variables. To facilitate the proof of HTL formulas over the runs of hybrid automata, we introduce *Concrete Phase Transition Systems* (CPTSs), a concrete instance of transition systems on phases of continuous state change [MMP92, NSY92, HMP93].

*This paper appeared in the *Proceedings of the Third International Symposium on Formal Techniques in Real-time and Fault-tolerant Systems*, Lecture Notes in Computer Science **863**, Springer-Verlag, 1994, pp. 431–454.

[†]Department of Computer Science, Stanford University, Stanford, California 94305. Supported in part by a National Science Foundation Graduate Research Fellowship.

[‡]Department of Computer Science, Cornell University, Ithaca, New York 14853. Supported in part by the National Science Foundation under grant CCR-9200794, by the United States Air Force Office of Scientific Research under contract F49620-93-1-0056, and by the Defense Advanced Research Projects Agency under contract NAG2-892.

[§]Department of Computer Science, Stanford University, Stanford, California 94305. Supported in part by the National Science Foundation under grant CCR-92-23226, by the Defense Advanced Research Projects Agency under contract NAG2-703 and NAG2-892, and, by the United States Air Force Office of Scientific Research under contract F49620-93-1-0139.

[¶]Department of Applied Mathematics, The Weizmann Institute of Science, Rehovot, Israel 76100. Supported in part by the European Community ESPRIT Basic Research Action Project 6021 (REACT).

We proceed in two steps. First we give a translation of hybrid automata into the computational model of CPTS. Second we present rules for proving safe HTL formulas over the runs of a CPTS. We consider both point-based and interval-based safety properties of hybrid systems. *Point-based properties* refer to all individual states along a run, such as the safety requirement that the value of the variable x never exceeds 5. *Interval-based properties* refer to time periods of positive duration on a run, such as the safety requirement that during all periods of duration at most 3 the value of x increases monotonically by at most 5. We introduce verification rules for both types of invariances, and illustrate their use on a variant of the gas burner example of [CHR91].

Our approach in this paper differs from that used in [MP93] in two respects. The logic used here is based on an interval temporal logic, while the logic of [MP93] is a point-based temporal logic. The advantages of an interval-based logic is that it provides a natural expression for developments and changes across an arbitrary interval. To express the same properties in a point-based logic it is always necessary to introduce additional auxiliary "freeze" variables which record the state at the beginning of the interval of interest. Since the continuous development over an interval, forming a phase in a phase transition system, is of principal interest, it is important to be able to express such properties in the most natural way.

Another difference is that the models for the logic used here are dense, while the models of [MP93] are based on a sampling semantics in which discrete transitions are interleaved, and continuous activities are sampled at discrete points. While our approach can be easily adjusted for an interleaving semantics, where it is possible for the system to be in multiple states at the same time, our truly continuous modeling of phases allows us to reason directly with limits and derivatives. It also enables one to express fundamental properties such as precise delay in a more direct and natural way than is possible under the sampling semantics.

2 Hybrid Temporal Logic

The behavior of a hybrid system is modeled by a function that assigns to each real-numbered time a system state, i.e., values for all system variables. We require that, at each point, the behavior function has a limit from the left and a limit from the right. Discontinuities are points where the two limits differ.

To specify properties of behavior functions, we present a continuous-time interval temporal logic with a chop operator [HKP82], denoted as ";", whose semantics is a continuous-time extension to [Mos85] discrete-time chop operator.

Syntax

Because we wish to reason about physical phenomena in a natural and formal way, we introduce a logic that allows derivatives and limits as atomic expressions. Our logic, HTL, is a variant of the hybrid temporal logic of [HMP93].[1] Let V be a finite set of typed variables, where the allowed types are *boolean*, *integer*, and *real*. We view the booleans and the integers as subsets of the reals, where *false* and *true* correspond to 0 and 1, respectively. For a variable $x \in V$, we write $\overleftarrow{x}$ for the limit from the right (the *right limit*), and $\overrightarrow{x}$ for the limit from the left (the *left limit*) of x. We write $\dot{\overleftarrow{x}}$ for the right derivative of x (with respect to time), and $\dot{\overrightarrow{x}}$ for the left derivative of x (with respect to time). Note that the terms, right-hand limit and left-hand limit, are consistent with standard calculus terminology, and that right-hand limits are applied at the left end of an interval, while left-hand limits are applied at the right end. To avoid confusion, we will mostly use the terms "limit from the right" and "limit from the left".

A *local formula* is a formula over the variables in V, their left and right limits, their left and right derivatives, and function and predicate symbols from a language $\mathcal{L}$. The formulas φ of *Hybrid Temporal Logic* (HTL) are defined inductively as follows:

$$\varphi \ := \ \psi \mid \mathit{fin} \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 ; \varphi_2 \mid \forall x.\, \varphi$$

where $x \in V$ and ψ is an atomic local formula.

A *state formula* is a first-order logic formula over the variables in V (i.e., in which no limits, derivatives, or chops appear). If ψ is a state formula, we write $\overleftarrow{\psi}$ (and $\overrightarrow{\psi}$) for the local formula that results from ψ

[1] We restrict ourselves to piecewise smooth functions that are always right continuous.

by replacing each variable occurrence x in ψ with its limit from the right $\overleftarrow{x}$ (and limit from the left $\overrightarrow{x}$, respectively).

Semantics

Let $\mathcal{R}$ be the set of real numbers. A *state* $\sigma \colon V \to \mathcal{R}$ is a type-consistent interpretation of the variables in V (i.e., boolean variables may only be interpreted as 0 or 1, and integer variables may only be interpreted over the integers). For each $x \in V$, let $\sigma[x]$ denote the value σ assigns to x. We write Σ_V for the set of states.

Time is modeled by the nonnegative real line R^+. A (left-closed right-open) *interval* $[a, b)$, where $a \in \mathrm{R}^+$, $b \in \mathrm{R}^+ \cup \{\infty\}$, and $a < b$, is the set of points $t \in \mathrm{R}^+$ such that $a \leq t < b$.

Let $I = [a, b)$ be an interval. A function $f \colon I \to \mathcal{R}$ is *piecewise smooth* in I if

- at a, the limit from the right of f exists, and the derivative from the right of f exists;
- at all internal points $t \in (a, b)$, the limit from the right, the limit from the left, and all left and right derivatives of f exist;
- at all points $t \in [a, b)$, f is continuous from the right;[2]
- if $b < \infty$, then the limit from the left of f exists at b, and the left derivative of f exists at b.

A *phase* $P = \langle I, f \rangle$ over V is a pair consisting of

- a nonempty left-closed right-open interval $I = [a, b)$, and
- a type-consistent family $f = \{f_x \mid x \in V\}$ of functions $f_x : I \to \mathcal{R}$ that are piecewise smooth in I and assign to each point $t \in I$ a value for the variable $x \in V$.

It follows that the phase P assigns to every real-valued time $t \in I$ a state $f(t) \in \Sigma_V$. Furthermore, the limit from the right of f at a, and the limit from the left of f at b, if $b < \infty$, are defined.

We write

$$\overleftarrow{P} \;=\; \lim_{t \to a} \{f(t) \mid a < t < b\}$$

for the *left-end limit state* $\overleftarrow{P} \in \Sigma_V$ of the phase P, and

$$\overrightarrow{P} \;=\; \lim_{t \to b} \{f(t) \mid a < t < b\}$$

for the *right-end limit state* $\overrightarrow{P} \in \Sigma_V$ of P, if $b < \infty$.

Let $I_1 = [a, b)$ and $I_2 = [c, d)$ be two intervals, and let $P_1 = \langle I_1, f \rangle$ and $P_2 = \langle I_2, g \rangle$ be two phases. The phase P_2 is a *subphase* of P_1 if $I_2 \subseteq I_1$ and, for all $t \in I_2$, $g(t) = f(t)$. The phases P_1 and P_2 are *adjacent* if $b = c$. For two adjacent phases $P_1 = \langle [a, b), f \rangle$ and $P_2 = \langle [b, c), g \rangle$, we denote by $P_1 {}^\frown P_2$ the phase $\langle [a, c), h \rangle$ such that h coincides with f on $t \in [a, b)$ and h coincides with g on $t \in [b, c)$. The phase P is said to be *partitioned* by the phases P_1 and P_2 if $P = P_1 {}^\frown P_2$.

The formulas of hybrid temporal logic are interpreted over phases. A phase $P = \langle [a, b), f \rangle$ *satisfies* the hybrid temporal formula φ, denoted $P \models \varphi$, according to the following inductive definition:

For a local formula ψ, we distinguish between two cases:

1. If ψ does not contain left limits or left derivatives, then
   $P \models \psi$ iff the local formula ψ evaluates to *true*, where
   - x is interpreted as the value of f_x at a,

$$x \;=\; f_x(a)$$

[2] This allows one to chop an arbitrary piecewise smooth function into intervals of the form $[a, b)$ that are continuous from both the left and the right.

- $\overleftarrow{x}$ is interpreted as the limit from the right of f_x at a,[3]

$$\overleftarrow{x} \;=\; \lim_{t \to a} \{ f_x(t) \mid a < t < b \}$$

- $\overleftarrow{\dot{x}}$ is interpreted as the right derivative of f_x at a,

$$\overleftarrow{\dot{x}} \;=\; \lim_{t \to a} \Big\{ (f_x(t) - \overleftarrow{x})/(t-a) \mid a < t < b \Big\}.$$

2. If ψ contains left limits or derivatives, then
   $P \models \psi$ iff $b < \infty$ and the local formula ψ evaluates to *true*, where we evaluate variables, right limits, and right derivatives as above, and
   - $\overrightarrow{x}$ is interpreted as the limit from the left of f_x at b,

   $$\overrightarrow{x} \;=\; \lim_{t \to b} \{ f_x(t) \mid a < t < b \}$$

   - $\overrightarrow{\dot{x}}$ is interpreted as the left derivative of f_x at b,

   $$\overrightarrow{\dot{x}} \;=\; \lim_{t \to b} \Big\{ (f_x(t) - \overrightarrow{x})/(t-b) \mid a < t < b \Big\}.$$

$P \models \mathit{fin}$ iff $b < \infty$.

$P \models \neg\varphi$ iff $P \not\models \varphi$.

$P \models \varphi_1 \vee \varphi_2$ iff $P \models \varphi_1$ or $P \models \varphi_2$.

$P \models \varphi_1 ; \varphi_2$ iff there are two phases, P_1 and P_2, that partition P such that $P_1 \models \varphi_1$ and $P_2 \models \varphi_2$.

$P \models \forall x.\, \varphi$ iff $P' \models \varphi$ for all phases $P' = \langle [a,b), f' \rangle$ that differ from P at most in the interpretation f'_x of x.

We will freely use the first-order connectives, "$\wedge$", "$\rightarrow$", and "$\exists$", in the rest of this paper, as they can be defined in terms of the other connectives in the usual way.

Note that due to the dependence of the satisfaction relation on the syntactic occurrence of left limits and derivatives in local formulas, one should be careful in substitutions of formulas referring to left limits and derivatives. For example, the formula $\overrightarrow{x} = \overrightarrow{x}$ is not equivalent to *true* because $\overrightarrow{x} = \overrightarrow{x}$ is false on all infinite intervals. Also, the formula $\exists y.\, \Box(y = \overleftarrow{\dot{x}})$ is not always valid. In particular, any phase in which $\overleftarrow{\dot{x}}$ is not continuous from the right will fail to satisfy the formula, since variables are required to be right continuous, while derivatives are not.

A *point-based* property is a property that can be expressed by an HTL formula which has no occurrences of limits or derivatives. For example, all state formulas express point-based properties. An *interval-based property* is a property that can only be expressed by an HTL formula that contains limits or derivatives. For example, $(\overleftarrow{x} = 1); (\overleftarrow{x} = 2)$ is a point-based property because it can also be expressed by the equivalent HTL formula $(x = 1); (x = 2)$. On the other hand, $(\overrightarrow{x} = 1); (\overleftarrow{x} = 2)$ specifies an interval-based property. For a variable x and a phase P, the semantics of HTL assigns the same value to $\overleftarrow{x}$ and x, and so all occurrences of right limits may be replaced by corresponding variable occurrences. Thus the presence of right limits in a formula doesn't preclude it from being a point-based property.

Abbreviations

As in [HMP93], we define abbreviations for common temporal formulas. The following abbreviations express that a leftmost subphase, a rightmost subphase, or any subphase of a phase satisfies the formula φ:

$\lhd\varphi$	stands for	$\varphi \vee (\varphi; \mathit{true})$
$\rhd\varphi$	stands for	$\varphi \vee (\mathit{true}; \varphi)$
$\Diamond\varphi$	stands for	$(\lhd\varphi) \vee (\rhd\varphi) \vee (\mathit{true}; \varphi; \mathit{true})$

[3] The requirement that f_x is continuous from the right, guarantees that $\overleftarrow{x} = f_x(a)$.

Thus we can express that all subphases of a phase satisfy φ as $\Box\,\varphi$, where:

$$\Box\,\varphi \quad \text{stands for} \quad \neg\Diamond\neg\varphi$$

We also introduce the abbreviations:

inf	stands for	$\neg\mathit{fin}$
$\Diamond_f\,\varphi$	stands for	$\Diamond(\mathit{fin}\wedge\varphi)$
$\Box_f\,\varphi$	stands for	$\Box(\mathit{fin}\rightarrow\varphi)$
$\varphi\Rightarrow_f\psi$	stands for	$\Box_f(\varphi\rightarrow\psi)$

The formulas $\Diamond_f\,\varphi$ and $\Box_f\,\varphi$ can be viewed as finitary versions of $\Diamond\,\varphi$ and $\Box\,\varphi$ which restrict our attention to finite intervals only.

A phase $\langle I, f\rangle$ is called *continuous* if for all $v\in V$, f_v is continuous at all internal points of I. The continuity of all variables can be specified by the formula

$$\mathit{continuous}:\quad \neg\exists U.\Big(\overleftarrow{U}=\overrightarrow{U}\ \wedge\ (\overleftarrow{U}=\overrightarrow{V});(\overleftarrow{V}\neq\overrightarrow{U})\Big)$$

where U and V are tuples of variables of the same length. This formula states that it is impossible to break the phase into two adjacent subphases such that the left limit of the state variables at the left subphase differs from the right limit of the state variables at the right subphase.

From now on, we will use $\dot{x}$ as an abbreviation for $\overleftarrow{\dot{x}}$.

Example

Before presenting our framework for specifying hybrid systems, we introduce a variant of the gas burner example of [CHR91] as motivation.

Suppose an engineer wishes to design a controller for a gas burner that has two switch settings, ($\mathtt{switch}\in\{\text{Off, On}\}$), representing Off and On, respectively. The environment expresses its desire to change the switch's setting through a request variable, $\mathtt{R}$, that also has two possible values, ($\mathtt{R}\in\{\text{Off, On}\}$). Unfortunately, when the switch is on, there is a possibility, due to various system failures, that some of the gas leaks. In this hazardous situation, gas leaks at a rate not greater than 1 unit/sec. Moreover, the controller has no way of determining the rate that gas is actually leaking when the switch is on. The only guarantee that the controller has is that no gas is leaking when the switch is in the off position.

In the competitive world of gas burner design, the engineer must meet the following safety requirement:

- In any subinterval, if the duration of the subinterval is at least 60 seconds, then the cumulative leak amount within the subinterval is less than one-sixth of the subinterval duration. The purpose of this requirement is to prevent an excessive amount of gas from leaking into the environment and causing a safety hazard. Letting $\dot{L}$ represent the rate at which gas leaks from the system, and x represent the system's global clock, we can express the above property as follows[4]:

$$\overrightarrow{x}-\overleftarrow{x}\geq 60 \quad\Rightarrow_f\quad 6(\overrightarrow{L}-\overleftarrow{L})\leq\overrightarrow{x}-\overleftarrow{x}$$

Connection with Linear Temporal Logic

Our desire to reason about point-based properties in HTL, leads to the obvious question; namely, when does a temporal formula φ have the "same semantics" as in HTL? The following proposition states that HTL subsumes linear-time temporal logic without nested temporal operators in a natural way.

Proposition 1 *For any state formula φ and phase $P=\langle I, f\rangle$:*

1. *$P\models\Diamond\,\varphi$ iff $\exists t\in I$ such that φ holds at t.*

[4]We have dropped the units in the equation, but if $\dot{L}$ were measured in lbs/sec, then the constant 6 in the equation would really be 6sec/lbs, otherwise the units for $6(\overrightarrow{L}-\overleftarrow{L})$ and $\overrightarrow{x}-\overleftarrow{x}$ would be different.

2. $P \models \Box\, \varphi$ *iff* $\forall t \in I$ φ *holds at* t.

The proof of this proposition follows in a straightforward manner from the definitions of the derived HTL operators $\Box$ and $\Diamond$.

The following proposition, stated without proof, allows us to use first order tautologies as valid formulas of hybrid temporal logic:

Proposition 2 *For any state formula* φ*, if* φ *is a tautology of first order logic then* $\Box\, \varphi$ *is valid.*

3 Concrete Phase Transition Systems

Following [HMP93], [MMP92], and [NSY92], we model hybrid systems as transition systems. Just as discrete transitions can be represented as binary relations on states, hybrid transitions can be represented as binary relations on phases. Phases are characterized by phase invariants, which are presented as assertions (first-order formulas) $\rho_\phi(V, \dot{V})$ in the two variable tuples V and $\dot{V}$, intended to hold at all intermediate points $t \in [a, b)$ of the phase.

For a given phase invariant ϕ, a phase $P = \langle I, f \rangle$ over V is said to be a *ϕ-phase* if $P \models$ *continuous* $\wedge$ $\Box(\rho_\phi(V, \dot{V}))$.

For example the phase invariant ϕ presented as:

$$\rho_\phi(V, \dot{V}):\ 3 \le x < 6 \ \ \wedge\ \ \dot{x} = 1$$

characterizes all phases in which x steadily increases at a rate of 1 and always remains within the interval $[3, 6)$.

A *Concrete Phase Transition System* (CPTS) $\mathcal{S} = (V, \Phi, \Theta, \mathcal{T})$ consists of four components:

1. A finite set V of *state variables*.
2. A finite set Φ of *phase invariants* over V. Each phase invariant $\phi \in \Phi$ is presented by an assertion of the form $\rho_\phi(V, \dot{V})$, referring to the state variables and their derivatives.
3. An initial condition, Θ, which is a state formula over V that specifies the initial value of the variables at the left end of the first phase in computations.
4. A set $\mathcal{T}$ of *transitions*. Each transition $\tau \in \mathcal{T}$ is associated with an assertion $\rho_\tau(V, V')$, relating values at the right-end limit state of a phase to the values at the left-end of a successor phase.

A *phase sequence* is a finite or infinite sequence of adjacent phases. For a phase sequence $\overline{P} = P_0, P_1, \ldots$, we denote by $\overline{P}^*$ the single phase obtained by the concatenation $P_0 {}^\frown P_1 {}^\frown \cdots$. An HTL-formula can be interpreted over a phase sequence $\overline{P}$ by interpreting it over the single phase $\overline{P}^*$.

Two phase sequences $\overline{P}_1$ and $\overline{P}_2$ are *equivalent* if $\overline{P}_1^* = \overline{P}_2^*$. It follows that all equivalence classes of state sequences are *closed under stuttering*: if a phase P_i of the phase sequence $\overline{P}$ is split into two phases P' and P'' that partition P_i, the resulting phase sequence

$$P_0, \ldots P_{i-1}, P', P'', P_{i+1}, \ldots P_n$$

is equivalent to $\overline{P}$. Closure under stuttering allows for undersampling and oversampling. That is, the truth value of a formula over a phase does not change by refinement or fusion of some of its subphases.

Let $\overline{P} = P_0, P_1, P_2, \ldots$ be an infinite phase sequence with $P_i = \langle [a_i, a_{i+1}), f_i \rangle$ for all $i \ge 0$. The infinite phase sequence $\overline{P}$ *diverges* if a_i grows beyond any bound as i increases. A finite phase sequence $\overline{P} = P_0, \ldots, P_n$, with $P_i = \langle [a_i, a_{i+1}), f_i \rangle$ for all $0 \le i \le n$, *diverges* if $a_{n+1} = \infty$.

A phase sequence is a *computation* of the CPTS $\mathcal{S}$ if it is equivalent to a phase sequence $\overline{P} = P_0, P_1, \ldots, P_n, \ldots$ that satisfies the following conditions:[5]

Initiality If $P_0 = [a, b)$ then Θ holds at a.

[5] $\overline{P}$ may be finite or infinite. If it is infinite, then $|\overline{P}| = \infty$.

Continuous activities For all $0 \leq i < |\overline{P}|$, there is a phase invariant $\rho_\phi \in \Phi$ such that P_i is a ϕ-phase.

Discrete transitions For all $0 \leq i < |\overline{P}| - 1$, there is a transition $\tau \in \mathcal{T}$ such that $\rho_\tau(\overrightarrow{P_i}[V], \overleftarrow{P_{i+1}}[V])$ holds.

Divergence $\overline{P}$ is divergent.

A finite sequence of finite phases $\overline{P} = P_0, P_1, \ldots, P_n$ is called a *run fragment* of $\mathcal{S}$ if it satisfies the first three requirements of a computation but is not required to be divergent. In fact, such a sequence cannot be divergent. The system $\mathcal{S}$ is called a *non-Zeno* CPTS if every run fragment of $\mathcal{S}$ can be extended to a computation of $\mathcal{S}$. From now on we restrict our attention to non-Zeno CPTS's.

The CPTS $\mathcal{S}$ *satisfies* a hybrid temporal formula φ, written $\mathcal{S} \models \varphi$, if all computations of $\mathcal{S}$ satisfy φ.

4 Hybrid Automata

Many of the standard automata and diagram-based methods for presenting hybrid systems have a natural representation as CPTSs. In this paper, we use hybrid automata to specify CPTSs.

A hybrid automaton is a directed labeled graph $D = (V_D, L, E, E_\theta, \Omega, \mu, \kappa)$ consisting of the following:

- A finite set V_D of *data variables.*
- A finite set L of locations where each location $\ell \in L$ is labeled by
  - a finite set $\Omega(\ell)$ of differential equations over the variables V_D
  - a *stay condition* $\mu(\ell)$ which specifies the conditions under which the system can stay in location ℓ.
- A finite set E of *edges* between the locations in L. Each edge is labeled by a guarded command $\kappa(e) : \gamma \rightarrow \alpha$, where γ is a state formula over the variables in V_D (the *guard* of e) and α is a conjunction of the form $u_1 := e_1 \wedge \cdots \wedge u_m := e_m$, where $\{u_1, \ldots, u_m\}$ is a subset of V_D and $e_1, \ldots, e_m$ are expressions over V_D.
- An *entry edge*, E_θ, that has no originating location, but an entry location $\ell_i \in L$. E_θ is labeled by a formula $\kappa(E_\theta)$ of the form $v_1 = c_1 \wedge \cdots \wedge v_n = c_n$, which specifies initial values for all the data variables $\{v_1, \ldots, v_n\} = V_D$.

A solution to the gas burner problem introduced earlier is given in Figure 1.

The system GAS has two environment variables: $\dot{L}$, which represents the rate at which gas leaks from the system, and which varies depending on the switch's setting; and `R`, which represents the environment's wish to change the switch's setting. We also have the control variables `switch`, x, y, and T, where:

- `switch` represents the setting of the gas burner switch.
- x represents the system's global clock and advances at the rate of 1 at all times.
- y represents a node's local clock.
- T represents the cumulative time spent in the leaking node ℓ_2 since the beginning of the computation or the most recent period in which `switch` has been continuously off for at least 100 time units.

In the figure, $\neg$Off = On and $\neg$On = Off. The transition from ℓ_1 to itself represents the environment's changing of the request variable. Similarly the transition from ℓ_0 to ℓ_2 represents the environment's changing of the request variable immediately followed by the system's response which, in our formalism, is represented as a single transition. As stated earlier, we wish to prove the following safety property about system GAS:

$$\overrightarrow{x} - \overleftarrow{x} \geq 60 \quad \Rightarrow_f \quad 6(\overrightarrow{L} - \overleftarrow{L}) \leq \overrightarrow{x} - \overleftarrow{x}\,.$$

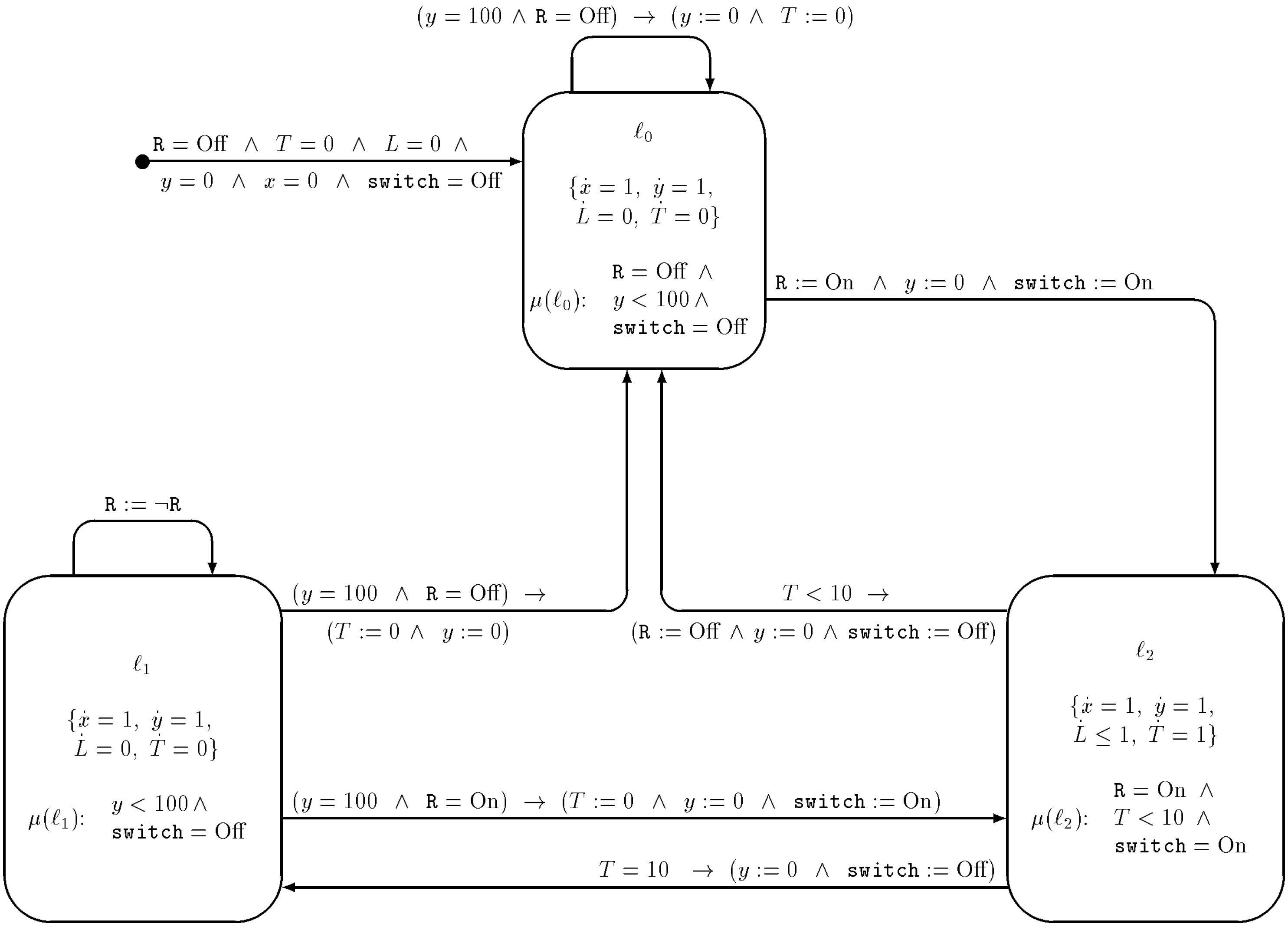

Figure 1: System GAS—Three state gas burner

$$\mathcal{S}_{\text{GAS}} \;=\; \big(V,\ \Phi,\ \Theta,\ \mathcal{T}\big), \text{ where:}$$

$$
\begin{array}{rl}
V = & \{\mathtt{R},\ L,\ T,\ \pi,\ x,\ y,\ \mathtt{switch}\} \\
\Phi = & \{\phi_{\ell_0}, \phi_{\ell_1}, \phi_{\ell_2}\} \\
\Theta : & \mathtt{R} = \text{Off} \ \wedge\ T = 0 \ \wedge\ L = 0 \ \wedge\ y = 0 \ \wedge\ \mathtt{switch} = \text{Off} \ \wedge\ \pi = \ell_0 \ \wedge\ x = 0 \\
\mathcal{T} = & \{\tau_{\langle \ell_0,\ell_0\rangle}, \tau_{\langle \ell_0,\ell_2\rangle}, \tau_{\langle \ell_1,\ell_0\rangle}, \tau_{\langle \ell_1,\ell_1\rangle}, \tau_{\langle \ell_1,\ell_2\rangle}, \tau_{\langle \ell_2,\ell_0\rangle}, \tau_{\langle \ell_2,\ell_1\rangle}\} \\
 & \\
\rho_{\ell_0} : & \dot{x} = 1 \ \wedge\ \dot{y} = 1 \ \wedge\ \dot{L} = 0 \ \wedge\ \dot{T} = 0 \\
 & \wedge\ y < 100 \ \wedge\ \mathtt{R} = \text{Off} \ \wedge\ \pi = \ell_0 \ \wedge\ \mathtt{switch} = \text{Off} \\
\rho_{\ell_1} : & \dot{x} = 1 \ \wedge\ \dot{y} = 1 \ \wedge\ \dot{L} = 0 \ \wedge\ \dot{T} = 0 \\
 & \wedge\ y < 100 \ \wedge\ \pi = \ell_1 \ \wedge\ \mathtt{switch} = \text{On} \\
\rho_{\ell_2} : & \dot{x} = 1 \ \wedge\ \dot{y} = 1 \ \wedge\ \dot{L} \leq 1 \ \wedge\ \dot{T} = 1 \\
 & \wedge\ \mathtt{R} = \text{On} \ \wedge\ T < 10 \ \wedge\ \pi = \ell_2 \ \wedge\ \mathtt{switch} = \text{Off} \\
\rho_{\langle \ell_0,\ell_0\rangle} : & y = 100 \ \wedge\ \mathtt{R} = \text{Off} \ \wedge\ \pi = \ell_0 \ \wedge\ \mathtt{R}' = \mathtt{R} \ \wedge\ L' = L \\
 & \wedge\ T' = 0 \ \wedge\ x' = x \ \wedge\ y' = 0 \ \wedge\ \mathtt{switch}' = \text{Off} \wedge\ \pi' = \ell_0 \\
\rho_{\langle \ell_0,\ell_2\rangle} : & \pi = \ell_0 \ \wedge\ \mathtt{R}' = \text{On} \ \wedge\ L' = L \\
 & \wedge\ T' = T \ \wedge\ x' = x \ \wedge\ y' = 0 \ \wedge\ \mathtt{switch}' = \text{On} \ \wedge\ \pi' = \ell_2 \\
\rho_{\langle \ell_1,\ell_0\rangle} : & \mathtt{R} = \text{Off} \ \wedge\ y = 100 \ \wedge\ \pi = \ell_1 \ \wedge\ \mathtt{R}' = \mathtt{R} \ \wedge\ L' = L \\
 & \wedge\ T' = 0 \ \wedge\ x' = x \ \wedge\ y' = 0 \ \wedge\ \mathtt{switch}' = \text{Off} \ \wedge\ \pi' = \ell_0 \\
\rho_{\langle \ell_1,\ell_1\rangle} : & \pi = \ell_1 \ \wedge\ \mathtt{R}' = \neg\mathtt{R} \ \wedge\ L' = L \\
 & \wedge\ T' = T \ \wedge\ x' = x \ \wedge\ y' = 0 \ \wedge\ \mathtt{switch}' = \mathtt{switch} \ \wedge\ \pi' = \ell_1 \\
\rho_{\langle \ell_1,\ell_2\rangle} : & \mathtt{R} = \text{On} \ \wedge\ y = 100 \ \wedge\ \pi = \ell_1 \ \wedge\ \mathtt{R}' = \mathtt{R} \ \wedge\ L' = L \\
 & \wedge\ T' = 0 \ \wedge\ x' = x \ \wedge\ y' = 0 \ \wedge\ \mathtt{switch}' = \text{On} \ \wedge\ \pi' = \ell_2 \\
\rho_{\langle \ell_2,\ell_0\rangle} : & T < 10 \ \wedge\ \pi = \ell_2 \ \wedge\ \mathtt{R}' = \text{Off} \ \wedge\ L' = L \ \wedge\ T' = T \\
 & \wedge\ x' = x \ \wedge\ y' = 0 \ \wedge\ \mathtt{switch}' = \text{Off} \ \wedge\ \pi' = \ell_0 \\
\rho_{\langle \ell_2,\ell_1\rangle} : & T = 10 \ \wedge\ \pi = \ell_2 \ \wedge\ \mathtt{R}' = \mathtt{R} \ \wedge\ L' = L \ \wedge\ T' = T \\
 & \wedge\ x' = x \ \wedge\ y' = 0 \ \wedge\ \mathtt{switch}' = \text{Off} \ \wedge\ \pi' = \ell_1
\end{array}
$$

Figure 2: The concrete phase transition system associated with system GAS

$V: \{\pi\} \cup V_D$
$\Theta: \kappa(E_\theta) \;\wedge\; \pi = \ell_i$ where ℓ_i is the entry location for E_θ
$\Phi: \{\phi_{\ell_i} \mid \ell_i \in L\}$ where, for each $\ell_i \in L$
$\quad \rho_{\ell_i}: \;\; \mu(\ell_i) \;\wedge\; \pi = \ell_i \;\wedge\; \left(\bigwedge_{\psi\in\Omega(\ell_i)} \psi\right)$
$\mathcal{T}: \{\tau_{\langle \ell_i,\ell_j\rangle} \mid \langle \ell_i,\ell_j\rangle \in E\}$ where, for each $e = \langle \ell_i,\ell_j\rangle \in E$ such that $\kappa(e): \gamma \;\rightarrow\; \alpha$
$\quad$ where α is of the form $\bigwedge_{i=1}^{m} u_i := e_i$,
$\quad \rho_{\langle \ell_i,\ell_j\rangle}: \;\; \gamma \;\wedge\; \left(\bigwedge_{i=1}^{m} u_i' = e_i\right) \;\wedge\; \pi = \ell_i \;\wedge\; \pi' = \ell_j \;\wedge\; \left(\bigwedge_{v\in(V-\mathtt{var}(\alpha))} v' = v\right)$

Figure 3: The concrete phase transition system $\mathcal{S} = (V, \Phi, \Theta, \mathcal{T})$ corresponding to the hybrid automaton, $D = (V_D, L, E, E_\theta, \Omega, \mu, \kappa)$

P-INV	PI1.	$\Theta \rightarrow \varphi(V)$	
	PI2.	$\varphi(V) \rightarrow \psi(V)$	
	PI3.	$\rho_\tau(V, V') \;\wedge\; \chi(V) \rightarrow \varphi(V')$	$\forall \tau \in \mathcal{T}$
	PI4.	$\rho_\phi(V, \dot{V}) \;\wedge\; \chi(V) \rightarrow \varphi(V)$	$\forall \phi \in \Phi$
	PI5.	*continuous* $\wedge \; \Box\, \rho_\phi(V, \dot{V}) \;\wedge\; \varphi(V) \;\Rightarrow_f\; \chi(\overrightarrow{V})$	$\forall \phi \in \Phi$
		$\Box\, \psi(V)$	

Figure 4: Rule P-INV—Invariance of point-based state formulas

The concrete phase transition system corresponding to the above system is given in Figure 2.

It is not difficult to construct a CPTS S, corresponding to a given hybrid automaton, and in Figure 3 we present this construction. In the figure, $\mathtt{var}(\alpha)$ is the set of variables that get assigned in α (i.e., $\{u_i | 1 \leq i \leq m\}$).

From now on, we restrict our attention to *non-Zeno hybrid automata*, i.e., hybrid automata whose corresponding CPTS's are non-Zeno.

5 Proof Rules

We first present the proof rules for point-based properties and then present a proof rule for proving interval-based properties.

Point-based

To prove point-based invariance formulas of the form $\Box\, \psi$ where ψ is a state formula, we use the rule P-INV given in Figure 4. We use the notation $\psi(V)$ to emphasize that ψ is a formula over the variables V, and $\psi(V')$ to indicate the result of replacing all variables in $\psi(V)$ by their primed versions.

The rule uses two auxiliary assertions φ and χ. Assertion φ is intended to be a stronger version of ψ that is inductive, while assertion χ is a weaker version of φ which holds not only at states within phases but also at the left limits of such states.

Premise PI1 states that φ, where φ is a state formula, is initially true. Premise PI3 states that if χ holds at some state, which could be a left limit of states in the computation, and a discrete transition τ is taken, then φ holds in the new state (since, for transitions, V' represents the values of the variables in the new state). Premise PI4 states that at internal points of a phase, $\chi(V)$ implies $\varphi(V)$.

L-INV	LI1.	$\Theta \rightarrow \varphi(V)$	
	LI2.	$\chi(V) \rightarrow \psi(V)$	
	LI3.	$\rho_\tau(V, V') \wedge \chi(V) \rightarrow \varphi(V')$	$\forall \tau \in \mathcal{T}$
	LI4.	$\rho_\phi(V, \dot{V}) \wedge \chi(V) \rightarrow \varphi(V)$	$\forall \phi \in \Phi$
	LI5.	*continuous* $\wedge \Box \rho_\phi(V, \dot{V}) \wedge \varphi(V) \Rightarrow_f \chi(\overrightarrow{V})$	$\forall \phi \in \Phi$
		$\Box \psi(\overrightarrow{V})$	

Figure 5: Rule L-INV—Invariance of left-limit state formulas

I-INV	II1.	$\varphi(V, V') \rightarrow \psi(V, V')$	
	II2.	*continuous* $\wedge \Box \rho_\phi(V, \dot{V}) \Rightarrow_f \varphi(\overleftarrow{V}, \overrightarrow{V})$	$\forall \phi \in \Phi$
	II3.	$\varphi(V_1, V_2) \wedge \rho_\tau(V_2, V) \wedge$ *continuous* $\wedge \Box \rho_\phi(V, \dot{V}) \Rightarrow_f \varphi(V_1, \overrightarrow{V})$	$\forall \tau \in \mathcal{T}$ $\forall \phi \in \Phi$
		$\Box_f \psi(\overleftarrow{V}, \overrightarrow{V})$	

Figure 6: Rule I-INV—Invariance of interval formulas

Premise PI5 is the only temporal premise among the five. It requires that if φ holds at the left end of a ϕ-phase, then χ holds at the state which is the limit from the left of the phase[6].

Premises PI1, PI3, PI4, and PI5 insure that for all time points t, φ holds. By premise PI2, ψ also holds at all time points, which can be written as $\Box \psi$.

For example, using the above rule we can prove the following point-based invariances for system GAS.

- $at\_\ell_0 \rightarrow (0 \leq y < 100 \wedge 0 \leq T < 10 \wedge \mathtt{R} = \text{Off} \wedge \mathtt{switch} = \text{Off})$
- $at\_\ell_1 \rightarrow (0 \leq y < 100 \wedge T = 10 \wedge \mathtt{switch} = \text{Off})$
- $at\_\ell_2 \rightarrow (0 \leq y < 10 \wedge 0 \leq T < 10 \wedge \mathtt{R} = \text{On} \wedge \mathtt{switch} = \text{On})$

We prove the first of these properties in the appendix, the others are proved in a similar fashion.

A similar rule L-INV can be used to prove properties of the form $\Box \psi(\overrightarrow{V})$, where $\psi(\overrightarrow{V})$ is an assertion in $\overrightarrow{V}$.

Interval-based

To prove interval-based invariance formulas of the form $\Box \varphi(\overleftarrow{V}, \overrightarrow{V})$ where φ is a formula whose variables appear as left or right limits, we use rule I-INV given in Figure 6.

Premise II1 expresses the monotonicity requirements of the rule. The temporal premise II2 states that any ϕ-phase satisfies φ. Premise II3 states that if φ is true over a phase P_1 and we take a discrete transition τ to another phase P_2 on which φ holds, then φ will be true over the phase $P_1 \frown P_2$. Premises II3 and II2 imply that any subphase satisfies φ, and by monotonicity, this guarantees $\Box_f \psi(\overleftarrow{V}, \overrightarrow{V})$.

In addition we may add any previously derived point invariants $p(V)$ to the left of any premise, and any previously derived invariants $q(\overrightarrow{V})$ or $r(\overleftarrow{V}, \overrightarrow{V})$ to the left of any temporal premise.

Before presenting example interval invariants, we introduce the following notation. For a variable $x \in V$,

[6] To prove temporal entailments such as PI5, we use some known facts based on elementary calculus such as *continuous* $\wedge \Box(\dot{x} = 0) \Rightarrow_f \overleftarrow{x} = \overrightarrow{x}$.

$$
\begin{array}{lll}
\text{I-MON} & \text{IM1.} & \Box_f\, \varphi_1(\overleftarrow{V}, \overrightarrow{V}) \\
 & \text{IM2.} & \Box_f\, \varphi_2(\overleftarrow{V}, \overrightarrow{V}) \\
 & \text{IM3.} & \varphi_1(\overleftarrow{V}, \overrightarrow{V}) \wedge \varphi_2(\overleftarrow{V}, \overrightarrow{V}) \Rightarrow_f \psi(\overleftarrow{V}, \overrightarrow{V}) \\
\hline
 & & \Box_f\, \psi(\overrightarrow{V}, \overleftarrow{V})
\end{array}
$$

Figure 7: Rule I-MON—Monotonicity of interval invariance formulas

Δx	stands for	$\overrightarrow{x} - \overleftarrow{x}$
$\Delta_1^2 x$	stands for	$x_2 - x_1$
$\Delta_1 x$	stands for	$\overrightarrow{x} - x_1$

For example using the above rule we can prove the following interval-based invariances for system GAS.

- $\overrightarrow{at}\_\ell_{0,1} \Rightarrow_f \Big((\Delta x \leq \overrightarrow{y} \wedge \Delta L = 0) \;\vee\; (\Delta x > \overrightarrow{y} \wedge \Delta L < \Delta x - \overrightarrow{y})\Big)$
- $\Box_f \left[(\psi_1 \;\vee \psi_2 \;\vee \psi_3) \;\wedge\; \psi_4 \right]$ where
  - ψ_1: $\Delta L \leq \Delta T$
  - ψ_2: $\Delta L \leq \overrightarrow{T} \wedge \Delta x \leq \overrightarrow{T} + 100$
  - ψ_3: $\Delta L \leq \Delta x - 100 \wedge \Delta x > \overrightarrow{T} + 100 \wedge 6(\Delta L) \leq \Delta x$
  - ψ_4: $\Big(\overrightarrow{at}\_\ell_{0,1} \wedge \Delta x \geq 110\Big) \;\rightarrow\; \Delta x \geq 50 + \overrightarrow{T} + 6(\Delta L - \overrightarrow{T})$
- $\Delta x \geq 60 \Rightarrow_f 6(\Delta L) \leq \Delta x$

The second property is used to prove the third property using rule I-MON presented in Figure 7.

6 Soundness of Proof Rules

We now prove the soundness of the rules.

Proposition 3 *Rule* P-INV *is sound.*

Proof of Soundness of P-INV**:**

Let $\mathcal{S} = (V, \Phi, \Theta, \mathcal{T})$ be an arbitrary CPTS.
Suppose φ, χ, ψ are state formulas such that the premises of rule P-INV hold.
We will show that for any computation $\overline{P}$ of $\mathcal{S}$, that $\overline{P}^* \models \Box(\psi)$.
Let $\overline{P}_1$ be an arbitrary computation of $\mathcal{S}$.
As $\overline{P}_1$ is a computation of $\mathcal{S}$, it is equivalent to a phase sequence of the form $\overline{P}_2 = P_0, P_1, \ldots$ where:

(1) For each $0 \leq i < |\overline{P}|$, $P_i = \langle [a_i, a_{i+1}), f_i \rangle$

(2) Θ holds at a_0.

(3) For all $0 \leq i < |\overline{P}|$, there is a phase invariant $\rho_\phi \in \Phi$ such that P_i is a ϕ-phase.

(4) For all $0 \leq i < |\overline{P}| - 1$, there is a transition $\tau \in \mathcal{T}$ such that $\rho_\tau(\overrightarrow{P_i}[V], \overleftarrow{P_{i+1}}[V])$ holds.

(5) $\overline{P}$ is divergent.

We proceed to prove that φ and ψ hold at all $t \in [a_0, \infty)$. The proof is by induction on j, $0 \leq j < |\overline{P}|$, showing that φ and ψ hold at all $t \in [a_j, a_{j+1})$.

Assume that we have already shown that φ and ψ hold at all $t \in [a_k, a_{k+1})$, for every k, $0 \leq k < j$. We will show that φ and ψ hold at all $t \in [a_j, a_{j+1})$.

Case: $t = a_j$ and $j = 0$

By requirement (2) above, Θ holds at a_0. As premise PI1 holds, φ holds at a_0. As premise PI2 holds, ψ holds at a_0.

Case: $t = a_j$ and $j \neq 0$

By requirement (4) above, there is a transition $\tau \in \mathcal{T}$ such that $\rho_\tau(\overrightarrow{P_{j-1}}[V], \overleftarrow{P_j}[V])$ holds. Fix such a τ. By requirement (3) above, there is a phase invariant $\rho_\phi \in \Phi$ such that P_{j-1} is a ϕ-phase. Fix such a phase invariant. Thus $P_{j-1} \models \mathit{continuous} \wedge \Box\, \rho_\phi(V, \dot{V})$. By the induction hypothesis, φ and ψ hold for all $t \in [a_{j-1}, a_j)$. Thus $P_{j-1} \models \varphi(V)$. So by premise PI5, $P_{j-1} \models \chi(\overrightarrow{V})$. As $\rho_\tau(\overrightarrow{P_{j-1}}[V], \overleftarrow{P_j}[V])$ holds, by premise PI3, $P_j \models \varphi(\overleftarrow{V})$. That is, φ holds at $a_j = t$. By premise PI2, ψ holds at t.

Case: $t \in (a_j, a_{j+1})$

By requirement (3) above, there is a phase invariant $\rho_\phi \in \Phi$ such that P_j is a ϕ-phase. Fix such a phase invariant. Consider the subphase $\widehat{P}_j = \langle [a_j, t), \widehat{f} \rangle$, where $\widehat{f}$ is the restriction of f to $[a_j, t)$. Obviously, $\widehat{P}_j$ is also a ϕ-phase. In particular, $\widehat{P}_j \models \mathit{continuous} \wedge \Box\, \rho_\phi(V, \dot{V})$. By the previous two cases, φ holds at a_j. As φ is a state formula, we have $\widehat{P}_j \models \varphi(V)$. So by premise PI5, $\widehat{P}_j \models \chi(\overrightarrow{V})$. That is, $\chi(\overrightarrow{V})$ holds at t. As P_j is continuous and t is an internal point in $[a_j, a_{j+1})$, we conclude that $\chi(V)$ holds at t. Since t is internal to $[a_j, a_{j+1})$, ρ_ϕ holds at t. By premise PI4, φ holds at t. So by premise PI2, ψ holds at t.

So by induction, φ and ψ hold for all $t \in [a_0, \infty)$. Thus $\Box\, \psi(V)$ holds by theorem 1.

Proposition 4 *Rule* I-INV *is sound.*

Proof of Soundness of I-INV**:**

Let $\mathcal{S} = (V, \Phi, \Theta, \mathcal{T})$ be an arbitrary CPTS.
Suppose $\varphi(V, V'), \psi(V, V')$ are state formulas, such that the premises of rule I-INV hold.
We will show that for any computation $\overline{P}$ of $\mathcal{S}$, that $\overline{P}^* \models \Box\, \psi(\overleftarrow{V}, \overrightarrow{V})$.
Let $\overline{P}_1$ be an arbitrary computation of $\mathcal{S}$ and P be an arbitrary finite subphase of $\overline{P}_1^*$. As P is a finite subphase of $\overline{P}_1^*$, it must be equivalent to a sequence of adjacent phases $P_1, \ldots, P_n$ $(n \geq 1)$ such that

(1) For each $i \in [1..n]$, there is a phase invariant $\rho_\phi \in \Phi$ such that P_i is a ϕ-phase.

(2) For each $i \in [1..n-1]$, there is a transition $\tau \in \mathcal{T}$ such that $\rho_\tau(\overrightarrow{P_i}[V], \overleftarrow{P_{i+1}}[V])$ holds.

We proceed by induction on $t \in [1..n]$ to show that $\varphi(\overleftarrow{V}, \overrightarrow{V})$ holds over the phase $P_{1..t} = P_1 {}^\frown P_2 {}^\frown \cdots {}^\frown P_t$.

Case: Base Case $t = 1$

By requirement (1) above, there is a phase invariant $\rho_\phi \in \Phi$ such that P_1 is a ϕ-phase. That is, $P_1 \models \mathit{continuous} \wedge \Box\, \rho_\phi(V, \dot{V})$. By premise II2, $P_1 \models \varphi(\overleftarrow{V}, \overrightarrow{V})$, and since $P_{1..1} = P_1$, the induction claim holds for $t = 1$.

Case: Induction Case — from t to $t + 1 \leq n$

Let phases $P_{1..t}$ and P_{t+1} be given by $\langle [a, b), g_t \rangle$ and $\langle [b, c), g_{t+1} \rangle$, respectively. Let U_1, U_2, and U_3 denote the values of $\overleftarrow{P_{1..t}}[V]$, $\overrightarrow{P_{1..t}}[V] = \overrightarrow{P_t}[V]$, and $\overleftarrow{P_{t+1}}[V]$, respectively.
By requirement (2) above, there is a transition $\tau \in \mathcal{T}$ such that $\rho_\tau(\overrightarrow{P_t}[V], \overleftarrow{P_{t+1}}[V])$ holds. By requirement (1) above, there is a phase invariant $\rho_\phi \in \Phi$ such that P_{t+1} is a ϕ-phase. Thus $P_{t+1} \models \mathit{continuous} \wedge \Box\, \rho_\phi(V, \dot{V})$. By the induction hypothesis, $P_{1..t} \models \varphi(\overleftarrow{V}, \overrightarrow{V})$, which implies that $\varphi(U_1, U_2) = \mathit{true}$ (that is, $\varphi(V_1, V_2)$ evaluates to *true* when we interpret V_1 as U_1 and V_2 as U_2. In a similar way, P_{t+1} being a τ-successor of P_t implies that $\rho_\tau(U_2, U_3) = \mathit{true}$.

Consider now the augmented phase $\widehat{P}_{t+1}$: $\langle [b,c), \widehat{g}_{t+1}\rangle$ where $\widehat{g}_{t+1}$ agrees with g_{t+1} on the values of V, that is, $\widehat{g}_{t+1}[V](r) = g_{t+1}[V](r)$ for each $r \in [b,c)$ and, in addition, $\widehat{g}_{t+1}$ interprets the additional variables V_1 and V_2 as the *constant* values U_1 and U_2, respectively. It is not difficult to see that the conjunction $\varphi(V_1, V_2) \wedge \rho_\tau(V_2, V_3) \wedge \mathit{continuous} \wedge \Box\, \rho_\phi(V_3, \dot{V}_3)$ holds over the phase $\widehat{P}_{t+1}$.

So by premise II3, $\widehat{P}_{t+1} \models \varphi(V_1, \overrightarrow{V})$. Since $\widehat{P}_{t+1}[V_1] = U_1 = P_{1..t}[V] = P_{1..t+1}[V]$ and $\overrightarrow{\widehat{P}_{t+1}}[V] = \overrightarrow{P_{t+1}}[V] = \overrightarrow{P_{1..t+1}}[V]$, it follows that $P_{1..t+1} \models \varphi(\overleftarrow{V}, \overrightarrow{V})$.

By induction, we conclude that $P_{1..n} \models \varphi(\overleftarrow{V}, \overrightarrow{V})$ which, by premise II1, leads to $P_{1..n} \models \psi(\overleftarrow{V}, \overrightarrow{V})$. As P is equivalent to $P_{1..n}$, $P \models \psi(\overleftarrow{V}, \overrightarrow{V})$.

Since P was an arbitrary finite phase of the computation $\overline{P}_1$ we get that $\Box\, \psi(\overleftarrow{V}, \overrightarrow{V})$ is an invariant of $\mathcal{S}$.

7 Related Work

The interval temporal logic (ITL) of [Mos85] uses a discrete semantics involving finite intervals consisting of a finite number of states. This is justified, since ITL is a logic for hardware verification, where discretization is both natural and possible. The logic we propose here is intended to be used for verification of controllers governing hybrid systems, which by definition have continuous components.

Our approach differs from that of the duration calculus community ([CHR91], [CRH93], [RRH93]). The duration calculus approach requires that both specification properties and possible implementation strategies be expressed as duration calculus formulas. Verification is the process of proving that the implementation implies the specification, and is done using an axiom system for the duration calculus. In our approach, implementation strategies are expressed using hybrid automata. It is our belief that automata offer a more natural formalism for describing controllers and other hybrid systems.

The extended duration calculus (EDC) [CRH93], intended for verification of hybrid systems, allows one to specify values at the left and right endpoints of a phase, a feature that is not present in the original duration calculus of [CHR91]. For example in EDC, the safety requirement for the gas burner would be $\mathbf{e}.x - \mathbf{b}.x \;\rightarrow\; 6(\mathbf{e}.L - \mathbf{b}.L) \leq \mathbf{e}.x - \mathbf{b}.x$. A thorough explanation of the gas burner, along with its verification using the original duration calculus, can be found in [RRH93]. The coding of the duration operator $\int$ in HTL is similar to the coding of it in EDC, the latter of which can be found in [CRH93].

Acknowledgments

We would like to thank Nikolaj Bjørner, Yassine Lakhneche, Hugh McGuire, Henny Sipma, and the anonymous referees for their feedback and comments.

References

[ACHH93] R. Alur, C. Courcoubetis, T.A. Henzinger, and P-H. Ho. Hybrid Automata: An Algorithmic Approach to the Specification and Verification of Hybrid Systems. In R.L. Grossman, A. Nerode, A.P. .Ravn, and H. Rischel, editors, *Hybrid Systems*, Lecture Notes in Computer Science 736, pages 209–229. Springer-Verlag, 1993.

[CHR91] Z. Chaochen, C.A.R. Hoare, and A.P. Ravn. A calculus of durations. *Information Processing Letters*, 40:269–276, 1991.

[CRH93] Z. Chaochen, A.P. Ravn, and C.A.R. Hoare. An Extended Duration Calculus for Hybrid Real-Time Systems. In R.L. Grossman, A. Nerode, A.P. .Ravn, and H. Rischel, editors, *Hybrid Systems*, Lecture Notes in Computer Science 736, pages 36–59. Springer-Verlag, 1993.

[HKP82] D. Harel, D. Kozen, and R. Parikh. Process Logic: Expressiveness, Decidability, Completeness. *J. Comp. Sys. Sci.*, 25:144–170, 1982.

[HMP93] T.A. Henzinger, Z. Manna, and A. Pnueli. Towards Refining Temporal Specifications into Hybrid Systems. In R.L. Grossman, A. Nerode, A.P. .Ravn, and H. Rischel, editors, *Hybrid Systems*, Lecture Notes in Computer Science 736, pages 60–76. Springer-Verlag, 1993.

[MMP92] O. Maler, Z. Manna, and A. Pnueli. From timed to hybrid systems. In J.W. de Bakker, K. Huizing, W.-P. de Roever, and G. Rozenberg, editors, *Real Time: Theory in Practice*, Lecture Notes in Computer Science 600, pages 447–484. Springer-Verlag, 1992.

[Mos85] B. Moszkowski. A temporal logic for multi-level reasoning about hardware. *IEEE Computer*, 18(2):10–19, 1985.

[MP91] Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems: Specification*, Springer-Verlag, 1991.

[MP93] Z. Manna and A. Pnueli. Models for reactivity. *Acta Informatica*, 30:609–678, 1993.

[NSY92] X. Nicollin, J. Sifakis, and S. Yovine. From ATP to timed graphs and hybrid systems. In J.W. de Bakker, K. Huizing, W.-P. de Roever, and G. Rozenberg, editors, *Real Time: Theory in Practice*, Lecture Notes in Computer Science 600, pages 549–572. Springer-Verlag, 1992.

[RRH93] A.P. Ravn, H. Rischel, and K.M Hansen. Specifying and Verifying Requirements of Real-Time Systems. *IEEE Transactions on Software Engineering*, 19(1):41–55, 1993.

[Schn88] F.B. Schneider. Real-time, reliable systems project. *Proceedings of the ONR Kickoff Workshop for the Foundations of Real-time Computing Research Initiative*, pages 28–32, Office of Naval Research, 1988.

A Verification of Gas Burner

A.1 Proofs of Point-based Formulas

We are interested in proving:

- $T \geq 0$
- $at\_\ell_0 \;\rightarrow\; (0 \leq y < 100 \;\wedge\; 0 \leq T < 10 \;\wedge\; \mathtt{R} = \mathrm{Off} \;\wedge\; \mathtt{switch} = \mathrm{Off})$
- $at\_\ell_1 \;\rightarrow\; (0 \leq y < 100 \;\wedge\; T = 10 \;\wedge\; \mathtt{switch} = \mathrm{Off})$
- $at\_\ell_2 \;\rightarrow\; (0 \leq y < 10 \;\wedge\; 0 \leq T < 10 \;\wedge\; \mathtt{R} = \mathrm{On} \;\wedge\; \mathtt{switch} = \mathrm{On})$

We prove the second of these four formulas, the others are proved similarly.
Proof of $at\_\ell_0 \;\rightarrow\; (0 \leq y < 100 \;\wedge\; 0 \leq T < 10 \;\wedge\; \mathtt{R} = \mathrm{Off} \;\wedge\; \mathtt{switch} = \mathrm{Off})$**:**

We take:

$$\begin{aligned} \psi,\ \varphi: &\quad at\_\ell_0 \;\rightarrow\; (0 \leq y < 100 \;\wedge\; 0 \leq T < 10 \;\wedge\; \mathtt{R} = \mathrm{Off} \;\wedge\; \mathtt{switch} = \mathrm{Off}) \\ \chi: &\quad at\_\ell_0 \;\rightarrow\; (0 \leq y \leq 100 \;\wedge\; 0 \leq T < 10 \;\wedge\; \mathtt{R} = \mathrm{Off} \;\wedge\; \mathtt{switch} = \mathrm{Off}) \end{aligned}$$

PI1: $\Theta \;\rightarrow\; \varphi(V)$
$\left[\mathtt{R} = \mathrm{Off} \;\wedge\; T = 0 \;\wedge\; y = 0 \;\wedge\; \mathtt{switch} = \mathrm{Off} \;\wedge\; \pi = \ell_0 \;\wedge\; \ldots\right] \;\rightarrow$
$\left[at\_\ell_0 \;\rightarrow\; (0 \leq y < 100 \;\wedge\; 0 \leq T < 10 \;\wedge\; \mathtt{R} = \mathrm{Off} \;\wedge\; \mathtt{switch} = \mathrm{Off})\right]$
which clearly holds.

PI2: $\varphi(V) \;\rightarrow\; \psi(V)$
As $\varphi(V)$ and $\psi(V)$ are the same formulas, we get $\varphi(V) \;\rightarrow\; \psi(V)$.

PI3: $\rho_\tau(V, V') \wedge \chi(V) \rightarrow \varphi(V')$ for every $\tau \in \mathcal{T}$
We only need to consider transitions of the form $\rho_{\langle \ell_i, \ell_0 \rangle}$ for $i \in \{0, 1, 2\}$ since for all other transitions $\pi' \neq \ell_0$, making the antecedent of $\varphi(V')$ false. Thus we have three transitions, $\rho_{\langle \ell_0, \ell_0 \rangle}$, $\rho_{\langle \ell_1, \ell_0 \rangle}$, and $\rho_{\langle \ell_2, \ell_0 \rangle}$, to consider.

$\rho_{(\ell_0,\ell_0)}$:

$$\begin{bmatrix} \pi = \ell_0 \ \wedge \ \mathtt{R}' = \mathtt{R} \\ \wedge \ T' = 0 \ \wedge \ y' = 0 \wedge \ \pi' = \ell_0 \\ \wedge \ \mathtt{switch}' = \mathrm{Off} \ \wedge \ \ldots \end{bmatrix} \wedge \ [at\_\ell_0 \ \rightarrow \ (\mathtt{R} = \mathrm{Off} \ \wedge \ \ldots)]$$
$$\rightarrow \ \left[at'\_\ell_0 \ \rightarrow \ \begin{pmatrix} 0 \le y' < 100 \ \wedge \ 0 \le T' < 10 \\ \wedge \ \mathtt{R}' = \mathrm{Off} \ \wedge \ \mathtt{switch}' = \mathrm{Off} \end{pmatrix}\right]$$

$\rho_{(\ell_1,\ell_0)}$:

$$\begin{bmatrix} \mathtt{R}' = \mathrm{Off} \ \wedge \ T' = 0 \ \wedge \ y' = 0 \\ \wedge \ \mathtt{switch}' = \mathrm{Off} \ \wedge \ \pi' = \ell_0 \ \wedge \ \ldots \end{bmatrix} \wedge \ \chi(V)$$
$$\rightarrow \ \left[at'\_\ell_0 \ \rightarrow \ \begin{pmatrix} 0 \le y' < 100 \ \wedge \ 0 \le T' < 10 \\ \wedge \ \mathtt{R}' = \mathrm{Off} \ \wedge \ \mathtt{switch}' = \mathrm{Off} \end{pmatrix}\right]$$

$\rho_{(\ell_2,\ell_0)}$:

$$\begin{bmatrix} \mathtt{R}' = \mathrm{Off} \ \wedge \ T < 10 \ \wedge \ T' = T \ \wedge \ y' = 0 \\ \wedge \ \mathtt{switch}' = \mathrm{Off} \ \wedge \ \pi' = \ell_0 \ \wedge \ \ldots \end{bmatrix} \wedge \ \chi(V)$$
$$\rightarrow \ \left[at'\_\ell_0 \ \rightarrow \ \begin{pmatrix} 0 \le y' < 100 \ \wedge \ 0 \le T' < 10 \\ \wedge \ \mathtt{R}' = \mathrm{Off} \ \wedge \ \mathtt{switch}' = \mathrm{Off} \end{pmatrix}\right]$$

The first two formulas are valid formulas, while the third formula also requires the previously established invariant, $T \geq 0$.

PI4: $\rho_\phi(V, \dot{V}) \ \wedge \ \chi(V) \rightarrow \varphi(V)$ for every $\phi \in \Phi$

We only have to consider the phase relation, ρ_{ℓ_0}, since the other phase relations have $\pi \neq \ell_0$, making the antecedent false.

$$[y < 100 \ \wedge \ \ldots] \ \wedge \ \left[at\_\ell_0 \ \rightarrow \ \begin{pmatrix} 0 \le y \le 100 \ \wedge \ 0 \le T < 10 \\ \wedge \ \mathtt{R} = \mathrm{Off} \ \wedge \ \mathtt{switch} = \mathrm{Off} \end{pmatrix}\right]$$
$$\rightarrow \ \left[at\_\ell_0 \ \rightarrow \ \begin{pmatrix} 0 \le y < 100 \ \wedge \ 0 \le T < 10 \\ \wedge \ \mathtt{R} = \mathrm{Off} \ \wedge \ \mathtt{switch} = \mathrm{Off} \end{pmatrix}\right]$$

PI5: $\mathit{continuous} \wedge \Box \, \rho_\phi(V, \dot{V}) \ \wedge \ \varphi(V) \ \Rightarrow_f \ \chi(\overrightarrow{V})$ for every $\phi \in \Phi$

We only have to consider the phase relation, ρ_{ℓ_0}, since the other phase relations have $\overrightarrow{\pi} \neq \ell_0$, making the antecedent false.

$$\mathit{continuous} \ \wedge \Box \begin{bmatrix} \dot{y} = 1 \ \wedge \ \dot{T} = 0 \ \wedge \\ y < 100 \ \wedge \ \mathtt{R} = \mathrm{Off} \\ \wedge \ \pi = \ell_0 \ \wedge \\ \mathtt{switch} = \mathrm{Off} \ \wedge \ \ldots \end{bmatrix} \ \wedge \ \begin{bmatrix} at\_\ell_0 \ \rightarrow \\ \begin{pmatrix} 0 \le y < 100 \ \wedge \\ 0 \le T < 10 \ \wedge \ \ldots \end{pmatrix} \end{bmatrix}$$
$$\Rightarrow_f \ \left[\overrightarrow{at}\_\ell_0 \ \rightarrow \ \begin{pmatrix} 0 \le \overrightarrow{y} \le 100 \ \wedge \ 0 \le \overrightarrow{T} < 10 \\ \wedge \ \overrightarrow{\mathtt{R}} = \mathrm{Off} \ \wedge \ \overrightarrow{\mathtt{switch}} = \mathrm{Off} \end{pmatrix}\right]$$

So consider an arbitrary phase P. Suppose $P \models \mathit{continuous} \wedge \Box \, \rho_{\ell_0} \wedge \varphi(V)$. As $\mathit{continuous} \wedge \Box(\dot{T} = 0) \Rightarrow_f \overleftarrow{T} = \overrightarrow{T}$, $P \models \overleftarrow{T} = \overrightarrow{T}$, and as $0 \le T < 10$, $P \models 0 \le \overrightarrow{T} < 10$. As $0 \le y < 100 \ \wedge \ \Box(\dot{y} = 1)$, $P \models 0 \le \overrightarrow{y}$. As $\mathit{continuous} \ \wedge \ \Box(y < 100)$, $P \models \overrightarrow{y} \le 100$. As $\mathit{continuous} \ \wedge \ \Box(\mathtt{R} = \mathrm{Off})$, $P \models \overrightarrow{\mathtt{R}} = \mathrm{Off}$. As $\mathit{continuous} \ \wedge \ \Box(\mathtt{switch} = \mathrm{Off})$, $P \models \overrightarrow{\mathtt{switch}} = \mathrm{Off}$. Thus, $P \models \chi(\overrightarrow{V})$.

A.2 Proofs of Interval-based Formulas

We are interested in proving:

- $\overrightarrow{at}\_\ell_{0,1} \;\Rightarrow_f\; \Big((\Delta x \leq \overrightarrow{y} \wedge \Delta L = 0) \;\vee\; (\Delta x > \overrightarrow{y} \wedge \Delta L < \Delta x - \overrightarrow{y})\Big)$
- $\Box_f \left[(\psi_1 \;\vee \psi_2 \;\vee \psi_3) \;\wedge\; \psi_4 \right]$ where
  ψ_1: $\Delta L \leq \Delta T$
  ψ_2: $\Delta L \leq \overrightarrow{T} \wedge \Delta x \leq \overrightarrow{T} + 100$
  ψ_3: $\Delta L \leq \Delta x - 100 \wedge \Delta x > \overrightarrow{T} + 100 \wedge 6(\Delta L) \leq \Delta x$
  ψ_4: $\Big(\overrightarrow{at}\_\ell_{0,1} \wedge \Delta x \geq 110\Big) \;\rightarrow\; \Delta x \geq 50 + \overrightarrow{T} + 6(\Delta L - \overrightarrow{T})$
- $\Delta x \geq 60 \;\Rightarrow_f\; 6(\Delta L) \leq \Delta x$

We prove the second formula below. The proof of the first formula is done in a similar manner. The third formula which is the safety requirement for the gas burner, follows from rule I-MON and the second formula.

Proof of $\Box_f \left[(\psi_1 \;\vee \psi_2 \;\vee \psi_3) \;\wedge\; \psi_4 \right]$**:**

We take:

$$\psi,\ \varphi:\ \left[(\psi_1 \;\vee \psi_2 \;\vee \psi_3) \;\wedge\; \psi_4 \right]$$

II1: $\varphi(\overleftarrow{V}, \overrightarrow{V}) \;\rightarrow\; \psi(\overleftarrow{V}, \overrightarrow{V})$
As $\varphi(\overleftarrow{V}, \overrightarrow{V})$ and $\psi(\overleftarrow{V}, \overrightarrow{V})$ are the same formulas, we get $\varphi(\overleftarrow{V}, \overrightarrow{V}) \;\rightarrow\; \psi(\overleftarrow{V}, \overrightarrow{V})$.

II2: *continuous* $\wedge \Box \rho_\phi(V, \dot{V}) \Rightarrow_f \varphi(\overleftarrow{V}, \overrightarrow{V})$ for every $\phi \in \Phi$
We must consider all three phase relations.

ρ_{ℓ_0}:

$$\textit{continuous} \;\wedge\; \Box \left[\begin{array}{l} \dot{x} = 1 \;\wedge\; \dot{y} = 1 \;\wedge\; \dot{L} = 0 \;\wedge\; \dot{T} = 0 \;\wedge \\ y < 100 \;\wedge\; \mathtt{R} = \mathrm{Off} \;\wedge\; \pi = \ell_0 \;\wedge\; \mathtt{switch} = \mathrm{Off} \end{array} \right] \Rightarrow_f \left[(\psi_1 \;\vee \psi_2 \;\vee \psi_3) \;\wedge\; \psi_4 \right]$$

As $\dot{L} = 0$, $\dot{T} = 0$, and *continuous*, we immediately get $\overrightarrow{L} = \overleftarrow{L}$ and $\overrightarrow{T} = \overleftarrow{T}$. This makes the first conjunct in the consequent of $\varphi(\overleftarrow{V}, \overrightarrow{V})$ true. By a previously established point invariant, we get $0 \leq \overrightarrow{y} \leq 100$ and $0 \leq \overleftarrow{y} < 100$, so $\overrightarrow{y} - \overleftarrow{y} \leq 100$. As $\Delta x = \overrightarrow{y} - \overleftarrow{y} \leq 100$, the second conjunct is also true.

ρ_{ℓ_1}:

$$\textit{continuous} \;\wedge\; \Box \left[\begin{array}{l} \dot{x} = 1 \;\wedge\; \dot{y} = 1 \;\wedge\; \dot{L} = 0 \;\wedge\; \dot{T} = 0 \;\wedge \\ y < 100 \;\wedge\; \pi = \ell_1 \;\wedge\; \mathtt{switch} = \mathrm{Off} \end{array} \right] \Rightarrow_f \left[(\psi_1 \;\vee \psi_2 \;\vee \psi_3) \;\wedge\; \psi_4 \right]$$

As $\dot{L} = 0$, $\dot{T} = 0$, and *continuous*, we immediately get $\overrightarrow{L} = \overleftarrow{L}$ and $\overrightarrow{T} = \overleftarrow{T}$. This makes the first conjunct in the consequent of $\varphi(\overleftarrow{V}, \overrightarrow{V})$ true. As $\Delta x = \overrightarrow{y} - \overleftarrow{y} \leq 100$, the second conjunct is also true.

ρ_{ℓ_2}:

$$\textit{continuous} \;\wedge\; \Box \left[\begin{array}{l} \dot{x} = 1 \;\wedge\; \dot{y} = 1 \;\wedge\; \dot{L} \leq 1 \;\wedge\; \dot{T} = 1 \;\wedge \\ \mathtt{R} = \mathrm{On} \;\wedge\; T < 10 \;\wedge\; \pi = \ell_2 \;\wedge\; \mathtt{switch} = \mathrm{On} \end{array} \right] \Rightarrow_f \left[(\psi_1 \;\vee \psi_2 \;\vee \psi_3) \;\wedge\; \psi_4 \right]$$

As $\overrightarrow{at}\_\ell_{0,1}$ is false, the second conjunct in the consequent is true. As *continuous* and $\Box(\dot{L} \leq \dot{T} = 1)$ implies $\Delta L \leq \Delta T$, the first conjunct in the consequent is true.

II3: $\varphi(V_1, V_2) \;\wedge\; \rho_\tau(V_2, V) \;\wedge\;$ *continuous* $\wedge\; \Box \rho_\phi(V, \overrightarrow{V}) \;\Rightarrow_f\; \varphi(V_1, \overrightarrow{V})$ for every $\tau \in \mathcal{T}$ and for every $\phi \in \Phi$.
There are seven cases to consider (one for each transition).

$\rho_{\langle \ell_0, \ell_0 \rangle}, \rho_{\ell_0}$:

As $\Box(\pi = \ell_0)$ and *continuous* implies $atl\ell 0$, we get:

$$(\Delta_1 x \leq \overrightarrow{y} \wedge \Delta_1 L = 0) \quad \vee \quad (\Delta_1 x > \overrightarrow{y} \wedge \Delta_1 L < \Delta_1 x - \overrightarrow{y})$$

continuous and $\Box(y < 100)$ implies $\overrightarrow{y} \leq 100$. *continuous* and $\Box(\dot{L} = \dot{T} = 0)$ implies $\overrightarrow{L} = L = L_2$ and $\overrightarrow{T} = T = 0$.

Case: $(\Delta_1 x \leq \overrightarrow{y} \wedge \Delta_1 L = 0)$

In this case, $\Delta_1 L \leq 0 = \overrightarrow{T}$ and $\Delta_1 x \leq \overrightarrow{y} \leq 100 \leq \overrightarrow{T} + 100$. So the first conjunct of the consequent holds. As $\Delta_1 x \leq 100$, the second conjunct of the consequent holds.

Case: $(\Delta_1 x > \overrightarrow{y} \wedge \Delta_1 L < \Delta_1 x - \overrightarrow{y})$

subcase: $\Delta_1 x = \overrightarrow{y}$

In this case, $\Delta_1 x \leq \overrightarrow{T} + 100$ and $\Delta_1 L \leq 0 = \overrightarrow{T}$, so the the first conjunct of the consequent holds. As $\Delta_1 L \leq 0$ the second conjunct holds.

subcase: $\Delta_1 x > \overrightarrow{y}$

subcase: $\overrightarrow{y} = 100$

In this case $\Delta_1 x > \overrightarrow{T} + 100$ and $\Delta_1 L \leq \Delta_1 x - \overrightarrow{y} \leq \Delta_1 x - 100$. Either $\Delta_1^2 L < 10$ or $(\Delta_1^2 L \leq \Delta_1^2 x - 100 \wedge 6(\Delta_1^2 L) \leq \Delta_1^2 x)$. In the first case, we get $6(\Delta_1^2 L) < \Delta_1 x$, and so the first conjunct holds. In the second case, $6(\Delta_1^2 L) \leq \Delta_1^2 x \leq \Delta_1 x$, and so the first conjunct holds.

subcase: $\overrightarrow{y} < 100$

If $\Delta_1 x \leq 100 + \overrightarrow{T}$ then the first invariant gives

$$(\Delta_1^2 x \leq y_2 \wedge \Delta_1^2 L = 0) \quad \vee \quad (\Delta_1^2 x > y_2 \wedge \Delta_1^2 L < \Delta_1^2 x - y_2)$$

As $y_2 = 100$ and $x - x_1 \leq 100 = y_2$, we get $\Delta_1^2 x \leq y_2$. Hence $\Delta_1^2 L = 0$ and $\Delta_1 L = 0 \leq \overrightarrow{T}$. Thus the first conjunct holds.

If $\Delta_1 x > 100 + \overrightarrow{T}$, then $\Delta_1 L \leq \Delta_1 x - 100$ and $6(\Delta_1 L) \leq \Delta_1 x$ as in the subcase $\Delta_1 x = \overrightarrow{y}$. Thus the first conjunct holds.

We still need to show that the second conjunct holds. We consider two cases.

subcase: $\Delta_1 x = 110$

In this case $\Delta_1 L = 0 = \overrightarrow{T}$, so the second conjunct holds.

subcase: $\Delta_1 x > 110$

If $\Delta_1^2 x < 110$ then $\Delta_1^2 L < 10$, and so the second conjunct holds. If $\Delta_1^2 x \geq 110$ then $\Delta_1^2 x \geq 50 + T_2 + 6(\Delta_1^2 L - T_2)$. As $\overrightarrow{L} = L_2$ and $\overrightarrow{T} = 0$, the second conjunct holds.

Thus in all subcases, both conjuncts of the consequent hold.

$\rho_{\langle \ell_0, \ell_2 \rangle}, \rho_{\ell_2}$:

As $\overrightarrow{at}\_\ell_{0,1}$ is false, the second conjunct holds. We still need to prove that the first conjunct of the consequent holds. We consider three cases corresponding to the three disjuncts of the first conjunct in the antecedent.

Case: $\Delta_1^2 L \leq \Delta_1^2 x$

As $L = L_2$ and $T = T_2$, we get $L - L_1 \leq T - T_1$. As *continuous* and $\Box(\dot{L} \leq \dot{T} = 1)$ implies $\overrightarrow{L} - L \leq \overrightarrow{T} - T$, we get $\Delta_1 L = \overrightarrow{L} - L + L - L_1 \leq \overrightarrow{T} - T + T - T_1 \leq \Delta_1 T$. So the first conjunct of the consequent holds.

Case: $\Delta_1^2 L \leq T_2$ and $\Delta_1^2 x \leq T_2 + 100$

As $x = x_2$ and $T = T_2$, $x - x_1 \leq T + 100$. As *continuous* and $\Box(\dot{x} = \dot{T} = 1)$ implies $\overrightarrow{x} - x = \overrightarrow{T} - T$, we get $\Delta_1 x = \overrightarrow{x} - x + x - x_1 \leq \overrightarrow{T} - T + T + 100 \leq \overrightarrow{T} + 100$. So the first conjunct of the consequent holds.

Case: $(\Delta_1^2 L \leq \Delta_1^2 x - 100)$ and $(\Delta_1^2 x > T_2 + 100)$ and $(6(\Delta_1^2 L) \leq \Delta_1^2 x)$

By reasoning similar to the previous cases, we get $\Delta_1 x > \overrightarrow{T} + 100$ and $\Delta_1 L \leq \Delta_1 x - 100$. We still need to show $6(\Delta_1 L) \leq \Delta_1 x$.
As $at_2\_\ell_0$ holds, by the previous invariant

$$(\Delta_1^2 x \leq y_2 \ \wedge\ \Delta_1^2 L = 0) \ \vee\ (\Delta_1^2 x > y_2 \ \wedge\ \Delta_1^2 L < \Delta_1^2 x - y_2)$$

subcase: $\Delta_1^2 x \leq y_2 \ \wedge\ \Delta_1^2 L = 0$

As $0 \leq T < 10$, and *continuous* and $\Box(\dot{L} \leq \dot{T} = 1)$ implies $\overrightarrow{T} - T \geq \overrightarrow{L} - L$, we get $10 \geq \overrightarrow{L} - L \leq \Delta_1 L$. As $\Delta_1 x > 100$, we get $6(\Delta_1 L) \leq 60 \leq 100 \leq \Delta_1 x > 100$.

subcase: $\Delta_1^2 x > y_2 \ \wedge\ \Delta_1^2 L < \Delta_1^2 x - y_2$

subcase: $\Delta_1^2 x < 110$

In this case $\Delta_1^2 L \leq \Delta_1^2 x - 100$ (using the point invariant to give $T_2 = 10$). So, $6(\Delta_1 L) = 6(\overrightarrow{L} - L + L - L_1) = 6(\overrightarrow{L} - L) + 6(L - L_1) \leq 6(\overrightarrow{x} - x) + 6(\Delta_1^2 x - 100) \leq (\overrightarrow{x} - x) + 5(\Delta_1 x) - 600 \leq \Delta_1 x$. The last inequality follows from the fact that $\Delta_1 x < 120$.

subcase: $\Delta_1^2 x \geq 110$

$\Delta_1 x = \overrightarrow{x} - x + x - x_1 = \overrightarrow{T} - T + \Delta_1^2 x = \overrightarrow{T} - T_2 + \Delta_1^2 x \geq \overrightarrow{T} - T_2 + 50 + T_2 + 6(\Delta_1^2 L - T_2) \geq \overrightarrow{T} + 50 + 6(\Delta_1^2 L) - 6T_2 \geq 6\overrightarrow{T} + 6(\Delta_1^2 L) - 6T_2 \geq 6(\overrightarrow{L} - L) + 6(\Delta_1^2 L) \geq 6(\Delta_1 L)$

Thus the first conjunct holds.

$\rho_{\langle \ell_1, \ell_0 \rangle}, \rho_{\ell_0}$:

This case is exactly the same as $\rho_{\langle \ell_0, \ell_0 \rangle}, \rho_{\ell_0}$.

$\rho_{\langle \ell_1, \ell_1 \rangle}, \rho_{\ell_1}$:

This case is exactly the same as $\rho_{\langle \ell_0, \ell_0 \rangle}, \rho_{\ell_0}$.

$\rho_{\langle \ell_1, \ell_2 \rangle}, \rho_{\ell_2}$:

As $\overrightarrow{at}\_\ell_{0,1}$ is false, the second conjunct holds. We still need to prove that the first conjunct of the consequent holds.
As $at_2\_\ell_0$ holds, by the previous invariant

$$(\Delta_1^2 x \leq y_2 \ \wedge\ \Delta_1^2 L = 0) \ \vee\ (\Delta_1^2 x > y_2 \ \wedge\ \Delta_1^2 L < \Delta_1^2 x - y_2)$$

Case: $\Delta_1^2 x \leq y_2 \ \wedge\ \Delta_1^2 L = 0$

As $L = L_2 = L_1$, $T = 0$, and *continuous* and $\Box(\dot{L} \leq \dot{T} = 1)$ implies $\overrightarrow{T} - T \geq \overrightarrow{L} - L$, we get $\overrightarrow{T} \geq \Delta_1 L$. As $y_2 = 100$, we have $\Delta_1^2 x \leq 100$. *continuous* and $\Box(\dot{x} = \dot{T} = 1)$ implies $\overrightarrow{T} - T = \overrightarrow{x} - x$. Thus, $\Delta_1 x \leq \overrightarrow{T} + 100$. So the first conjunct holds.

Case: $\Delta_1^2 x > y_2 \ \wedge\ \Delta_1^2 L < \Delta_1^2 x - y_2$

This case is identical to the third case of $\rho_{\langle \ell_0, \ell_2 \rangle}, \rho_{\ell_2}$. Thus the first conjunct holds.

$\rho_{\langle \ell_2, \ell_0 \rangle}, \rho_{\ell_0}$:

The proof of the first conjunct is very similar to the case $\rho_{\langle \ell_0, \ell_0 \rangle}, \rho_{\ell_0}$. Instead of $\overrightarrow{T} = T_2$ we have $0 \leq \overrightarrow{T} \leq 10$. The proof of the second conjunct is very similar to the case $\rho_{\langle \ell_2, \ell_1 \rangle}, \rho_{\ell_1}$.

$\rho_{\langle \ell_2, \ell_1 \rangle}, \rho_{\ell_1}$:

We consider three cases corresponding to the three disjuncts of the first conjunct in the antecedent.

Case: $\Delta_1^2 L \leq \Delta_1^2 x$

In this case $\Delta_1 L \leq \Delta_1 T \leq 10$, so both the first and second conjunct of the consequent hold.

Case: $\Delta_1^2 L \leq T_2$

In this case $\Delta_1 L \leq \overrightarrow{T} \leq 10$, so both the first and second conjunct of the consequent hold.

Case: $\Delta_1^2 L \leq \Delta_1^2 x - 100$ and $\Delta_1^2 x > T_2 + 100$

If $\Delta_1^2 x \geq 110$ then as $\overrightarrow{T} = T_2$ and $\overrightarrow{L} = L_2$, we get $\Delta_1 x \geq \Delta_1^2 x \geq 50 + T_2 + 6(\Delta_1^2 L - T_2) \geq 50 + \overrightarrow{T} + 6(\Delta_1 L - \overrightarrow{T})$. So the second conjunct holds. If $\Delta_1^2 x < 110$ then $\Delta_1^2 L \leq 10$, and so the second conjunct holds. In either case, $\Delta_1 x \geq \Delta_1^2 x \geq 6(\Delta_1^2 L) \geq 6(\Delta_1 L)$, so the first conjunct holds.