Using Abstractions for the Verification of Linear Hybrid Systems *

A. Olivero J. Sifakis S. Yovine

VERIMAG †
Miniparc-Zirst rue Lavoisier
38330 Montbonnot St. Martin, France

1 Introduction

Hybrid systems are dynamical systems consisting of interacting discrete and continuous components [NSY91, MMP91]. They are used to model the combined behavior of embedded real-time systems and their physical environments. Recently, there have been attempts to develop verification methods for hybrid systems by working in two complementary directions :

- The first direction concerns the identification of subclasses of hybrid systems for which there exist decidability results and effective verification methods for various classes of properties. The main decidability results concern very restricted classes of hybrid systems. For timed graph, automata extended with *clocks* (i.e., continuous variables that increase uniformly at a rate equal to one with respect to time) real-time properties expressed in TCTL are decidable [ACD90, HNSY92]. Also, for integration graphs which are automata with integrators, continuous variables which can measure the time spent at states, invariance and some liveness properties are known to be decidable [KPSY93, BES93]. However, the verification problem for non trivial properties becomes undecidable if the classes mentioned are augmented, for instance by having both clocks and integrators [KPSY93].
- The second direction concerns the elaboration of a general verification methodology for classes of systems for which tractable semi-decision methods are applicable. One interesting class is linear hybrid systems [NOSY93, ACHH93], i.e., systems where conditions on discrete transitions and evolution laws of continuous variables are linear constraints. For such systems it has been shown that the model-checking procedure given in [HNSY92] can be applied (without however guarantee of termination). A key idea to cope with this problem, is the application of approximation techniques or of techniques of abstract interpretation that enforce the termination of the verification algorithm and yield sufficient verification conditions for certain classes of properties, in particular safety properties. Such methods have been applied in [Hal93, WTD93].

This paper deals with the verification of linear hybrid systems by bringing results in the two mentioned directions :

- It identifies a class of linear hybrid systems which are shown to be bisimilar to hybrid systems with a unique constant slope and for which the satisfaction of TCTL properties is decidable exactly as for timed graphs.
- It studies transformations of general linear hybrid systems which define abstractions on which properties expressed in TCTL are decidable. Then it extends well-known results [BBLS92, GL93] concerning

*Supported by the ESPRIT project N°6021 REACT-P
†VERIMAG is a joint laboratory of CNRS, INPG, UJF and VERILOG S.A.

property preservation by abstractions, to show that properties of ∀TCTL, a fragment of TCTL, are satisfied on a linear hybrid system provided they are satisfied on some abstraction for which they are decidable.

The paper is organized as follows :

Section 2 presents the model of Linear Hybrid Systems (LHS) where continuous variables evolve according to linear functions with slopes varying within an interval. We define two sub-classes of LHS that will be considered in the subsequent sections : Constant Slope Hybrid Systems (CSHS) [KPSY93], where the slopes of the evolution functions are constant and K-Timed Graphs (K-TG) that are CSHS where for all variables the slope is equal to a constant K.

In Section 3 we review the syntax and the semantics of the logic TCTL used to describe system properties.

In Section 4 we give a simple transformation that maps the sub-class of CSHS with non-zero slopes into equivalent timed graphs in the sense that the underlying models are bisimilar. This implies in particular, that the initial and the transformed system satisfy the same TCTL formulas modulo a linear time transformation. These results are used to show that satisfaction of TCTL is decidable for transformable CSHS.

In Section 5 we prove that the results of Section 4 cannot be extended to general LHS. We propose an extension of the transformation of Section 4 which applied to a LHS yields a timed graph which is an abstraction of it. Then we prove that the validity of ∀TCTL formulas is preserved for timed graphs that are abstractions of LHS. Thus, for some properties (among which safety properties) their satisfaction on a timed graph abstraction of a LHS implies the satisfaction on the concrete system.

2 Linear Hybrid Systems

2.1 Syntax

Let X be a set of *variables* ranging over the set $\mathbf{R}$ of real numbers. A *valuation* X_0 of X assigns to each variable $x \in X$ a real number $x_0 \in \mathbf{R}$. A *linear predicate* over X is a boolean combination of linear inequalities with integer coefficients over X.

A *linear hybrid system* (LHS) H is a structure $\langle S, X, E, A, B, \phi \rangle$ where:

- S is a finite set of *locations*. In a graphical representation of the system they are drawn as the nodes of the graph.
- X is a finite set of real-valued *variables*. These variables change *continuously* at locations and *discretely* via transitions.
- E is a finite set of *edges*. Each edge $e \in E$ is a tuple $\langle s, a, \psi, \upsilon, s' \rangle$, where $s \in S$ is the *source*, $s' \in S$ is the *target*, a is the *label*, ψ is a linear predicate called the *guard*, and υ is an *assignment* represented as a set $\{x := \upsilon_x \mid x \in Y \subseteq X\}$ where υ_x is an interval with end-points in $\mathbf{Z} \cup \{-\infty, +\infty\}$.

  In the graphical representation, each $e \in E$ is drawn as an edge from the source location to the target location with the label (a, ψ, υ).
- A and B associate to each location $s \in S$ the functions A_s and B_s from X to $\mathbf{Z}$ such that $A_s(x) \leq B_s(x)$. $A_s(x)$ and $B_s(x)$ define the bounds of a closed interval to which belongs the rate of change of the variable x at the location s.
- ϕ associates with each location $s \in S$ a linear predicate ϕ_s over X called the *invariant* at s. We require ϕ_s to be such that if $\phi_s(X_0 + \Lambda t)$, with $\Lambda \in [A_s, B_s]$, then $\phi_s(X_0 + \Lambda t')$ for all $0 \leq t' \leq t$.

A *Constant Slope Hybrid System* (CSHS) [KPSY93] is a linear hybrid system such that $A = B$. That is, for all locations $s \in S$ and for all variables $x \in X$, the left-hand and right-hand end-points of the rate interval are the same. Any variable x changes continuously at a constant rate $A_s(x)$ at s. We denote a CSHS as a tuple $H = \langle S, X, E, A, \phi \rangle$ rather than $H = \langle S, X, E, A, A, \phi \rangle$

A K-*Timed Graph* (K-TG) is a constant slope hybrid system where all variables are nonnegative and change *uniformly* at the same rate $K > 0$, that is $A_s(x) = K$. Guards are boolean combinations of inequalities of the form $l \prec x \prec u$ where $\prec \in \{<, \leq\}$ and $l \in \mathbf{N}$ and $u \in \mathbf{N} \cup \{+\infty\}$. We denote a K-TG as a tuple $H = \langle S, X, E, \vec{K}, \phi\rangle$.

A 1-*Timed Graph* differs from a timed graph [ACD90, Alu91, NSY91] in the sense that assignments are intervals rather than resets to zero. 1-Timed Graphs are an extension of timed graphs for which all the decidability and model-checking results concerning timed graphs can also be applied. For this reason 1-timed graphs are hereafter simply called timed graphs.

Notation: If A is a tuple of scalars and c is a scalar, we write:

- $A(i)$ to represent the i-th component of A.
- $\frac{c}{A}$ to represent the tuple with i-th component $\frac{c}{A(i)}$
- $A \prec B$ if $A(i) \prec B(i)$ for any component and $\prec \in \{<, \leq\}$.

2.2 Semantics

Let $H = \langle S, X, E, A, B, \phi\rangle$ be a linear hybrid system. A *state* of H is a pair (s, X_0) such that $\phi_s(X_0)$, that is, the invariant at s is true for X_0. We denote by Q the set of states. For $q = (s, X_0) \in Q$, $q(x)$ is the value x_0 of x at the valuation X_0.

H changes its state either by a *discrete* and *instantaneous* move through an edge, or by a *continuous* transformation of its variables while time elapses. The semantics of H is a labeled transition system $\langle Q, \rightarrow\rangle$ where the transition relation $\rightarrow$ between states is defined by the following rules:

- An edge $\langle s_0, a, \psi, \upsilon, s_1\rangle \in E$ is *enabled* at a state (s_0, X_0) if X_0 satisfies the guard ψ. Whenever an edge is enabled at a state it may be taken, and the resulting state is a pair (s_1, X_1) where X_1 is such that for every variable $x \in X$, $x_1 \in \upsilon_x$ if $x := \upsilon_x \in \upsilon$, and $x_1 = x_0$ otherwise. We denote by $\upsilon(X_0)$ the set of such valuations.
$$\frac{\langle s_0, a, \psi, \upsilon, s_1\rangle \in E, \psi(X_0), X_1 \in \upsilon(X_0)}{(s_0, X_0) \xrightarrow{a} (s_1, X_1)}$$
- Time can progress by t at (s, X_0), if there is a valuation X_1 reached from X_0 for a rate $\Lambda \in [A_s, B_s]$ and X_1 satisfies the invariant associated to s.
$$\frac{X_1 = X_0 + \Lambda t, \Lambda \in [A_s, B_s], \phi_s(X_1)}{(s, X_0) \xrightarrow{t} (s, X_1)}$$

We introduce the following definitions:
A *trajectory* σ is an infinite sequence $q_0 \overset{t_0}{\mapsto} q_1 \overset{t_1}{\mapsto} \ldots$ where for all $i \geq 0$ $q_i \overset{t_i}{\mapsto} q_{i+1}$ is such that

- $q_i \xrightarrow{t_i} q_{i+1}$, or
- there exists a label a such that $q_i \xrightarrow{a} q_{i+1}$ and $t_i = 0$.

A *position* π of σ is a pair (i, t) with $0 \leq t \leq t_i$. We define a total order $\preceq$ on the positions, as follows:

$$(i, t) \preceq (j, t') \text{ iff } i < j \text{ or } i = j \wedge t < t'$$

Let $q_i = (s_i, X_{0i})$ and $q_{i+1} = (s_i, X_{0i+1})$ where $X_{0i+1} = X_{0i} + \Lambda_i.t_i$, with $\Lambda_i \in [A_{s_i}, B_{s_i}]$. The *state at position* (i, t) of σ is $\sigma(i, t) = (s_i, X_{0i} + \Lambda_i.t)$. The *time elapsed at position* (i, t) is $\tau_\sigma(i, t) = t + \sum_{j<i} t_j$, that is, the time elapsed since the beginning of the trajectory.

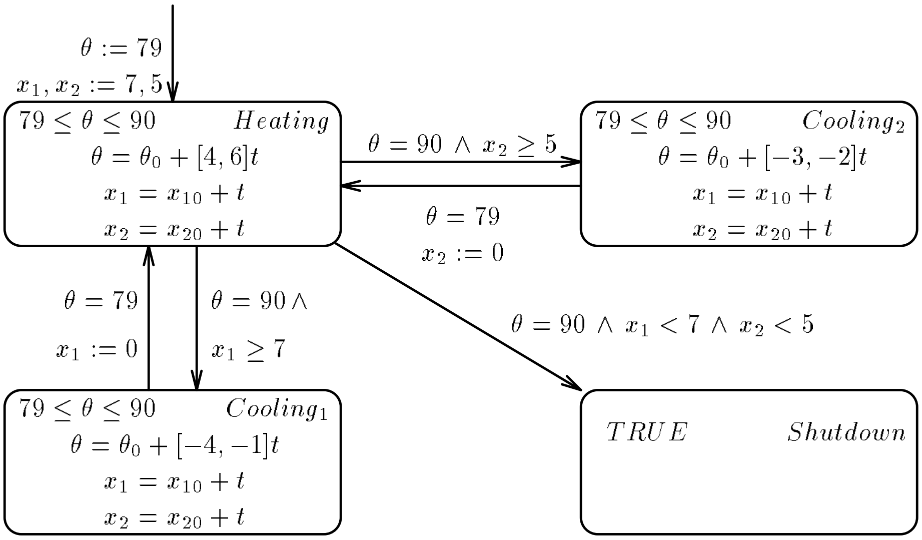

Figure 1: Temperature control system

A trajectory σ *diverges* if for all $t \in \mathbf{R}^+$ there exists a position π such that $\tau_\sigma(\pi) > t$. The set of all divergent trajectories is represented by Σ, and the set of all divergent trajectories starting at q by $\Sigma(q)$.

Remark: A different semantics for LHS is proposed in [HH93] for which the results developed in the paper are also valid.

2.3 Example

The temperature of a reactor tank grows linearly with time at rates belonging to the interval [4,6]. For safety reasons the temperature must be kept within a minimum of 79 and a maximum of 90 degrees. A controller cools the tank by moving two independent rods. The rates of cooling belong to the intervals [-4,-1] and [-3,-2], respectively. Furthermore, each rod can be used again only if a given time has elapsed since the end of its previous movement. These minimum times are 7 and 5 minutes, respectively. If the temperature cannot be decreased because there is no available rod, a complete shutdown is required. A variant of this example is given in [JLHM91, NOSY93].

Figure 1 shows a linear hybrid system for the controller. We use three variables: θ measures the temperature of the tank and x_1 and x_2 count the time elapsed since the last use of the respective rod. Initially, the temperature takes its minimum value and both rods can be used.

The equations at locations specify the evolution laws of the variables corresponding to the bounds on the slopes. This notation will be used in the sequel.

3 The logic TCTL

The real-time temporal logic TCTL is a real-time extension of CTL [CES86]. Many slightly different versions of TCTL have been defined [ACD90, Alu91, HNSY92]. We adopt here the one defined in [ACD90] using the temporal operators $\exists\mathcal{U}$ and $\forall\mathcal{U}$ of CTL with subscripts that limit their scope in time.

Intuitively, $f_1 \exists\mathcal{U}_{\#n} f_2$ means that there exists a trajectory such that f_2 holds at some state at a time t satisfying $t \# n$ and f_1 continuously holds at all intermediate states. $f_1 \forall\mathcal{U}_{\#n} f_2$ means that for every trajectory the above property holds. For example, we can write $\mathtt{true}\exists\mathcal{U}_{<5}p$ to say that along some trajectory, p becomes true before time 5.

3.1 Syntax

Let P be a finite set of atomic propositions. The formulas of TCTL are defined by the following grammar:

$$f \quad ::= \quad p \mid l \prec x \prec u \mid \neg f \mid f_1 \vee f_2 \mid f_1 \exists\mathcal{U}_{\#n} f_2 \mid f_1 \forall\mathcal{U}_{\#n} f_2$$

where $p \in P$, $x \in X$, $l, u \in \mathbf{Z} \cup \{-\infty, +\infty\}$, $\prec \in \{<, \leq\}$, $n \in \mathbf{N}$ and $\# \in \{<, \leq, >, \geq, =\}$.

We use standard abbreviations such as $\forall\Diamond_{\#n} f$ for $\mathtt{true}\forall\mathcal{U}_{\#n} f$, $\exists\Diamond_{\#n} f$ for $\mathtt{true}\exists\mathcal{U}_{\#n} f$, $\exists\Box_{\#n} f$ for $\neg\forall\Diamond_{\#n}\neg f$ and $\forall\Box_{\#n} f$ for $\neg\exists\Diamond_{\#n}\neg f$. In Section 5 we use the abbreviation $f_1 \forall\mathcal{W}_{\#n} f_2$ for the formula $\neg(\neg f_1 \exists\mathcal{U}_{\#n} \neg f_2)$. The unrestricted temporal operators of CTL correspond to TCTL operators subscripted by ≥ 0.

3.2 Semantics

TCTL formulas are interpreted over the divergent trajectories generated by the model of a linear hybrid system. Let H be a LHS, $\langle Q, \rightarrow\rangle$ its model, Σ the set of its divergent trajectories and M an interpretation of atomic propositions over the set of states, that is, $M(p) \subseteq Q$ for all $p \in P$.

A state $q \in Q$ *satisfies* under the interpretation M the formula f, denoted $q \models_{\Sigma,M} f$, if

- $q \models_{\Sigma,M} p$ iff $q \in M(p)$;
- $q \models_{\Sigma,M} l \prec x \prec u$ iff $l \prec q(x) \prec u$;
- $q \models_{\Sigma,M} \neg f$ iff $q \not\models_{\Sigma,M} f$;
- $q \models_{\Sigma,M} f_1 \vee f_2$ iff $q \models_{\Sigma,M} f_1$ or $q \models_{\Sigma,M} f_2$;
- $q \models_{\Sigma,M} f_1 \exists\mathcal{U}_{\#n} f_2$ iff for some sequence $\sigma \in \Sigma(q)$ there exists a position π such that $\sigma(\pi) \models_{\Sigma,M} f_2$ and $\tau_\sigma(\pi)\#n$, and for all $\pi' \preceq \pi$, $\sigma(\pi') \models_{\Sigma,M} f_1 \vee f_2$;
- $q \models_{\Sigma,M} f_1 \forall\mathcal{U}_{\#n} f_2$ iff for all sequences $\sigma \in \Sigma(q)$ there exists a position π such that $\sigma(\pi) \models_{\Sigma,M} f_2$ and $\tau_\sigma(\pi)\#n$, and for all $\pi' \preceq \pi$, $\sigma(\pi') \models_{\Sigma,M} f_1 \vee f_2$;

H satisfies f under M, denoted $H \models_{\Sigma,M} f$, if all the states satisfy f.

3.3 Example

We express in TCTL three properties of the example 2.3.

- The location *Shutdown* is not reachable:

$$(\mathit{Heating} \wedge \theta = 79 \wedge x_1 = 7 \wedge x_2 = 5) \Rightarrow \forall\Box\neg\mathit{Shutdown} \tag{1}$$

- Rod 1 can be used again only if at least 7 minutes have elapsed since the end of its previous movement.

$$(\mathit{Heating} \wedge \theta = 79 \wedge x_1 = 0) \Rightarrow \neg\exists\Diamond_{<7}\mathit{Cooling}_1 \tag{2}$$

- Rod 2 can be used again only if at least 5 minutes have elapsed since the end of its previous movement.

$$(\mathit{Heating} \wedge \theta = 79 \wedge x_2 = 0) \Rightarrow \neg\exists\Diamond_{<5}\mathit{Cooling}_2 \tag{3}$$

4 From Constant Slope Hybrid Systems to Timed Graphs

We define the class of Non-Zero Constant Slope Hybrid System, denoted $\mathrm{CSHS}_{\neq 0}$, such that:

- All the rates are different from zero.
- The invariant and guards are boolean combinations of inequalities of the form $l \prec x \prec u$ with $\prec \in \{<, \leq\}$.
- For all edges $e = \langle s, a, \psi, v, s' \rangle \in E$ and for all variables $x \in X$, if the rates of change of x are different at s and s', then x is an assignment in v.
- If at some location s the slope of x is positive (negative) then assignments to x in edges with target location s or in conditions on x in guards of edges with source location s the lower bounds (upper bounds) are different from $-\infty$ ($+\infty$).

The restriction $\mathrm{CSHS}_{\neq 0}$ is justified by the fact that the class of CSHS where slopes equal to zero are allowed strictly contains the class timed graphs. As shown in [KPSY93] for instance, the reachability problem is undecidable for general CSHS, while it is decidable for timed graphs.

In this section we show how a given $\mathrm{CSHS}_{\neq 0}$ can be transformed into an equivalent TG. To this end, we use two transformations: the K-transformation and the $\frac{1}{K}$-transformation, whose successive application to a $\mathrm{CSHS}_{\neq 0}$ gives a K-timed graph and a timed graph, respectively. The key idea is to apply linear transformations of variables which are proper to each location. For the K-transformation the aim is to obtain the same evolution laws for all variables and locations by multiplying by appropriate constants. Consequently, conditions and assignments are modified. The $\frac{1}{K}$-transformation consists in changing the time scale. Both transformations preserve bisimilarity of the underlying models.

4.1 Translating $\mathrm{CSHS}_{\neq 0}$ into K-TG

4.1.1 The K-transformation

Given $H = \langle S, X, E, A, \phi \rangle$ in $\mathrm{CSHS}_{\neq 0}$, we define the set of functions $\kappa = \{\kappa_s \mid s \in S\}$ as follows:

$$\kappa_s(X) = \frac{K}{A_s} X + C_s$$

where:

- $K = \mathsf{lcm}\{\mathrm{abs}(A_s(x)) \mid s \in S, x \in X\}$, that is, K is the least common multiple of the absolute values of the rates appearing in H.
- C_s is a tuple such that $C_s(x)$ is the maximum of the absolute values of all the constants appearing in assignments to x in edges with target location s or in conditions on x in guards of edges with source location s, multiplied by $\mathrm{abs}(\frac{K}{A_s(x)})$.

For given $H = \langle S, X, E, A, \phi \rangle$ in $\mathrm{CSHS}_{\neq 0}$, we construct a K-timed graph $H_K = \langle S, X', E', \vec{K}, \phi' \rangle$ such that:

- X' is in bijection with X.
- To compute E' and ϕ', replace every condition $l \prec x \prec u$ appearing in guards of edges with source s, in assignments of edges with target s or in ϕ_s by a condition $\frac{K}{A_s(x)} l + C_s(x) \prec x' \prec \frac{K}{A_s(x)} u + C_s(x)$ when the rate $A_s(x)$ is positive, or by a condition $\frac{K}{A_s(x)} u + C_s(x) \prec x' \prec \frac{K}{A_s(x)} l + C_s(x)$ when the rate $A_s(x)$ is negative.

Notice that H_K is constructed from H so that the relation $X' = \kappa_s(X)$ holds for each location s.

4.1.2 Property preservation by K-transformation

We want to prove that H and H_K are bisimilar. We recall here the definition of bisimulation.

Definition 4.1 Let $T_1 = \langle Q_1, \rightarrow_1 \rangle$ and $T_2 = \langle Q_2, \rightarrow_2 \rangle$ be two labeled transition systems over a set $\mathcal{L}$ of labels and a relation $\rho \subseteq Q_1 \times Q_2$.

The relation ρ is a *bisimulation* between T_1 and T_2, if $\rho(q_1, q_2)$ implies for every label $\ell \in \mathcal{L}$:

- If $q_1 \xrightarrow{\ell}_1 q_1'$, then there exists q_2' such that $q_2 \xrightarrow{\ell}_2 q_2'$ and $\rho(q_1', q_2')$.
- If $q_2 \xrightarrow{\ell}_2 q_2'$, then there exists q_1' such that $q_1 \xrightarrow{\ell}_1 q_1'$ and $\rho(q_1', q_2')$.

We say that T_1 and T_2 are *bisimilar*, denoted $T_1 \sim T_2$, if there exists a relation ρ such that ρ is a bisimulation between T_1 and T_2.

For H_1 and H_2 linear hybrid systems, we write $\langle H_1, q_1 \rangle \sim \langle H_2, q_2 \rangle$ if the transition systems generated respectively for q_1 and q_2 are bisimilar. We write $H_1 \sim H_2$ if there exists a relation ρ such that ρ is a bisimulation between the models of H_1 and H_2. ■

We naturally extend the function κ to a relation on states in the following way:

$$\kappa((s, X), (s', X')) \text{ iff } s = s' \text{ and } X' = \kappa_s(X)$$

Proposition 4.1 *For all CSHS$_{\neq 0}$ H, $H \sim H_K$.*

Proof: It is straightforward to prove that the relation κ is a bisimulation between H and H_K. ■

Our goal is to prove that H and H_K satisfy the same TCTL formulas modulo the transformation of the predicates over X according to κ. So, for any formula f we define a formula $\mid f \mid_K$, such that H satisfies f iff H_K satisfies $\mid f \mid_K$. The formula $\mid f \mid_K$ is defined as follows:

$$\begin{array}{rcl}
\mid p \mid_K & = & p \\
\mid l \prec x \prec u \mid_K & = & \bigvee_{s \in S} p_s \wedge \kappa_{s,x}(l \prec x \prec u) \\
\mid \neg f \mid_K & = & \neg \mid f \mid_K \\
\mid f_1 \ op\ f_2 \mid_K & = & \mid f_1 \mid_K \ op\ \mid f_2 \mid_K \ \text{ for } \ op \in \{\vee, \exists\mathcal{U}_{\#n}, \forall\mathcal{U}_{\#n}\}
\end{array}$$

Where p_s is an atomic proposition which holds only at location s and $\kappa_{s,x}(l \prec x \prec u)$ is the condition $l' \prec x' \prec u'$ as in Section 4.1.1.

Proposition 4.2 *For any H in CSHS$_{\neq 0}$, f formula of* TCTL *and interpretation M,*

$$H \models_{\Sigma,M} f \text{ iff } H_K \models_{\Sigma_K,M} \mid f \mid_K$$

Proof: By induction on the structure of the formula based on the fact that $H \sim H_K$. ■

4.1.3 Example (continued)

The CSHS H of Figure 2 is a variant of the LHS of the Figure 1. The evolution law for θ is different at all states. However, since all conditions are of the form $\theta = c$ (for a constant c) we can add the assignment $\theta := c$ without changing the semantics of the system. Thus, $H \in$ CSHS$_{\neq 0}$ and the K-transformation is applicable to obtain the K-TG of Figure 3. The set of functions κ is given by:

$$\begin{array}{rcll}
\theta' & = & 2\theta + 180 & \text{at location } \mathit{Heating} \\
\theta' & = & -3\theta + 270 & \text{at location } \mathit{Cooling}_1 \\
\theta' & = & -4\theta + 360 & \text{at location } \mathit{Cooling}_2 \\
x_1' & = & 12x_1 + 84 & \text{at all locations} \\
x_2' & = & 12x_2 + 60 & \text{at all locations}
\end{array}$$

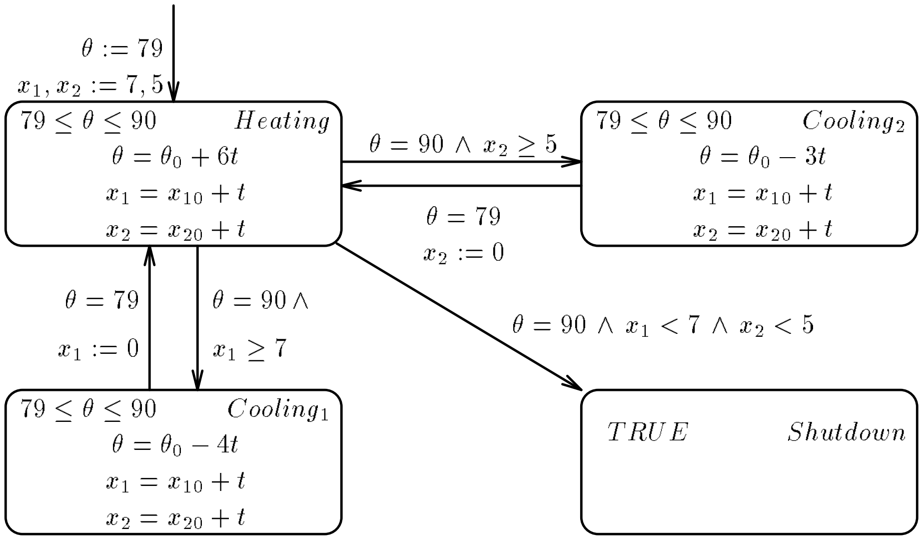

Figure 2: Temperature control system (CSHS)

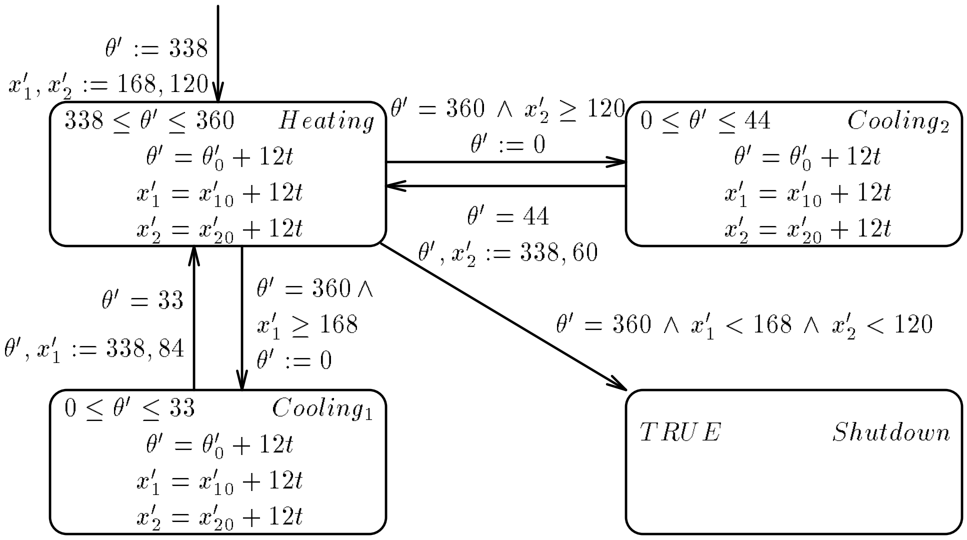

Figure 3: Temperature control system (K-TG)

The transformation of formulas (1), (2) and (3) according to $|\cdots|_K$ gives:

$$(Heating \wedge \theta' = 338 \wedge x_1' = 168 \wedge x_2' = 120) \Rightarrow \forall\Box\neg Shutdown \tag{4}$$

$$(Heating \wedge \theta' = 338 \wedge x_1' = 84) \Rightarrow \neg\exists\Diamond_{<7} Cooling_1 \tag{5}$$

$$(Heating \wedge \theta' = 338 \wedge x_2' = 60) \Rightarrow \neg\exists\Diamond_{<5} Cooling_2 \tag{6}$$

By proposition 4.2, H satisfies formulas (1), (2) and (3) iff H_K satisfies formulas (4), (5) and (6), respectively.

4.2 Translating K-TG into TG

We show that the problem of verifying TCTL formulas on K-timed graphs can be reduced to the problem of verifying TCTL formulas on timed graphs.

4.2.1 The $\frac{1}{K}$-transformation

Given a K-timed graph $H_K = \langle S, X, E, \vec{K}, \phi\rangle$, we define a timed graph $H_1 = \langle S, X, E, \vec{1}, \phi\rangle$. That is, an evolution law of the form $x = x_0 + Kt$ in H_K is replaced by the law $x = x_0 + t$ in H_1.

Let $\langle Q, \rightarrow_K\rangle$, $\langle Q, \rightarrow_1\rangle$ be the models of H_K and H_1 respectively. Both models have the same set of states because H_K and H_1 only differ in the evolution laws. Besides, they are related as follows:

- discrete transitions are identical in both models, that is for all a:

$$q_0 \xrightarrow{a}_K q_1 \text{ iff } q_0 \xrightarrow{a}_1 q_1$$

- and for all t a continuous evolution by t in $\langle Q, \rightarrow_K\rangle$ corresponds to a continuous evolution by Kt in $\langle Q, \rightarrow_1\rangle$ and conversely, that is:

$$q_0 \xrightarrow{t}_K q_1 \text{ iff } q_0 \xrightarrow{Kt}_1 q_1$$

Let Σ_1 and Σ_K be the sets of divergent trajectories of H_1 and H_K respectively. Σ_1 and Σ_K are in bijection, that is:

$$\sigma_K = q_0 \overset{t_0}{\mapsto}_K q_1 \overset{t_1}{\mapsto}_K \ldots \in \Sigma_K \text{ iff } \sigma_1 = q_0 \overset{Kt_0}{\mapsto}_1 q_1 \overset{Kt_1}{\mapsto}_1 \ldots \in \Sigma_1$$

and besides for all i and time t, $\pi_K = (i, t)$ is a position of σ_K iff $\pi_1 = (i, Kt)$ is a position of σ_1, satisfying:

- $\sigma_K(\pi_K) = \sigma_1(\pi_1)$
- $\tau_{\sigma_1}(i, Kt) = Kt + \sum_{j<i} Kt_j = K(t + \sum_{j<i} t_j) = K\tau_{\sigma_K}(i, t)$

From these remarks it follows that for any trajectory of H_K there exists a trajectory of H_1 with the same visited states and such that the time elapsed in H_1 is K times the time elapsed in H_K, and conversely.

4.2.2 Property preservation by $\frac{1}{K}$-transformation

Now we want to prove that verifying a TCTL formula on H_K is equivalent to verifying on H_1 an appropriate TCTL formula, where the time bounds are multiplied by K. Given a formula f, we define a formula $|\, f \,|_{\frac{1}{K}}$ as follows:

$$\begin{array}{rcl}
|\, p \,|_{\frac{1}{K}} & = & p \\
|\, l \prec x \prec u \,|_{\frac{1}{K}} & = & l \prec x \prec u \\
|\, \neg f \,|_{\frac{1}{K}} & = & \neg \,|\, f \,|_{\frac{1}{K}} \\
|\, f_1 \vee f_2 \,|_{\frac{1}{K}} & = & |\, f_1 \,|_{\frac{1}{K}} \vee |\, f_2 \,|_{\frac{1}{K}} \\
|\, f_1 \exists\mathcal{U}_{\#n} f_2 \,|_{\frac{1}{K}} & = & |\, f_1 \,|_{\frac{1}{K}} \exists\mathcal{U}_{\#Kn} \,|\, f_2 \,|_{\frac{1}{K}} \\
|\, f_1 \forall\mathcal{U}_{\#n} f_2 \,|_{\frac{1}{K}} & = & |\, f_1 \,|_{\frac{1}{K}} \forall\mathcal{U}_{\#Kn} \,|\, f_2 \,|_{\frac{1}{K}}
\end{array}$$

Proposition 4.3 *Given a K-timed graph H_K and H_1 for every* TCTL *formula f:*

$$H_K \models_{\Sigma_K,M} f \text{ iff } H_1 \models_{\Sigma_1,M} | f |_{\frac{1}{K}}$$

Proof: Based on the remarks of Section 4.2.1. ■

4.2.3 Example (continued)

The $\frac{1}{K}$-transformation is applicable to the system H_K of Figure 3 to obtain a TG H_1. The transformation of formulas (4), (5) and (6) according to $| \cdots |_{\frac{1}{K}}$ gives:

$$(Heating \wedge \theta' = 338 \wedge x'_1 = 168 \wedge x'_2 = 120) \Rightarrow \forall\Box\neg Shutdown \quad (7)$$

$$(Heating \wedge \theta' = 338 \wedge x'_1 = 84) \Rightarrow \neg\exists\Diamond_{<84} Cooling_1 \quad (8)$$

$$(Heating \wedge \theta' = 338 \wedge x'_2 = 60) \Rightarrow \neg\exists\Diamond_{<60} Cooling_2 \quad (9)$$

By Proposition 4.3 H_K satisfies formulas (4), (5) and (6) iff H_1 satisfies formulas (7), (8), and (9), respectively. The following results were obtained using the tool KRONOS [NSY92] to verify the formulas (7), (8) and (9) on the TG H_1.

formula	time in sec.	iterations	result
(7)	0.050	4	*true*
(8)	0.066	4	*true*
(9)	0.083	4	*true*

Then H_K satisfies formulas (4), (5) and (6) and by Proposition 4.2 the $\text{CSHS}_{\neq 0}$ H of Figure 2 satisfies formulas (1), (2) and (3).

4.3 Synthesis of results

By combination of the propositions 4.2 and 4.3, we obtain:

Proposition 4.4 *For any $CSHS_{\neq 0}$ H, interpretation M and* TCTL *formula f,*

$$H \models_{\Sigma,M} f \text{ iff } H_K \models_{\Sigma_K,M} | f |_K \text{ iff } H_1 \models_{\Sigma_1,M} || f |_K |_{\frac{1}{K}}$$

This proposition shows that the model-checking problem for $\text{CSHS}_{\neq 0}$ and TCTL is reduced to the problem of model-checking for TG. Now, the model-checking algorithm in [HNSY92] can be adapted for the timed graphs consider here, that is timed graphs having assignments of intervals instead of resets to zero. It can be shown that in this case the meaning of the formulas can be expressed with the same class of state predicates. Hence, the verification of TCTL formulas on $\text{CSHS}_{\neq 0}$ is decidable.

Figure 4 gives a diagram illustrating the results of Proposition 4.4.

5 From Linear Hybrid Systems to Timed Graphs

In this section we extend the translation method proposed for CSHS to LHS. We first define a subclass of LHS, denoted $\text{LHS}_{\neq 0}$, such that:

- For all locations $s \in S$ and variables $x \in X$, the end-points of the rate interval $A_s(x)$ and $B_s(x)$ are both positive or both negative, that is $0 \notin [A_s(x), B_s(x)]$.
- The invariant and the guards are boolean combinations of inequalities of the form $l \prec x \prec u$ with $\prec \in \{<, \leq\}$.

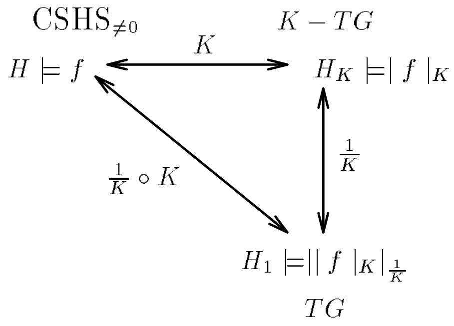

Figure 4: diagram.

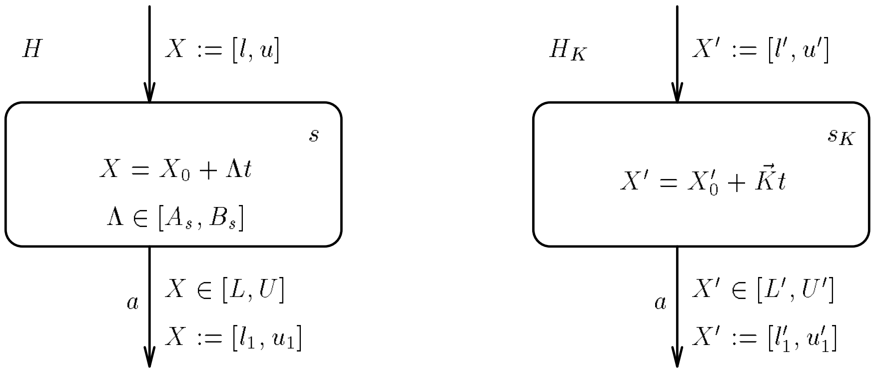

Figure 5: States s and s_K of H and H_K

- For all edges $e \in E$ and for all variables $x \in X$, if the rates of change of x are different at the source location and at the target location, then x must be in the assignment.
- If at some location s the slope of x is positive (negative) then assignments to x in edges with target location s or in conditions on x in guards of edges with source location s the lower bounds (upper bounds) are different from $-\infty$ ($+\infty$).

5.1 Translating $\mathrm{LHS}_{\neq 0}$ into K-TG

The following proposition shows that unfortunately the result that for any H in $\mathrm{CSHS}_{\neq 0}$ there exist a bisimilar K-TG cannot be extended to $\mathrm{LHS}_{\neq 0}$.

Proposition 5.1 *Given a $H = \langle S, X, E, A, B, \phi\rangle$ in $LHS_{\neq 0}$ such that for some $s \in S$*

- *$A_s < B_s$*
- *there exists $e \in E$ such that $e = \langle s, a, [L, U], \upsilon, s'\rangle$*

there exists no H_K in K-TG with initial state q_K such that $\langle H, q\rangle \sim \langle H_K, q_K\rangle$ for all the states q from which there exists a trajectory crossing the edge e.

Proof: Suppose that the proposition is false and let X and X' be respectively the set of variables of H and H_K such that there exist a relation ρ and states q, q_K such that $\langle H, q\rangle \sim_\rho \langle H_K, q_K\rangle$. Then there exists a sequence of bisimilar states from q and q_K respectively leading to state (s, X_0) and (s_K, X'_0) such that $\rho((s, X_0), (s_K, X'_0))$, $A_s < B_s$ and there exists $e \in E$ with source s such that $e = \langle s, a, [L, U], v, s'\rangle$. As ρ is a bisimulation there should exist an edge e_K from s_K of the form $e_K = \langle s_K, a, [L', U'], v', s'_K\rangle$
The Figure 5 illustrates this situation.

- Suppose that $X_0 \notin [L, U]$ which implies that $X'_0 \notin [L', U']$. Consider t such that $X'_0 + \vec{K}t \in [L', U']$ and for all $t' < t$ $X'_0 + \vec{K}t' \notin [L', U']$. Then as $\rho((s, X_0), (s_K, X'_0))$ for any $\Lambda \in [A_s, B_s]$ $X_0 + \Lambda t \in [L', U']$, in particular $X_0 + A_s t \in [L', U']$. Let Λ' be a rate $A_s < \Lambda' \leq B_s$ and $t' < t$ such that $A_s t = \Lambda' t'$. Then $X_0 + \Lambda' t' \in [L, U]$ and by the fact that $\rho((s, X_0), (s_K, X'_0))$, we have $X'_0 + \vec{K}t' \in [L', U']$ yielding a contradiction.

- Suppose that $X_0 \in [L, U]$ which implies that $X'_0 \in [L', U']$. Consider t such that $X'_0 + \vec{K}t \in [L', U']$ and for all $t' > t$ $X'_0 + \vec{K}t' \notin [L', U']$. Then as $\rho((s, X_0), (s_K, X'_0))$ for any $\Lambda \in [A_s, B_s]$ $X_0 + \Lambda t \in [L', U']$, in particular $X_0 + B_s t \in [L', U']$. Let Λ' be a rate $A_s \leq \Lambda' < B_s$ and $t' > t$ such that $B_s t = \Lambda' t'$. Then $X_0 + \Lambda' t' \in [L, U]$ and by the fact that $\rho((s, X_0), (s_K, X'_0))$, we have $X'_0 + \vec{K}t' \in [L', U']$ yielding a contradiction.

5.1.1 The generalized K-transformation

Proposition 5.1 states that it is not possible (in general) to transform a given LHS$_{\neq 0}$ into a bisimilar K-TG. However, we define a transformation of H into an abstract H', in the sense that every transition in the model of H corresponds to a transition in the model of H' (the model of H simulates the model of H').

Given $H = \langle S, X, E, A, B, \phi\rangle$ in LHS$_{\neq 0}$, and a set of variables X' in bijection with X, we define the relation K as the set of relations $\kappa = \{\kappa_s \mid s \in S\}$ relating X and X' as follows:

$$\kappa_s(X, X') \text{ iff } \frac{K}{B_s}X + C_s \leq X' \leq \frac{K}{A_s}X + C_s$$

where

- $K = \mathsf{lcm}\{\text{abs}(A_s(x)), \text{abs}(B_s(x)) \mid x \in X, s \in S\}$, that is K is the least common multiple of the absolute values of all different end-points of the rate intervals.

- C_s is a tuple such that $C_s(x)$ is the maximum of the absolute values of all the constants appearing in assignments to x in edges with target location s or in conditions on x in guards of edges with source location s, multiplied by $\mathsf{max}(\text{abs}(\frac{K}{A_s(x)}), \text{abs}(\frac{K}{B_s(x)}))$.

From H and κ the K-timed graph $H_K = \langle S, X', E', \vec{K}, \phi'\rangle$ is defined as follows:

- X' is in bijection with X.

- To compute E' and ϕ' we replace every condition $l \prec x \prec u$ appearing in guards of edges with source s, in assignments of edges with target s or in ϕ_s by a condition $\frac{K}{B_s(x)}l + C_s(x) \prec x' \prec \frac{K}{A_s(x)}u + C_s(x)$ when $A_s(x)$ and $B_s(x)$ are positive, or $\frac{K}{A_s(x)}u + C_s(x) \prec x' \prec \frac{K}{B_s(x)}l + C_s(x)$ when $A_s(x)$ and $B_s(x)$ are negative.

Is important to note that when $A = B$, H is a CSHS$_{\neq 0}$ and the generalized K-transformation coincides with the K-transformation defined in Section 4.1.1.

5.1.2 Simulation

We want to prove that H simulates H_K. We first recall the definition of simulation.

Definition 5.1 Let $T_1 = \langle Q_1, \rightarrow_1 \rangle$ and $T_2 = \langle Q_2, \rightarrow_2 \rangle$ be two labeled transition systems over a set $\mathcal{L}$ of labels and a relation $\rho \subseteq Q_1 \times Q_2$.

The relation ρ is a *simulation* from T_1 to T_2, if $\rho(q_1, q_2)$ implies for every label $\ell \in \mathcal{L}$:

- If $q_1 \xrightarrow{\ell} q_1'$, then there exists q_2' such that $q_2 \xrightarrow{\ell} q_2'$ and $\rho(q_1', q_2')$.

We say that T_1 *simulates* T_2, denoted $T_1 \sqsubseteq T_2$, if there exists a relation ρ such that ρ is a simulation from T_1 to T_2.

For H_1 and H_2 linear hybrid systems, we write $H_1 \sqsubseteq H_2$ if there exists a relation ρ such that ρ is a simulation from the model of H_1 to the model of H_2. ■

We naturally extend the relation κ on states in the following way:

$$\kappa((s, X), (s', X')) \text{ iff } s = s' \text{ and } \kappa_s(X, X')$$

Lemma 5.1 *For all LHS*$_{\neq 0}$ *H, $H \sim_\kappa H_K$ if only timed transitions are considered.*

Proof: Consider X_0, X_0' such that $\kappa((s, X_0), (s, X_0'))$. Then $\frac{K}{B_s} X_0 + C_s \leq X_0' \leq \frac{K}{A_s} X_0 + C_s$.

- Suppose $(s, X_0) \xrightarrow{t} (s, X)$ which implies $X_0 + A_s t \leq X \leq X_0 + B_s t$. Consider X' such that $X' = X_0' + \vec{K} t$ which implies $(s, X_0') \xrightarrow{t} (s, X')$. By combination of the inequalities, we obtain:
  $\frac{K}{B_s} X_0 + C_s + \vec{K} t \leq X' \leq \frac{K}{A_s} X_0 + C_s + \vec{K} t$ i.e. $\frac{K}{B_s}(X_0 + B_s t) + C_s \leq X' \leq \frac{K}{A_s}(X_0 + A_s t) + C_s$.
  Then $\frac{K}{B_s} X + C_s \leq X' \leq \frac{K}{A_s} X + C_s$, that is $\kappa((s, X), (s, X'))$.

- Suppose $(s, X_0') \xrightarrow{t} (s, X')$ which implies $X' = X_0' + \vec{K} t$. Consider X such that $X = X_0 + \Lambda t$ with $\Lambda \in [A, B]$ which implies $(s, X_0) \xrightarrow{t} (s, X)$ and $X_0 + A_s t \leq X \leq X_0 + B_s t$. By combination of the inequalities, we obtain:
  $\frac{K}{B_s} X_0 + C_s + \vec{K} t \leq X' \leq \frac{K}{A_s} X_0 + C_s + \vec{K} t$ i.e. $\frac{K}{B_s}(X_0 + B_s t) + C_s \leq X' \leq \frac{K}{A_s}(X_0 + A_s t) + C_s$.
  Then $\frac{K}{B_s} X + C_s \leq X' \leq \frac{K}{A_s} X + C_s$, that is $\kappa((s, X), (s, X'))$. ■

Lemma 5.2 *For all LHS*$_{\neq 0}$ *H, $H \sqsubseteq H_K$ if only discrete transitions are considered.*

Proof: Let X_0, X_0' such that $\kappa((s, X_0), (s, X_0'))$ for some location s and $(s, X_0) \xrightarrow{a} (s_1, X_1)$ by crossing an edge $e = \langle s, a, [L, U], [l_1, u_1], s_1 \rangle$ as in Figure 5.
Then $X_0 \in [L, U]$ and $X_1 \in [l_1, u_1]$. As $K_s(X_0, X_0')$ we have $\frac{K}{B_s} X_0 + C_s \leq X_0' \leq \frac{K}{A_s} X_0 + C_s$, and consequently $X_0' \in [L', U']$. This implies that an action a can be executed from state (s, X_0').
Let (s_1, X_1') be the resulting state, i.e. $(s, X_0') \xrightarrow{a} (s_1, X_1')$. Then $X_1' \in [l_1', u_1']$ which is equivalent to $\frac{K}{B_s} l_1 + C_s \leq X_1' \leq \frac{K}{A_s} u_1 + C_s$ (by definition of H_K). Thus, $\kappa((s_1, X_1), (s_1, X_1'))$. ■

Proposition 5.2 *For all LHS*$_{\neq 0}$ *H, $H \sqsubseteq H_K$.*

Proof: By combining Lemmas 5.1 and 5.2. ■

5.1.3 Property preservation by K-transformation

We show that an interesting subset of TCTL, called ∀TCTL, is preserved by the relation K from H_K to H, that is, if $f \in$ ∀TCTL is satisfied by H_K then H satisfies a corresponding formula $\mid f \mid_K \in$ ∀TCTL. ∀TCTL is the subset of TCTL defined as follows:

$$f \quad ::= \quad p \mid \neg p \mid l \prec x \prec u \mid f_1 \wedge f_2 \mid f_1 \vee f_2 \mid f_1 \forall\mathcal{W}_{\# n} f_2 \mid f_1 \forall\mathcal{U}_{\prec n} f_2$$

where $f_1 \forall\mathcal{W}_{\# n} f_2$ and p, x, l, u, $\prec$, n and $\#$ are as in definition of Section 3.1.

For any formula f in ∀TCTL we define a formula $\mid f \mid_K$ as follows:

$$\begin{array}{rcl} \mid p \mid_K & = & p \\ \mid \neg p \mid_K & = & \neg \mid p \mid_K \\ \mid l \prec x \prec u \mid_K & = & \bigvee_{s \in S} p_s \wedge {\kappa_{s,x}}^{-1}(l \prec x \prec u) \\ \mid f_1 \; op \; f_2 \mid_K & = & \mid f_1 \mid_K \; op \; \mid f_2 \mid_K \;\; \text{for} \;\; op \in \{\wedge, \vee, \forall\mathcal{W}_{\# n}, \forall\mathcal{U}_{\prec n}\} \end{array}$$

where ${\kappa_{s,x}}^{-1}(l \prec x \prec u)$ is $\frac{l - C_s(x)}{K} A_s(x) \prec x \prec \frac{u - C_s(x)}{K} B_s(x)$.

Proposition 5.3 *For any $H \in LHS_{\neq 0}$ and any f formula of* ∀TCTL*,*

$$\textit{if } H_K \models f \textit{ then } H \models \mid f \mid_K .$$

Proof: Let $\langle Q, \rightarrow \rangle$ and $\langle Q_K, \rightarrow_K \rangle$ be the models of H and H_K, respectively.

Notice that for any two states $q \in Q$ and $q' \in Q_K$ satisfying $\kappa(q, q')$ Lemma 5.1 shows that for every t, all time successors of q by t are related by κ to the *unique* time successor of q' by t, because the model of H_K is deterministic with respect to timed transitions.

Then, trajectories of H are related to trajectories of H_K in the following way. Let $q_0 \in Q$ and $q'_0 \in Q_K$ such that $\kappa(q_0, q'_0)$. For any trajectory $\sigma = q_0 \overset{t_0}{\mapsto} q_1 \ldots \in \Sigma(q_0)$ there exists an unique trajectory $[\sigma] = q'_0 \overset{t_0}{\mapsto} q'_1 \ldots \in \Sigma_K(q'_0)$ such that for all $i \geq 0$, $\kappa(q_i, q'_i)$ and for all $0 < t \leq t_i$, $\kappa(\sigma(i,t), [\sigma](i,t))$.

Now we prove that for every formula $f \in$ ∀TCTL and for every state $q' \in Q_K$, $q' \models f$ implies for every state $q \in Q$ such that $\kappa(q, q')$ $q \models \mid f \mid_K$. The proof is carried out by induction on the structure of f. We give hereafter hints of proof for temporal operators assuming that the proposition holds for f_1 and f_2.

- Let f be the formula $f_1 \forall\mathcal{W}_{\# n} f_2$ and $q' \in Q_K$ such that $q' \models f$. We show that for all $q \in Q$ such that $\kappa(q, q')$ we have $q \models \mid f \mid_K$. We proceed by contradiction. Suppose that there is a $q \not\models \mid f \mid_K$. Then, there exists a trajectory $\sigma \in \Sigma(q)$ and a position π such that $\sigma(\pi) \not\models \mid f_2 \mid_K$, $\tau_\sigma(\pi) \# n$ and for all $\pi' \preceq \pi$, $\sigma(\pi') \not\models \mid f_1 \wedge f_2 \mid_K$. Then, by induction hypothesis we have that the corresponding trajectory $[\sigma]$ is such that $[\sigma](\pi) \not\models f_2$, $\tau_{[\sigma]}(\pi) \# n$ and for all $\pi' \preceq \pi$, $[\sigma](\pi') \not\models f_1 \wedge f_2$. This implies $q' \not\models f$ yielding a contradiction.

- Let f be the formula $f_1 \forall\mathcal{U}_{\prec n} f_2$ and $q' \in Q_K$ such that $q' \models f$. We show that for all $q \in Q$ such that $\kappa(q, q')$ we have $q \models \mid f \mid_K$. We proceed by contradiction. Suppose that there is a $q \not\models \mid f \mid_K$. Then, there exists a trajectory $\sigma \in \Sigma(q)$ such that for all positions π if $\tau_\sigma(\pi) \prec n$ then $\sigma(\pi) \not\models \mid f_2 \mid_K$ or there exists a $\pi' \preceq \pi$ such that $\sigma(\pi') \not\models \mid f_1 \vee f_2 \mid_K$. Then, by induction hypothesis we have that the corresponding trajectory $[\sigma]$ is such that for all positions π, if $\tau_{[\sigma]}(\pi) \prec n$ then $[\sigma](\pi) \not\models f_2$ or there exists a $\pi' \preceq \pi$ such that $[\sigma](\pi') \not\models f_1 \vee f_2$. This implies $q' \not\models f$ yielding a contradiction. ■

5.2 Example

Consider the example of Section 2.3 modeled by the LHS H of Figure 1. The Figure 6 shows the K-TG H_K.

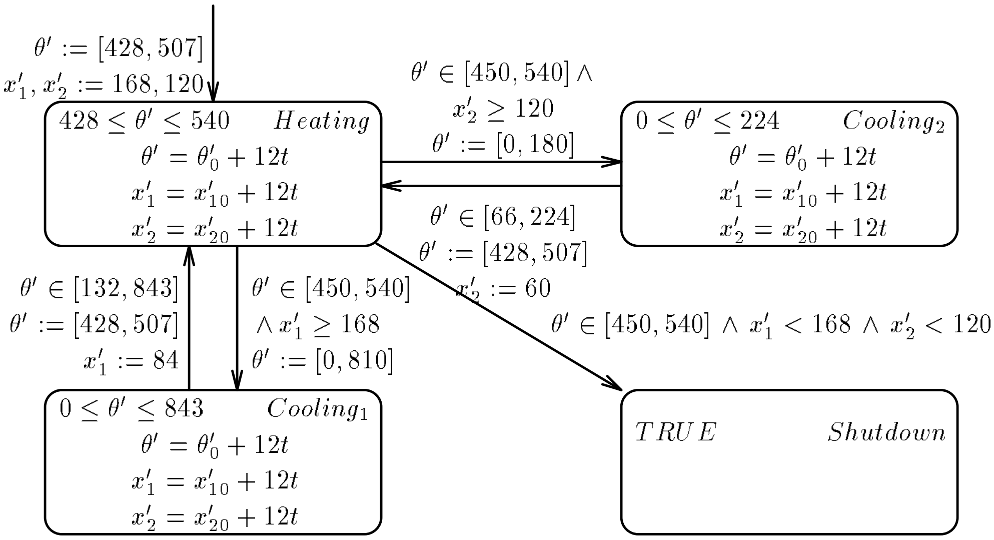

Figure 6: Temperature control system (H_K)

The relation κ for H is:

$$\begin{array}{rcccll}
2\theta + 270 & \le & \theta' & \le & 3\theta + 270 & \text{at location } Heating \\
-12\theta + 1080 & \le & \theta' & \le & -3\theta + 1080 & \text{at location } Cooling_1 \\
-6\theta + 540 & \le & \theta' & \le & -4\theta + 540 & \text{at location } Cooling_2 \\
 & & x'_1 & = & 12x_1 + 84 & \text{at all locations} \\
 & & x'_2 & = & 12x_2 + 60 & \text{at all locations}
\end{array}$$

The $\frac{1}{K}$-transformation is applicable to the system H_K of Figure 6 to obtain a TG H_1. Consider the following formulas:

$$(Heating \wedge 428 \le \theta' \le 507 \wedge x'_1 = 168 \wedge x'_2 = 120) \Rightarrow \forall\Box\neg Shutdown \tag{10}$$

$$(Heating \wedge 428 \le \theta' \le 507 \wedge x'_1 = 84) \Rightarrow \neg\exists\Diamond_{<84} Cooling_1 \tag{11}$$

$$(Heating \wedge 428 \le \theta' \le 507 \wedge x'_2 = 60) \Rightarrow \neg\exists\Diamond_{<60} Cooling_2 \tag{12}$$

It can be shown that if H_1 satisfies formulas (10), (11) and (12) then the LHS$_{\neq 0}$ H of Figure 1 satisfies formulas (1), (2) and (3).

The following results were obtained using the tool Kronos to verify the formulas (10), (11) and (12) on the TG H_1.

formula	time in sec.	iterations	result
(10)	0.084	7	*false*
(11)	0.117	4	*true*
(12)	0.084	4	*true*

Notice that formulas (11) and (12) are verified which implies that formulas (2) and (3) are satisfied by the system of Figure 1. On the contrary, formula (10) is not verified and nothing can be said about the validity of formula (1).

6 Conclusion

As mentioned in the introduction, the paper contributes in two different directions to the development of a verification methodology for LHS:

- it shows that decidability results for TCTL on timed graphs and, in particular the associated verification methods and tools, can be extended to a non-trivial class of CSHS, the so called Non-Zero Constant Slope Hybrid Systems $\mathrm{CSHS}_{\neq 0}$. Even though the latter class is semantically equivalent to timed graphs, we noticed that several examples of LHS in the literature happen to belong to $\mathrm{CSHS}_{\neq 0}$.
- it shows that well-known results of property preservation by abstractions can be adapted to the case of $\mathrm{LHS}_{\neq 0}$. The generalized K-transformation presented in Section 5 maps this class to timed graphs and, consequently, the verification of a large class of properties such as invariance and bounded inevitability, on some element of $\mathrm{LHS}_{\neq 0}$, can be reduced to the verification of the same property on the corresponding timed graph. It remains to evaluate through examples the usefulness of this approach, that is how much faithful are the abstractions defined by K.

Although the results in each direction are qualitatively different, the approach followed to obtain them is the same: it consists in applying transformations yielding abstractions. As noticed, the K-transformation is a special case of the K-transformation for CSHS such that the initial system is not only similar to the transformed system but also bisimilar. From this point of view, a different exposition of the results could be done by presenting first the general case.

The study of a general framework for the definition and computation of property preserving abstractions of LHS is the object of a forthcoming paper.

References

[ACD90] R. Alur, C. Courcoubetis, and D. Dill. Model-checking for real-time systems. In *Proc. 5th Symp. on Logics in Computer Science*, pages 414–425. IEEE Computer Society Press, 1990.

[ACHH93] R. Alur, C. Courcoubetis, T. A. Henzinger, and Pei-Hsin Ho. Hybrid automata: an algorithmic approach to the specification and analysis of hybrid systems. In *Workshop on Theory of Hybrid Systems*, Lyngby, Denmark, June 1993. Lecture Notes in Computer Science 736, Springer-Verlag.

[Alu91] R. Alur. *Techniques for automatic verification of real-time systems.* PhD thesis, Department of Computer Science, Stanford University, August 1991.

[BBLS92] A. Bouajjani, S. Bensalem, C. Loiseaux, and J. Sifakis. Property preserving simulations. In *Proc. 4th Workshop on Computer-Aided Verification.* Lecture Notes in Computer Science 663, Springer-Verlag, 1992.

[BES93] A. Bouajjani, R. Echahed, and J. Sifakis. On model checking for real-time properties with durations. In *Proc. 8th Symp. on Logics in Computer Science.* IEEE Computer Society Press, 1993.

[CES86] E.M. Clarke, E.A. Emerson, and A.P. Sistla. Automatic verification of finite-state concurrent systems using temporal logic specifications. *ACM Transactions on Programming Languages and Systems*, 8(2):244–263, 1986.

[GL93] S. Graf and C. Loiseaux. A tool for symbolic program verification and abstraction. In C. Courcoubetis, editor, *Proc. 5th Workshop on Computer-Aided Verification*, Greece, June 1993. Lecture Notes in Computer Science 697.

[Hal93] N. Halbwachs. Delay analysis in synchronous programs. In C. Courcoubetis, editor, *Proc. 5th Workshop on Computer-Aided Verification*, Greece, June 1993. Lecture Notes in Computer Science 697.

[HH93] T. Henzinger and P.-H. Ho. Automatic symbolic verification of embedded systems. In *Real-Time Systems Symposium*, 1993.

[HNSY92] T.A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model-checking for real-time systems. In *Proc. 7th Symp. on Logics in Computer Science*. IEEE Computer Society Press, 1992.

[JLHM91] M. Jaffe, N. Leveson, M. Heimdahl, and B. Melhart. Software requirements analysis for real-time process-control systems. *IEEE Transactions on Software Engineering*, 17(3):241–258, 1991.

[KPSY93] Y. Kesten, A. Pnueli, J. Sifakis, and S. Yovine. Integration graphs: a class of decidable hybrid systems. In *Workshop on Theory of Hybrid Systems*, Lyngby, Denmark, June 1993. Lecture Notes in Computer Science 736, Springer-Verlag.

[MMP91] O. Maler, Z. Manna, and A. Pnueli. From timed to hybrid systems. In *Proc. REX Workshop "Real-Time: Theory in Practice"*, the Netherlands, June 1991. Lecture Notes in Computer Science 600, Springer-Verlag.

[NOSY93] X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. An approach to the description and analysis of hybrid systems. In *Workshop on Theory of Hybrid Systems*, Lyngby, Denmark, June 1993. Lecture Notes in Computer Science 736, Springer-Verlag.

[NSY91] X. Nicollin, J. Sifakis, and S. Yovine. From ATP to timed graphs and hybrid systems. In *Proc. REX Workshop "Real-Time: Theory in Practice"*, the Netherlands, June 1991. Lecture Notes in Computer Science 600, Springer-Verlag.

[NSY92] X. Nicollin, J. Sifakis, and S. Yovine. Compiling real-time specifications into extended automata. *IEEE TSE Special Issue on Real-Time Systems*, 18(9):794–804, September 1992.

[WTD93] H. Wong-Toi and D. Dill. Using iterative symbolic approximations for timing verification. In *First AMAST International Workshop on Real-Time Systems*, Iowa, November 1993.